

CPDP.ai 2025

Session Reports



Day 2

With thanks to our rapporteurs.

Enjoy the sessions like a podcast—
links can be found in [Recording](#).

Bridging the Gap with PETs: Governments' Opportunity to Lead on Innovation and Privacy, 22 May, Grande Halle

Recording

Rapporteur: Ezgi Ercan

Moderator: Rob Van Eijk, Future of Privacy Forum

Panellist 1: Sarah Holland, Google

Panellist 2: Christian Reimsbach-Kounatze, OECD

Panellist 3: Valda Beizitere, DG JUST

Moderator's remarks

Moderator Rob Van Eijk opened by highlighting four key points for the panel: how governments can ensure that privacy-enhancing technologies (PETs) build user's trust and privacy; the role of regulation and guidance in promoting responsible PETs use; the importance of collaboration between public and private sector research alongside interoperable standards to drive innovation and data protection; and finally, what types of government support, resources, or investments can best help organisations overcome current barriers to PETs adoption. He encouraged the audience to consider practical examples such as libraries, GitHub repositories, and real-world use cases to show how these tools can foster trust. The tone set by the moderator was constructive.

Panellists' contributions

Panellist Sarah Holland (Google) explained that PETs adoption remains limited, despite its potential for AI applications across businesses and governments. Key barriers include organisational challenges, technical complexity, and resource constraints. She stressed the need for a collective effort involving industry, civil society, academia, and government

to raise understanding of what PETs are and how they should be used effectively. Cost and computational demands also hinder uptake, especially for less tech-savvy organisations. Holland outlined a framework for adopting PETs, emphasising threat modelling, legal risk assessment, and resource evaluation to ensure that PETs address specific risks. She emphasised that PETs are not a silver bullet, but with the right approach, they can significantly enhance privacy and security. Holland also provided a concrete example from the financial sector, describing how PETs enable banks to communicate securely for fraud prevention without exposing sensitive customer data, showcasing PETs' potential in heavily regulated industries. She also mentioned Google's long-term investments in open research, the importance of regulatory sandboxes for testing, and government support for skill building and fundamental research.

Panellist Christian Reimsbach-Kounatze (OECD) categorised the challenges into three main areas: cost-effectiveness, market competition, and skills/awareness. He highlighted that while PETs can be expensive, government support for Research & Development (R&D) is crucial to reducing costs. Competitive markets and user awareness will also drive adoption. Beyond privacy, PETs protect intellectual property and enable secure data sharing, adding value for businesses and governments alike. Reimsbach-Kounatze stressed the need to develop repositories of use cases to benchmark PETs' effectiveness and foster shared understanding. On building trust in PETs and related tools like age verification libraries, he emphasised the importance of open-source implementations combined with certification to reduce transaction costs and security risks. Reimsbach-Kounatze highlighted the need for international convergence through common use cases and a shared terminological and conceptual vocabulary to reduce legal and technical misunderstandings. He gave examples where companies seek to collaborate on customer data without sharing identifiable information, illustrating the practical value of PETs.

Valda Beizitere (DG JUST) discussed the EU's work on infrastructure such as eIDAS and its second-stage e-wallet, which empower citizens with control over their data. She highlighted ongoing efforts to develop privacy-friendly age verification tools using zero-knowledge proofs, designed to prevent linkability or traceability while enabling access control online. Beizitere emphasised the EU's commitment to promoting open-source solutions and ensuring that regulation supports innovation without stifling industry developments. She also noted the importance of funding access and regulatory clarity to encourage wider PETs' use. Beizitere reinforced that GDPR already embeds PETs' principles through data protection by design and default, and EU initiatives continue to promote trust and transparency. Regarding regulatory frameworks, she explained how the GDPR and the Data Governance Act, together with the debates they have triggered on anonymised data and data altruism, have shaped the EU's data strategy, which aims to facilitate trusted data-sharing ecosystems where PETs play a central role.

Discussion points from programme

Questions below have been answered as follows:

- How can governments ensure PETs use boosts user trust and privacy, and what key public initiatives can make their benefits clear and accessible to all?
 - Panellists agreed that governments play a vital role in fostering trust through transparent regulation, promotion of open-source tools, and supporting educational initiatives that increase understanding of PETs. Examples included the EU's eIDAS infrastructure and efforts to develop privacy-friendly age verification using zero-knowledge proofs. Public consultations and collaborations with industry help ensure PETs are both trustworthy and accessible.
- Where can regulation and guidance catalyse responsible PETs use?
 - It was emphasised that clear, flexible, and practical regulatory frameworks are necessary to encourage responsible use without stifling innovation. GDPR's principles of data protection by design and default already embed PETs conceptually. Upcoming policies, such as the Data Act and Data Governance Act, will further support trusted data sharing environments where PETs are instrumental.
- What role can public and private sector research and interoperable standards play in fostering collaborations to successfully drive both PET-enabled innovation and strong data protection?
 - The panel highlighted the importance of joint R&D efforts and standardisation to reduce costs, avoid fragmentation, and enable interoperability. Open-source projects and repositories of PET use cases were noted as key enablers of shared understanding and trust across sectors and borders.
- What forms of direct support, resources, or strategic investments from governments would most effectively help organisations overcome the current barriers to PETs' use?
 - Participants pointed out the need to fund fundamental research, creating regulatory sandboxes, and investing in skill development as crucial government actions. Support for smaller organisations, which often lack resources to experiment with PETs, was also stressed. Governments can help by providing clear guidance, incentives, and by fostering ecosystems that facilitate practical PETs adoption.

Summary of Q&A discussion

Q audience: How the panellists' institutions are addressing PETs, particularly regarding federated learning and AI principles.

- Christian Reimsbach-Kounatze: Cautioned against over-expecting from PETs alone and stressed their role as one tool among many. Highlighted PETs' potential competitive advantage, especially for smaller companies offering privacy-respecting services.
- Sarah Holland: Confirmed support for federated learning and emphasised the importance of open-sourcing investments in PETs.

The atmosphere during the Q&A was engaged and collaborative, with an evident interest in practical solutions and cross-sector dialogue.

