EVENT REPORT

eu-LISA Industry Roundtable

DATA MANAGEMENT



9-10 Sep 2026, Strasbourg, France

eu-LISA

ÉIRE2026.EU
IRELAND2026.EU

Data Management

eu-LISA Industry Roundtable

9-10 September 2026, Strasbourg, France



Contents

Executive summary 3

Day 1 7

Opening remarks 8

Session I: Setting the scene and sharing experience: Member States and Institutions 12
Insights from the Directorate-General for Migration and Home Affairs 12
Moving up the Data Maturity Staircase: From Silos to Sovereignty 13
Engineering Trust into Data: High-Assurance Data for Identity & Border Systems 14

Session II: Data governance and compliance by design 16
Data Governance Model 16
CRRS: Delivering Trusted, Auditable Data 17
Scalable Compliance by Design: Security Automation with Trusted Execution Environments 18

Session III: Secure and scalable data architectures for the public sector 20
The Foundation of Data Management: The eu-LISA Platform Journey 20
Securing Critical Communication Networks: Quantum Secure Communication for Europe 21
Federated Insights, Sovereign Data: A Zero-Trust Data Mesh for the Public Sector 22
Setting Data Free Securely: AI's Challenge 23
Bridging On-Premises Data with Microsoft Fabric and Purview 24

Day 2 27

Keynote presentation
Data Management at Scale: Lessons from the Schengen Information System 28

Session IV: Solutions for data sharing 30
The Role of Data Spaces in the European Data Union Strategy 30
Building the Interoperability Backbone for Sovereign European Data Spaces 31
Public Procurement Data Space 32
Sensitive Data Spaces and Trusted Data Transactions 33

Session V: Data exploitation, analytics and AI readiness 35
The Model Travels to the Data 35
Revolutionising Fisheries Control with AI-Driven Data Automation 36
Presentation: Dell Technologies 37
Unlocking Enterprise Data with Large Language Models & Model Context Protocol 38

Closing remarks 40



Executive summary

The 2026 edition of the eu-LISA Industry Roundtable, titled 'Data Management', brought together close to 400 participants across EU Member States, EU institutions and agencies, academia and industry. The event was held at the European Parliament in Strasbourg, France on 9 and 10 September, and organised in cooperation with the Irish Presidency of the Council of the European Union. During the event, discussions focused on data governance, interoperability, secure and scalable architectures, data sharing, analytics and artificial intelligence (AI), and how these capabilities can support trusted and effective digital services across the area of freedom, security and justice.

Key messages and strategic takeaways

Data as a strategic asset

Speakers highlighted the growing importance of data as a strategic capability supporting policymaking, operational effectiveness and public service delivery. Discussions reflected a broader shift from focusing primarily on the deployment and operation of systems towards making better use of the information they contain through analytics, reporting and evidence-based decision-making.

Trust and data quality as the foundation of digital transformation

Trust emerged as a recurring theme throughout the event. Participants stressed that secure, reliable and trustworthy digital services require strong governance frameworks, clear accountability, robust cybersecurity, and data protection both by design and by default. Data quality was repeatedly identified as a prerequisite for interoperability, analytics and AI. In that regard, speakers emphasised the importance of quality controls, data lineage, transparency and auditability throughout the data lifecycle.



Interoperability and data sharing for a connected Europe

As European IT systems become increasingly interconnected, organisations must strengthen cooperation across institutions, sectors and national borders. Common standards, shared governance frameworks, semantic interoperability and trusted data-sharing mechanisms such as the ones promoted through the EU data spaces initiative, were presented as key enablers of secure and controlled information exchange.

Sovereign, secure and scalable foundations

The Industry Roundtable highlighted the need for resilient and scalable infrastructures capable of supporting growing volumes of data and increasingly complex digital ecosystems. Shared platforms, cloud-native technologies, federated architectures, privacy-enhancing technologies and secure-by-design approaches were presented as key enablers of future digital services. At the same time, speakers stressed the importance of maintaining control over critical infrastructures, data platforms and strategic information assets.

Preparing the foundations for analytics and AI

Advanced analytics and AI offer significant opportunities to improve decision-making and operational effectiveness. However, speakers consistently underlined that successful adoption depends on high-quality, well-governed and trustworthy data. Human oversight, explainability, transparency, bias mitigation and compliance with European legal and regulatory frameworks were identified as essential requirements for the responsible use of AI in the public sector.