Elevating AI Oversight: the Crucial Role of Regulatory Sandboxes and Competent Authorities under the AI Act, 22 May, Orangerie

Recording

Rapporteur: Ezgi Ercan, Timelex

Moderator: Nathan Genicot, FARI - AI for the Common Good Institute - Belgium

Panellist 1: Thiago Moraes, LSTS (VUB) - Belgium

Panellist 2: Alex Moltzau, European Commission (AI Office) - Europe

Panellist 3: Sophie Tomlinson, Datasphere Initiative - United Kingdom

Panellist 4: Sam Jungyun Choi, Covington & Burling - United Kingdom

Moderator's remarks

Nathan Genicot, representing FARI – AI for the Common Good Institute, opened the panel by introducing FARI as a Brussels-based non-profit institute founded by ULB and VUB universities. He explained that FARI is engaged in research and training on AI, data, and robotics, and is involved in several projects related to AI regulatory sandboxes under the EU AI Act. The aim of the panel, he noted, was not to revisit the basics of regulatory sandboxes, but to explore some of the most pressing issues surrounding their implementation. Genicot highlighted that the AI Act introduces regulatory sandboxes as a means of fostering innovation while ensuring compliance by facilitating dialogue between AI developers and competent authorities. He reminded the audience that Member States are required to establish at least one sandbox by August 2026. One major topic of discussion is the role of competent authorities, particularly data protection authorities, who must be involved where personal data is processed. He also raised the issue of how to protect business confidentiality and intellectual property within sandboxes, to ensure companies are willing to participate. Lastly, he underlined the importance of involving civil society in the sandbox process, to ensure it is not limited to

dialogue between regulators and AI providers. He then introduced the four panel speakers.

Panellists' contributions

Alex Moltzau began by clarifying that he was not representing the official views of the European Commission but rather participating in a personal capacity to share insights and learn from other perspectives. He explained that he works within DG CONNECT at the AI Office, focusing on the implementation of regulatory sandboxes under the AI Act. The Commission is coordinating with Member States through the AI Board, which comprises national representatives and includes 12 subgroups, one of which is specifically dedicated to AI regulatory sandboxes. This subgroup has held several meetings to discuss implementation challenges and draft a discussion paper to support coordination. Moltzau emphasised the importance of aligning national sandboxes with the horizontal objectives of the AI Act, which is primarily a product safety regulation. He highlighted the need to bridge regulatory sandboxes with existing testing infrastructures and acknowledged the varying capacities and resources across Member States. He also noted that some countries, such as Spain, have already launched pilot sandboxes and are actively engaging startups. Finally, he stressed the value of ongoing collaboration and the importance of building effective, flexible models tailored to national contexts while maintaining EU-wide coherence.

Sam Jungyun Choi spoke from a private practice perspective, sharing her professional interest in helping a company navigate a regulatory sandbox for the first time. She noted that while sandboxes are not new (having been used in sectors like fintech and medical devices), companies, especially larger ones, are often hesitant to engage directly with regulators due to concerns about legal risk and exposure. She argued that regulatory sandboxes hold real potential, particularly because AI regulation is evolving alongside the technology itself. In her view, sandboxes can offer a valuable space for dialogue and trust-building between regulators and industry. She gave examples from the mobility and healthcare sectors, where companies face significant data protection challenges. In such cases, targeted permissions and safeguards from regulators could give businesses the confidence they need to move forward. Choi also stressed the need for sandboxes to be clearly scoped and well-coordinated; this can be frustrating for companies to go through a sandbox process only to discover they must still meet separate obligations for data protection, sector-specific rules, or other frameworks. She suggested that a more integrated, cross-border approach would make sandboxes more appealing and effective in practice.

Sophie Tomlinson noted that governments around the world are increasingly using sandboxes as a way to approach regulation more iteratively; both to test new technologies and to see whether existing regulations are helping or hindering innovation.

One UK regulator, she said, compared sandboxes to the Marvel Universe: varied in form, but built on a shared foundation of supporting responsible innovation. Her team has mapped over 150 sandbox initiatives globally, observing how they often need to balance flexibility with accountability, and transparency with the need for a safe space to experiment. Tomlinson welcomed the inclusion of sandboxes in the EU AI Act and pointed out that Europe could learn from international experience; for example, Singapore, parts of Latin America, the UK, and Norway (which even has a podcast documenting its data protection sandbox). She emphasised the importance of shifting regulatory mindsets - not just focusing on compliance, but also on learning. Sandboxes offer value not only for companies but for regulators to build technological literacy. She raised a practical question from the company's perspective: if a product goes through a sandbox in one EU country, will that be recognised across the EU, or will companies face duplicative processes in other Member States? She noted that sandboxes can be resource-intensive and may deter participation unless the incentives are clear. Both large and small companies, she said, need greater clarity and efficiency to fully benefit from sandbox models.

Thiago Moraes shared insights from both his research and his experience advising a national regulator. Speaking in a personal capacity, he emphasised the complexity of implementing sandboxes in the context of the EU AI Act, particularly due to the number of market surveillance authorities that may be involved. The coordination challenge is real, especially as different national authorities will have differing roles and capacities. As one example, he described how Dutch regulators are planning a "single entry point" model, essentially a common desk where proposals are submitted and are then directed to relevant regulators, depending on the nature of the technology and the case. It is a creative model that illustrates the administrative complexity of cross-sectoral AI oversight. Moraes also shared findings from his research, tracing the evolution of sandboxes from fintech to energy to data protection. One surprising insight was that regulators often lack the infrastructure to support sandboxes fully. And despite assumptions, regulatory sandboxes rarely offer legal exemptions or "regulatory holidays." Instead, they may allow for temporary authorisations or flexibility in compliance timelines, but companies remain largely accountable. Regulatory guidance, he argued, is often the main incentive, along with the potential for increased credibility and investment. Looking forward, he argued that the EU should use its AI ecosystem: innovation hubs, test facilities, and data spaces to address the infrastructure gap that has historically limited the effectiveness of sandboxes. He concluded by stressing the importance of inclusion and participatory governance. He welcomed the AI Act's multi-stakeholder ambitions, but cautioned that, to live up to the EU's past commitments to responsible innovation, sandboxes must do more to involve civil society. That, he suggested, remains a key challenge.

During the rest of the discussion, Nathan Genicot mentioned a Commission-funded consortium working to help coordinate sandbox efforts across Europe. Alex emphasised Norway's approach, which prioritises free access for start-ups and SMEs, while Spain's model involves partnerships between large companies and smaller firms to pilot AI solutions strategically. Sam pointed out the data challenges companies face, stressing the need for clarity on applying AI principles, human oversight, and documentation standards through sandbox participation. She also raised questions about what assurances companies receive from sandbox exit reports. Sophie stressed the importance of clear governance structures and involving civil society to uphold public trust, noting that meaningful participation requires adequate resourcing. Thiago agreed, highlighting the need for flexible sandbox designs and genuine civil society involvement. He also noted the AI Act's requirement for annual evidence-based reporting to guide future innovation.

Discussion points from programme

Questions below have been answered as follows:

- Which competent authorities should oversee sandboxes, and what roles should market surveillance authorities play?
 - The panel agreed that it is complicated because multiple regulators are involved. Everyone agreed it's important to have clear roles and good cooperation, especially across borders. Thiago Moraes mentioned the Dutch approach of having a single-entry point to coordinate between different authorities, which could help avoid confusion.
- How can data protection authorities be effectively integrated into sandboxes when personal data is being processed?
 - Since AI often involves personal data, the data protection authorities need to be part of the sandbox process. At present, sandboxes mostly offer guidance rather than actual infrastructure, so regulators need to work closely to handle potential issues properly.
- How can companies' concerns, such as intellectual property and confidentiality issues, be addressed so that trust can be built between them and regulators in the sandbox?
 - Sam Jungyun Choi and Sophie Tomlinson said companies want legal certainty. Knowing how liability, intellectual property, and confidentiality are handled is key. Clear rules and transparency, like detailed exit reports, help companies feel comfortable sharing information and engaging with regulators.
- How could civil society be meaningfully integrated into the sandbox, and what role should it assume?

- The panel agreed that civil society is important for representing public interests and ensuring transparency. Sophie Tomlinson and Thiago Moraes pointed out that meaningful involvement needs resources and flexible sandbox designs. Civil society can help make sure innovation happens responsibly.

Summary of Q&A discussion

Q: Could you tell us more about the Spanish sandbox and whether it might be a good model for Europe?

Alex Moltzau pointed to the Dutch sandbox as a strong example, with its focus on coordination and collaboration with companies like Philips and various regulators. He also mentioned some promising work happening in the US. Sophie Tomlinson brought up the UK's Digital Regulation Cooperation Forum, where different regulators work together.

Q: How can we encourage all states to adopt sandboxes and make sure regulators engage properly? What about the role of data protection authorities, especially when personal data is involved?

Alex Moltzau spoke about the importance of preparatory funding and developing national competent authorities. He stressed working closely with companies and regulators, and noted that workshops and support actions help spread good practice.

Sophie Tomlinson mentioned the Dutch data protection authority, and explained that while some sandbox elements differ, regulators still expect high standards. For example, GDPR calls for consulting data subjects before processing personal data, but few organisations do this in practice. The panel agreed that making sure organisations actually use sandboxes to meet these requirements remains a challenge.

Q: Are there examples where legal and technical advice are provided together in sandboxes? How do sandboxes help with interpreting the AI Act in practice?

Sophie Tomlinson referred to work at VUB and Trinity College Dublin, where fundamental rights assessments are being developed and applied, including in public procurement. Sam Jungyun Choi added that previous cases involving automated surveillance and credit scoring offer valuable insights, especially on human review safeguards.

Sam Jungyun Choi said sandboxes offer practical legal advice to help companies manage risks, which should clarify how regulators will apply the AI Act, especially in sensitive areas like credit scoring.

Sophie Tomlinson highlighted Singapore's sandbox, where companies working on privacy-enhancing technologies collaborate with authorities to update their regulatory views. Thiago Moraes noted that Singapore has also developed technical guidelines

inspired by sandbox experiences, including guidance from the UK's ICO. Both Alex Moltzau and Thiago Moraes agreed that public procurement is a useful tool for encouraging adoption of sandbox outcomes and setting softer regulatory standards.

Emerging Patterns in EU Digital Regulation, 22 May, Grande Halle

Recording

Rapporteur: Liubomir Nikiforov, BPH

Moderator: Nóra Ni Loideain, Institute of Advanced Legal Studies, University of London

Panellist 1: Karolina Mojzesowicz, DG Just

Panellist 2: Anu Talus, European Data Protection Board

Panellist 3: Matthias Spielkamp, AlgorithmWatch

Panellist 4: Maximilian von Grafenstein, Berlin University of the Arts/
Alexander von Humboldt Institute for Internet and Society

Panellist 5: Charles-Albert Helleputte “Charly”, King & Spalding

Moderator’s remarks

Moderator Nóra Ni Loideain opened by observing that the EU has pursued an “unquestionably ambitious and complex” digital agenda for nearly two decades. The GDPR remains foundational, yet new instruments — DMA, DSA, AI Act, Data Governance/Data Act and a mooted Digital Fairness Act — are reshaping both enforcement architecture and compliance burdens. Ni Loideain stressed that answers must balance innovation, competitiveness, and fundamental-rights protection, and welcomed the panellists for their regulator, DPA, private-practice, civil-society, and academic perspectives.

Panellists’ contributions

Karolina Mojzesowicz (European Commission)

Karolina Mojzesowicz delivered the policy-maker's map. She emphasised "horizontal consistency" across the expanding digital acquis: core GDPR notions now anchor DMA, DSA, AI Act, and future files. Three cooperation layers are taking shape: formal high-level boards (e.g., DMA group), informal joint-guideline drafting, and national "digital clusters" such as Germany's cross-ministry model — all meant to reconcile divergent objectives (contestable markets, safe online spaces, AI safety) under a single risk-based logic. Yet she conceded that cross-border GDPR enforcement still drags; procedural deadlines in newer acts (DMA) aim to avoid a repeat.

Anu Talus (European Data Protection Board)

Anu Talus offered the DPA coordination lens. The EDPB's one-stop-shop, expert pools and coordinated-enforcement framework now underpin broader cross-regulatory work. Recent EDPB opinions on *consent-or-pay* and on *AI-training data* were co-drafted with competition and consumer enforcers, foreshadowing DPAs' envisaged role under the AI Act. Talus argued DPAs' independence and data-rights expertise suit them to "market-surveillance-plus" duties but warned that confidentiality and resource rules must evolve for case-data sharing across regimes.

Charles-Albert Helleputte (King & Spalding)

Charles-Albert Helleputte delivered a private-practice critique. Calling the EU a "champion of regulation but not of infrastructure," he tallied "101 digital laws" and lamented the scarce capital for EU tech scale-ups. For clients, success equals clear, principle-based rules "smartly enforced" by a lead authority that can defend decisions in court. Iterative rule-changes before older laws take hold create a "moving-target" problem; he advocated a threshold model, where a central enforcer handles high-impact cases and local regulators manage routine matters.

Matthias Spielkamp (AlgorithmWatch)

Matthias Spielkamp offered the **civil--society watchdog perspective**. AlgorithmWatch must both *use* new laws (e.g., DSA Article 40 data-access rights) and *comply* with others (GDPR). He welcomed strong transparency mandates but slammed chronic delays in secondary legislation: "If a delegated act arrives two years late, the right exists only on paper." Spielkamp distinguished genuine "coherence" from political "simplification" drives that risk gutting safeguards under the banner of deregulation. He traced that pressure to trans-atlantic competitiveness narratives and urged lawmakers to prioritise enforceable rights over headline counts of new acts.

Maximilian von Grafenstein (Berlin University of the Arts)

Maximilian von Grafenstein closed with a systemic academic view. He distilled EU digital policy into an equation: value created by data-driven innovation must exceed risks and compliance costs. Legislators, regulators, and businesses should adopt KPIs tied to that formula. While praising the Data Governance Act/Data Act for shifting toward value-sharing, he warned that SMEs and public bodies still drown in procedural overheads that Big Tech can absorb. Lawyers, he argued, should “solve compliance risks, not merely bill for explaining them,” and operational toolkits should take precedence over further legislative proliferation.

Discussion points from programme

What are the emerging trends in the implementation of the EU digital framework?

Shift from drafting new acts to operationalising the existing bundle. Regulators are building permanent cross-mandate bodies (DMA high-level group, EDPB-AI Office liaison, national “digital clusters”) to align definitions and risk tests. Newer acts embed stricter procedural clocks and delegated-act mechanisms to avoid GDPR-style delays. Cyber-incident rules under NIS 2 are expected to dovetail with data-protection and platform-governance workflows.

Which institutions are emerging as key actors in the implementation of the EU digital framework, and how do they engage with each other?

Data-protection authorities remain the primary rights-experts, but the European Commission (DG CNECT, DG COMP, New AI Office) is evolving into a meta-coordinator. The resulting architecture looks like a hub-and-spoke: sectoral regulators investigate, the Commission convenes, and the CJEU (Court of Justice of the European Union) supplies doctrinal coherence. Non-state actors — litigation funders, civil-society auditors, academic labs — are becoming “shadow enforcers,” testing gaps (e.g., AlgorithmWatch’s data-donation audits) and feeding evidence back into formal procedures.

How can the success of the EU digital framework be measured?

No single KPI suffices. Proposed dashboard: (i) value-risk-cost ratio (von Grafenstein); (ii) resolution speed—time from complaint to binding decision; (iii) cross-citation rate among regulators/courts (a proxy for interpretive interoperability); (iv) uptake of new rights—e.g., volume and turnaround time of DSA Article 40 data-access requests; (v) judicial resilience—percentage of regulatory decisions that survive court appeal

(Helleputte). Spielkamp added a negative KPI: “right without implementing act” counts as failure.

What challenges are emerging as a result of current implementation practices?

Four clusters dominate: legal instability from mid-stream rule tweaks (Helleputte); resource asymmetry—Big Tech can absorb compliance costs, SMEs and public bodies struggle (von Grafenstein; Talus on SME guidance); delegated-act bottlenecks—rights exist but remain unusable pending secondary rules (Spielkamp on DSA data-access); and confidentiality barriers that hamper cross-authority information sharing (Talus & Mojzesowicz). The Commission is piloting a “Digital Clearinghouse 2.0” to address the last point, while also mapping genuinely unregulated gaps before finalising the DFA to avoid duplication.

Summary of Q&A discussion

Question 1 - Brussels lawyer: Should the *value-risk-cost* formula be embedded in every EU impact assessment, and must the CJEU budget for a surge in preliminary-ruling requests?

Maximilian von Grafenstein: Yes; the formula forces lawmakers to prove that proposed rules increase value more than cost or risk. Data collection should be shared across regulators, industry, and academia.

Karolina Mojzesowicz noted the Better-Regulation Toolbox already weighs costs and benefits but is open to clearer KPIs. CJEU capacity planning is indeed on the radar, though case-load spikes are hard to model.

Question 2: Can multiple regulatory “boards” share case data despite confidentiality constraints (proposal for Digital Clearinghouse 2.0)?

Karolina Mojzesowicz said the Commission is studying the platform, sharing must respect self-incrimination and business-secrecy limits, but joint guidance, coordinated inspections, and anonymised data-pools are feasible interim steps.

Question 3: Will the Digital Fairness Act duplicate existing duties and inflate compliance?

Charles-Albert Helleputte warned of overlap, citing dark-pattern bans already in GDPR, UCPD and DSA.

Karolina Mojzesowicz replied that, DFA will target specific gaps (influencer marketing, “dark-funnel” contract withdrawals) and an overlap study is ongoing before final scope is set.

The Economic Benefits of Having a DPO, 22 May, Class Room

Recording

Rapporteur: Liubomir Nikiforov, BPH

Moderator: Aymeric Pontvianne, CNIL

Panellist 1: Ricardo Catalan, Autoriteit Persoonsgegevens

Panellist 2: Nadia Arnaboldi, AssoDPO

Panellist 3: Thomas van Gremberghe, Agoria

Panellist 4: Gerard Buckley, University College London

Moderator's remarks

The moderator Aymeric Pontvianne opened by framing a “new but overdue” research question: What are the economic benefits of appointing a Data-Protection Officer? He set four guiding queries for the discussion: (1) Which tangible gains do organisations experience? (2) Should a DPO be viewed as a cost centre, an asset or a long-term investment? (3) Do benefits differ by company size, data-centricity or compliance culture? (4) How can firms maximise these gains in practice? Pontvianne previewed CNIL's own survey of 3 500 French DPOs, which found that larger, data-driven and compliance-positive firms report the most value—from fine avoidance to smoother tender bids and stronger cybersecurity. He asked the panel to ground their answers in evidence rather than intuition.

Panellists' contributions

Gerard Buckley

Gerard Buckley offered the researcher practitioner synthesis. Interviewing C-suites across sectors, he found two headline effects: GDPR fines “focused the corporate mind,” boosting privacy awareness and halting indiscriminate data hoarding; and GDPR “shifted internal power,” giving DPOs and infosec teams bigger budgets and earlier involvement in product cycles. Secondary benefits — modernised infrastructure, trust signal value and faster international launches — materialised when DPOs were embedded at project inception rather than at the signoff stage. Buckley framed GDPR as a “personal fitness trainer: painful at first, but ultimately health promoting.”

Nadia Arnaboldi

Nadia Arnaboldi presented findings from a pan-European “DPOs for DPOs” survey (60 questions, more than 1 000 respondents). She reported chronic under-resourcing, role misunderstanding and psychological stress—yet clear upside when governance culture is supportive. A well-placed DPO prevents breaches, integrates privacy into CSR reporting and accelerates tender wins. Key success factors: clear boardroom reporting line, champion allies in commercial and IT units, and continuous upskilling (e.g., AI governance).

Thomas van Gremberghe

Thomas van Gremberghe spoke for SMEs and scale-ups. Short-term, a DPO looks like a sunk cost, long-term, it unlocks trust with clients, investors and regulators. Belgian law now requires DPOs for high-risk public-sector processing, and large private buyers increasingly demand proof of a DPO in B2B contracts. Court rulings—such as the Brussels Labour Court awarding dismissal protection to a hospital DPO—are elevating the role’s status. Van Gremberghe argued that pragmatic, business-savvy DPOs can shorten contract negotiations by providing a common language for privacy clauses.

Ricardo Catalan

Ricardo Catalan offered the DPA viewpoint. Impact = *management access + resources + skills*. Without C-suite proximity a DPO cannot exercise independence or monitoring powers. The Dutch AP (Autoriteit Persoonsgegevens) therefore encourages “DPO offices” rather than one person shows and calls for university level DPO degree programmes. Catalan cautioned that proposals to relax SME recordkeeping e.g., Record of Processing Activities (ROPA) thresholds, may weaken the profession and create two-tier data protection.

Discussion points from programme

What are the economic gains associated with a DPO ?

Direct risk-mitigation: CNIL's French survey shows firms with an embedded DPO log 28 % fewer reportable breaches and face materially lower fine trajectories (one case: a €150 k fine instead of a projected €400 k because the DPO had documented DPIAs). Reputational lift: Buckley reported B2C companies using a "GDPR-verified by DPO" trust badge that raised e-commerce conversion by 2-3 %. Revenue enablement: Arnaboldi noted that DPO sign-off is now a mandatory field in many EU public-tender portals, shaving weeks off procurement cycles. Operational efficiencies: Automated ROPA and retention-deletion programmes led by DPOs drove double-digit storage-cost savings for two Dutch hospitals. Capital access: SMEs said a robust DPO file expedited VC due diligence, adding "green-flag" value alongside ISO 27001.

Should a DPO be considered as an investment and an asset for a firm ?

Consensus: a long-term strategic investment akin to an internal auditor and a product-safety officer. Up-front cost (salary €75-130 k or external retainer €20-60 k) is offset by (i) avoided fines/breach costs, (ii) 5-10 % higher win-rates in data-sensitive tenders, and (iii) faster go-live of new digital services. When DPOs sit only in Legal, gains skew to risk containment; when they join product strategy boards they feed innovation—e.g., a fintech DPO co-designed anonymisation pipelines that enabled a data-monetisation spin-off valued at €15 m.

Which controllers can benefit from this?

High-volume data enterprises (finance, health, cloud SaaS) extract maximum ROI because breach/fine exposure is large and tender requirements frequent. Public-sector bodies in critical infrastructure also benefit: Belgian municipalities cited smoother eID roll-outs due to DPO-mediated vendor vetting. SMEs in trust-critical B2B niches (med-tech, HR SaaS) can punch above weight, yet they struggle with fixed salary costs—hence the rise of fractional or "cluster" DPO offices. Governance culture is pivotal: firms that treat the DPO as an "innovation partner" report broader gains, while box-tickers see little beyond compliance.

How to reap these benefits in practice ?

Embed at C-level: DPO in Executive Committee meetings correlated with faster breach containment (median 36 h vs 60 h). Multi-disciplinary offices: pairing legal, infosec and data-science secondees prevents "lone-ranger" fatigue and delivers richer DPIAs. KPI dashboards: speakers proposed tracking (a) breach volume and dwell time, (b) contract-cycle reduction, (c) Data Subject Access Request turnaround (DSAR), (d)

training coverage, and (e) infrastructure modernisation ROI. Link to ESG: mapping privacy metrics into sustainability reports attracts ESG-aligned investors. Future-proofing: up-skill on AI governance—DPOs who already manage AI-impact assessments become indispensable as the AI Act rolls in. Regulators can help by publishing model job descriptions, clarifying that DPOs supervise rather than execute compliance, and by spotlighting “good-practice” ROI case studies on their websites.

Summary of Q&A discussion

Question 1 SME DPO: How can I “sell” my value when I flag risks but can’t fix them?

Ricardo Catalan: He likened the role to a statutory auditor: “An auditor doesn’t close the books—he certifies them. A DPO’s currency is independence and assurance, not hands-on patching.” He recommended fortnightly risk dashboards to the CEO, mapping open issues, owners and due dates.

Nadia Arnaboldi: She advised converting activities into business metrics: “Log every DSAR, every breach you averted, every euro saved on a vendor renegotiation—boards speak KPI.” She cited an Italian utility where her annual DPO report helped secure a €3m cybersecurity budget uplift.

Question 2 EDPS: How can regulators nudge cross-agency cooperation despite confidentiality walls?

Ricardo Catalan: He proposed tiered sharing: anonymised patterns and procedural lessons can circulate freely; factual dossiers require dual-consent gateways. He floated a pilot ‘Digital Clearinghouse 2.0’ sandbox where DPAs, competition, and consumer authorities can co-review systemic cases under sealed protocols.

Question 3 DPO: Does raising the SME threshold for ROPA records risk downgrading the DPO role?

Ricardo Catalan: Officially neutral, but personally sceptical—lighter records will not spur innovation and may create two-tier protection.

Gerard Buckley: SMEs need simplification, but gaming the threshold is easy; customer expectations shouldn't depend on headcount.

Question 4 Academic attendee: Tying DPO duties to CSR/ESG metrics—opportunity or independence threat?

Aymeric Pontvianne: He welcomed the trend: “Privacy is the ‘P’ silently sitting inside the ‘S’ of ESG.” The key is a two-report model: a factual KPI annex for CSR teams and a confidential assurance letter to the audit committee, preserving candid oversight.

Question 5 Start-up privacy lead: What are first steps for a “one-person show” DPO?

Gerard Buckley: He outlined a “3-A sprint”: Audit data flows; Align with business KPIs; Announce quick wins—e.g., a retention-policy clean-up that frees server space.

Nadia Arnaboldi: Register with your DPA, conduct data mapping/ROPA, then build quick-win training sessions to gain visibility.



Navigating the Interface Between the AI Act and GDPR: Combining Innovation and Privacy in Europe, 22 May, Grande Halle

Recording

Rapporteur: Ine van Zeeland (imec-SMIT-VUB / Hasselt University)

Moderator: Leonardo Cervera Navas (EDPS)

Panellist 1: Markus Wünschelbaum (Hamburg's Data Protection Commissioner)

Panellist 2: Uljan Sharka (iGenius)

Panellist 3: Ignasi Belda (The Spanish Artificial Intelligence Supervisory Agency, AESIA)

Panellist 4: Marietje Schaake (Stanford Cyber Policy Center)

Discussion points from programme

Questions on the programme:

- *How will the experience with the GDPR help us effectively implement the AI Act?*
- *To what extent do the measures laid down in the AI Act serve to achieve and reinforce the parallel goals of the GDPR, such as fostering innovation and strengthening data protection?*
- *How are businesses ensuring compliance with both the GDPR and AI Act provisions?*

Panellists' contributions

Leonardo Cervera Navas (Moderator): How do we assess the current landscape in the field of AI?

Marietje Schaake: Even if AI policy and politics are a relatively new field, we have already seen important changes. Governments around the world have realised that this is a deeply impactful technology and we have seen a convergence on preventing harms and ensuring security. The US has signalled that it believes rules get in the way of innovation. This has had deep ripple effects around the world, because many impactful AI companies are based in the US. Fierce competition between these companies has led to incautious experimentation. We are at the early stages of seeing where generative AI will take us and how regulatory guardrails will work out in practice. We will soon see how that will play out. The AI Act introduces mitigating measures within a risk-based model, whereas there is no binding law in the US at the federal level, so we will be able to see in real time what the different effects will be.

Cervera Navas (Moderator): How do European companies struggle in this competitive environment?

Uljan Sharka: Look beyond the hype. There is a different world beyond the reality distortion; AI is actually an instrument to create new monopolies and wealth for some. This is not the age of information, the birth of the web. Comparing the current evolution with the evolution of the printing press, looking at the history of that can tell us about the future of AI. If you look at the generative AI model, the artefact is a word file which has 20 trillion words copy-pasted into it. How can that simplicity be autonomous? It is clearly being instrumentalised. This is not difficult to regulate.

We have a problem in terms of culture in Europe. Everyone wants to follow the US when it comes to investment and for that, you need to have the same capital and the same tools, but that won't work, because we have a different culture. We have leadership in other industries, but we don't have leadership in this industry. If we compare it with the printing press revolution, we will see that it is an intellectual property revolution. This is high stakes, so why is Europe not building it? It is a matter of capital, but not a matter of human capital - we have the talent.

If we don't regulate AI, everyone in Europe using AI is exporting their intellectual property to the US. With generative AI, putting data in an LLM is like putting sugar into a cake. In ten years' time, if everyone is using centralised models, those that own the models will have everyone's intellectual property. This is about human rights as well. If everyone is to own their intellectual property, they need to own their own AI.

Markus Wünschelbaum: Google DeepMind had an interesting project around the use of the Gemini AI model to run with coding done by a human, to evaluate and give feedback. The outcomes of the feedback loop of the AI system can be looked at by a developer. This made things more efficient, and it can be incredible. In fact, there was quite a lot of nonsense that came out of it, but because humans could have a look at it, we could sift out the valuable nuggets. If we use these systems lazily, to automate things without thinking about it, we get mediocre results.

There is an opportunity for data protection to guide innovation in this field in a meaningful direction. For instance, purpose specification can be a good support in that. It is not only about human oversight or humans in the loop, but it is also about human insights, because these machines hallucinate a lot.

Cervera Navas (Moderator): Which lessons can we learn from the implementation process of the GDPR?

Schaake: There are always lessons to be learned from legislation and it is not necessarily bad. The GDPR was hyped beyond reasonable heights. That was one lesson to be learned. Another lesson was that enforcement was lacking; it was not resourced sufficiently and there were not enough progressive notions regarding dealing with the biggest cases first. Some of the lessons from the GDPR have been helpful in the development of the AI Act because more attention has been paid to enforcement, also regarding hiring the best talent and better resources.

Another mistake made with the GDPR is that at a crucial moment of AI innovation, the EU was only thinking about protecting personal data, not about the opportunities of, for instance, large datasets to train AI models. That has been a difficult lesson learned.

How can regulators regulate AI? It is very personalised and crucial information, in the hands of companies. The AI Act was clearly designed on a risk-based model, focusing on liability, but questions around 'How is AI different?' have not been asked. Which different capabilities, new resources, and changes in the oversight process may we need?

Cervera Navas (Moderator): Which resources do we need, then?

Sharka: The hype is on many levels, for instance, on when AI is going to be used widely. As a society, we have been trying to cure something that is hardly even in use yet. We shouldn't think 2-3 years, it will not be pervasive for another 20 years. We think of it as a flying car, but it is currently a very useful electric car. We are regulating the fact that this technology has one feature: hallucination. Hallucination is not the problem.

What this means is that we have time. We are not out of the game. We need to take responsibility for that. We need more resources, but not a large amount of supercomputers in the next few months. Europe needs to be a third mover in the game, which means letting OpenAI pay the bills for R&D and letting Google leverage their advantage of scale, while Europe waits for the time to present a nice final product. We must have the fundamental rights protections and a clear strategy. We can take the money, as one of the biggest economies in the world, and use AI as a tool to transact. We can turn our largest companies into technology companies. We need to trust the fact that Europe can make it and needs to be strategic.

Ignasi Belda: There is an obligation for Member States in the AI Act: by August 2026, they have to implement a Regulatory Sandbox. The Spanish government is pioneering; we have already implemented such a sandbox. A lot of our companies are SMEs, and we are supporting them with the sandbox, to help them with the red tape. We are now starting with a pilot for the sandbox, from which we and the companies are learning. We are starting with 12 companies and hope to implement the final version of the sandbox at the end of this year, so half a year before the deadline. We are setting an example for other countries in Europe. We are explaining our experiences in working groups on this topic.

Cervera Navas (Moderator) :Markus Wünschelbaum, you have done research into governance structures in the EU, what are your findings?

Wünschelbaum: How do we actually regulate AI? In Germany, we have this notion that data protection is becoming annoying. The narrative, in a commission of prominent experts, was that data privacy, fire safety, and building preservation were holding back Germany. That sentiment extends to AI governance and regulation. In Germany, they are thinking about which kind of authority should regulate AI. I have looked at all the draft laws out there in the EU. By the beginning of August this year, we have to be ready, but there is no definitive law in Europe yet, except for Spain. None of them have officially appointed an AI authority. In some countries, like the Netherlands, they have designated the DPA as coordinating the AI authority. In other countries, Ireland and Nordic countries, they have designated other authorities as the AI supervisory authorities. Nations like Italy, Spain, and Poland have designated new, dedicated authorities.

Germany already has a lot of authorities, partly due to the federal system. This time, they chose one as a single authority. They have thought about excluding the DPAs altogether, because they hinder innovation. This is an interesting process, but what we have now is that we have a network of authorities that have never worked before.

There is going to have to be a shift in how we collaborate. We cannot always look only at data processing. It is going to become about products. People always say the AI Act is product regulation, but what does that mean exactly? You look at quality management and safety measures and end up with conformity assumptions. This is such a different approach from data protection, where we were rarely able to indicate an ideal target state. In product regulation, this is very different.

The cooperation will be different. ISO norms will state what compliance will be, by checking all the boxes. We have to look at technical details and define a target state and allow products onto the market that will not be perfect. The idea of what is necessary will change, and what is a legitimate interest under the GDPR will change. The free movement, the second goal of the GDPR, will become more prominent.

Summary of Q&A discussion

[Question raised by another Data Supervisory Authority representative in the room]: We are forgetting the free flow of data, and we are often focusing on data protection. The aim of the GDPR is not to introduce new roles or make people's lives difficult. In our new role, we cannot go around prohibiting everything. However, in the new role we also need new resources. These are new challenges for DPAs, but we all must understand where we must go in Europe, which is also the comfortable life. We need to be more transparent and open to each other.

Wünschelbaum: *It will be our job to explain these changes to the people. On the free movement of data, there is a great article in the EDPL making the point that the free flow of data cannot be really enforced.*

Cervera Navas: *Our role is not to protect. Even the name 'data protection', we should consider changing it, the GDPR is also about empowering. We have developed a tunnel vision focusing on human rights, and we should also be thinking about creating public value.*

Workshop Title: AI Act in Practice – Case- Based Analysis of AI Act Compliance Fictitious Case: CVision AI Scanner in Human Resources

Panel Rapporteurs: Adam Sereir & Sofia Llull, Rijksuniversiteit Groningen.

Date and Location: Thursday, May 22 — 16:00 - 17:15, Board Room

Facilitator(s): Peter Hense and Tea Mustać (Spirit Legal)

Workshop Attendees: 23 participants

Introduction

- **Workshop Objective:** The workshop centred on two structured debate-style discussions based on a fictional legal case involving the use of an AI CV scanner in Human Resources. Inspired by a real case handled by Spirit Legal (also serving as the host), the exercise offered practical insight into how legal professionals handle emerging EU legislation. The first discussion focused on interpreting the roles of “deployer” vs. “provider” under the AI Act (“Act”), while the second addressed the classification of the risks under the Act's provisions. Participants developed legal arguments, debated them, and reflected on which side made the stronger legal case.
- **Overview of Topics Covered:**
 - **Key Definitions under the AI Act:** Understanding roles such as “deployer,” “provider,” and other legal designations relevant to AI systems.
 - **Risk and Harm Categorisation:** Interpretation of how the AI CV scanner fits into the AI Act’s risk-based classification system and identifying potential legal harms.
 - **Governance Schemes:** Exploration of regulatory frameworks, compliance obligations, and internal governance for high-risk AI systems.
 - **Legal Interpretation of New Legislation:** Engagement with the structure and logic of (newly adopted or soon to be adopted) EU laws, including ambiguities and evolving standards.
 - Secondary topic covered — **Regulatory Challenges in HR Contexts:** Discussion of the intersection of AI, employment law, and fundamental rights (e.g. non-discrimination in hiring).

Key Workshop Activities

- **Activity 1:** First Round of Practice Case — **Is CVision the deployer or the provider? Debate between Groups 1 and 2.**
 - **Description:** The allocated spokesperson of each group presented their case, presenting the arguments that they discussed in the 15-minute preparation time. Each group spoke in two rounds — 5 minutes in the first round, and a second round of counterarguments of two minutes.
 - **Outcome:** Lively discussions, with no clear legal solution. The AI deployer must comply with the regulation and has a high burden of responsibility compared to the provider. Definitions are not clear, and this leads to regulatory gaps. The AI Act differs from the GDPR, and the focus is much broader than data protection. A crucial point concerned the contract — if this was concluded before the AI was developed, this may indicate provider status. IT procurement is different from AI system procurement.

- **Activity 2:** Second Round of Practice Case — **In what risk category can the AI Scanner be classified?**

Debate between Groups 3 and 4.

- **Description:** Similarly to Round 1, groups 3 and 4 presented their argument. Each group spoke in two rounds — 5 minutes in the first round, and a second round of counterarguments of two minutes.
- **Outcome:** Developing HR software comes with responsibility. High-risk systems are held to a very high standard of care. Registered high-risk, AI-compliant systems are rare, but might be useful for AI Act compliance. Product liability and data protection are also very systematic legal regimes.

Participant Contributions

- **Group Discussions:**

- **Round 1: Group 1 vs. Group 2 – Legal Qualification of CVision under the AI Act**

- Group 1 (CVision as a developer)
 - Argued that CVision functions as a developer of a foundational AI model, which is not independently placed on the market but is instead integrated and adapted by clients (providers). CVision constructs its system based on hiring criteria provided by companies, ensuring transparency and fairness through built-in safeguards. They relied on Article 3(2) of the AI Act to support their claim that legal responsibility lies with the provider—i.e., the entity that incorporates the system into their operations. CVision, in this view, simply offers a flexible, adjustable foundation and does not make the final, deployable product.
- Group 2 (CVision as a provider)
 - Took the opposing stance, asserting that CVision is not merely offering a foundational model but is actively designing and constructing a complete AI system for CV screening. The system is based on specific algorithms (e.g., decision trees) and is not substantially modified by clients. As such, CVision assumes the role of provider under the AI Act, bearing full legal responsibility for the system's development, marketing, and intended use. The argument emphasized that the lack of meaningful adaptation by clients makes CVision the true provider.

- **Round 2: Group 3 vs. Group 4 – Risk Classification under the AI Act**

- Group 3 (Not a High-Risk System)

- Argued that the AI CV scanner should not be classified as a high-risk system under the AI Act. The tool functions solely in a pre-screening capacity, processing only structured data without making any employment decisions. It serves as a support tool for human decision-makers and lacks any autonomous decision-making power. Since the final hiring decision remains with a human and the system neither employs nor excludes candidates directly, Group 3 contended that it falls outside the scope of Article 6 and related high-risk provisions.
 - Group 4 (Yes, a High-Risk System)
 - Contended that the system does qualify as high-risk under Article 6(2)(a) of the AI Act, which covers AI systems intended to be used for making decisions in employment, including recruitment and selection. Even if the tool assists rather than replaces human decision-makers, its role in shaping or filtering candidate pools can significantly affect individuals' employment opportunities. Group 4 emphasised the intended purpose and actual impact of the system—automating critical aspects of the recruitment process to improve efficiency—which places it within the high-risk category.
- **Individual Feedback:** While no individual feedback was formally provided by the host, the session was actively facilitated to ensure focused, high-level discussion. The host guided participants through the legal and regulatory complexities of the case, prompting critical reflection and encouraging rigorous argumentation. The conversations were intellectually engaging, with participants contributing thoughtfully from their diverse professional backgrounds.

Challenges or Issues

- **Challenges Encountered:**
 - Time management proved challenging, with Round 1 running longer than anticipated, which compressed time for the second discussion. This also meant that the entire workshop ran overtime.
- **Solutions Implemented:**
 - No structural adjustments were made during the session; however, participant engagement remained high despite the overtime.

Workshop Outcomes and Learnings

- **Key Takeaways:** The workshop highlighted the prevalence of regulatory gaps in the rapidly evolving field of technology law, particularly in the context of AI regulation. Participants gained insight into how legal practitioners must navigate these uncertainties with strategic reasoning. Rather than relying solely on

explicit legal provisions, lawyers often need to interpret and apply the law creatively and persuasively to construct robust legal arguments in novel scenarios.

- **Skills or Knowledge Gained:**
 - **Legal Negotiation and Argumentation:** Practicing structured legal reasoning through live debate, simulating adversarial legal settings.
 - **Case Reading and Analysis:** Rapidly understanding the facts and legal issues in a fictional case inspired by real litigation.
 - **Debate Preparation Under Time Constraints:** Preparing and defending arguments within limited time, reflecting real-world legal pressures.
 - **Legal Strategy in Practice:** Evaluating and choosing the most effective lines of argumentation when dealing with novel technologies and regulation.
 - **Collaborative Legal Problem-Solving:** Working in groups to identify legal issues, divide tasks, and present a coherent case.

Evaluation and Feedback

- **Feedback Summary:** N/A
- **Suggestions for Improvement:** Time management and more guidance from the hosts.

Conclusion

- **Summary of Overall Success:** The activity description claimed that the exercise is designed for professionals with prior knowledge of the AI Act, ML/AI technologies, and Data Quality Management. Although the intensive workshop focuses on solving complex, real-life challenges, it is accessible for anyone with some knowledge of AI, and enough time is given for participants to prepare by reading the AI Act. The objectives are met because the workshop efficiently equips participants with actionable insights and strategies for navigating the complexities of AI and the AI Act.
- **Future Recommendations:** A little more guidance on the correct legal reasoning would be appropriate to enhance learning during the workshop. Additionally, ensure that no contradictory information is provided between the hosts. Also, less time could be allocated for preparation to better manage overall time constraints.

Additional Notes (Optional)

- **Audience Engagement:** Participants were highly engaged throughout the workshop, bringing a mix of expertise from academia, policymaking, legal practice, and roles as Data Protection Officers (DPOs).

Their enthusiasm and willingness to contribute led to dynamic discussions and thoughtful debate, as well as insightful questions. The group demonstrated strong legal reasoning skills, actively challenged one another's arguments, and showed a deep understanding of both the AI Act and its broader implications. The atmosphere was lively, collaborative, and intellectually stimulating.

- **Media and Documentation:** The workshop was supported by a PowerPoint presentation that outlined key legal concepts, discussion structure, and guiding questions. Each of the four groups received printed copies of the case overview and tailored argument prompts, allowing them to prepare from distinct legal perspectives. These materials were essential in guiding group discussions and helping participants focus their arguments. While no photos or videos were formally taken or used during the session, the emphasis was on live interaction and oral debate. The use of printed handouts and visual aids on the slides contributed to a clear structure and helped maintain momentum throughout the session. Each group represented a different point of view in the case, creating a rich, multi-angled legal dialogue.