Call to action

As European institutions continue to expand their use of data, analytics and AI, this Industry Roundtable reinforced the importance of investing in data quality, governance, interoperability and secure digital infrastructures. Across the two days of discussions, one conclusion emerged clearly: data has become a critical asset for Europe's digital future. Realising its full value will require sustained efforts to strengthen trust, improve data quality, advance interoperability and preserve digital sovereignty, ensuring that Europe can better support evidence-based policymaking and harness data responsibly, effectively and at scale.

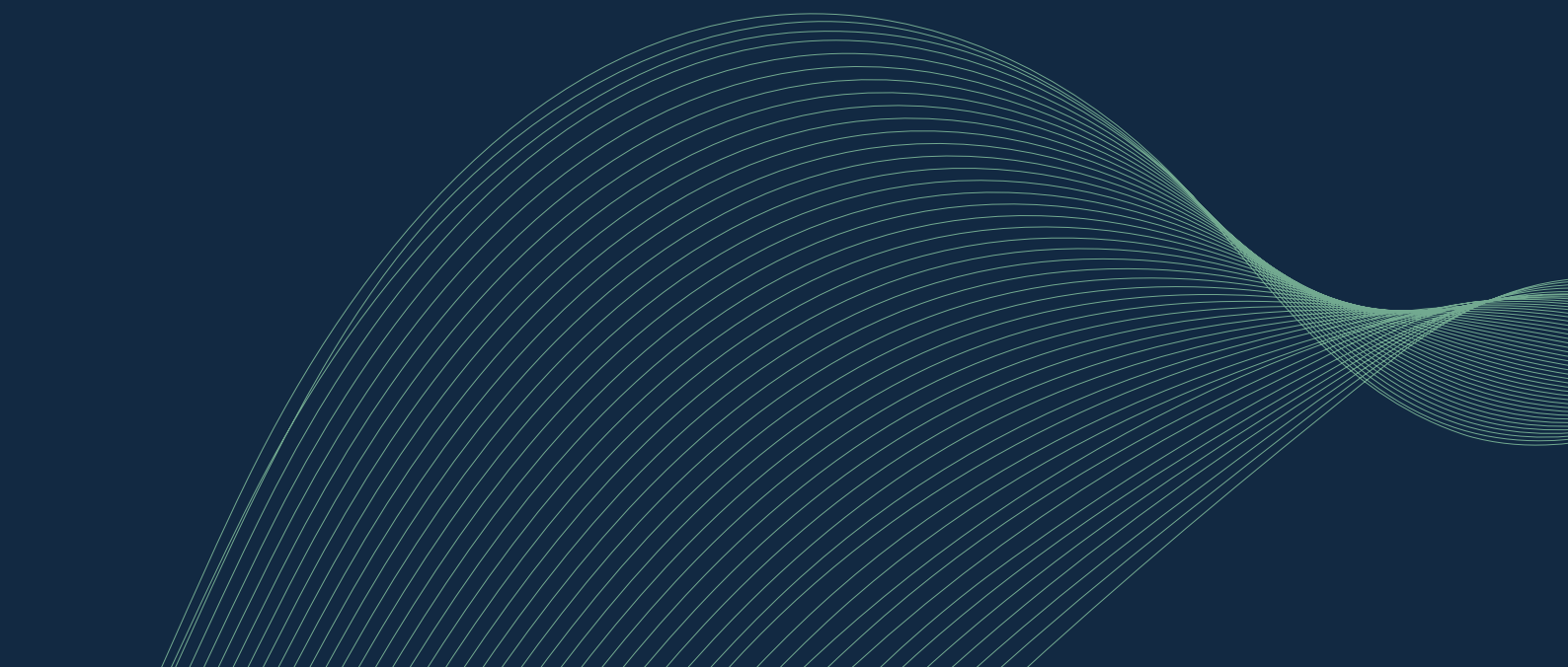
Day 1

Opening remarks

Session I | Setting the scene and sharing experience: Member States and Institutions

Session II | Data governance and compliance by design

Session III | Secure and scalable data architectures for the public sector



DAY 1

01

Opening remarks

Tillmann Keber



Tillmann Keber;
Executive Director;
eu-LISA

Tillmann Keber opened the 2026 edition of the Industry Roundtable by emphasising the strategic importance of data management across Europe as a foundation for effective digital governance. Framing the event around the opportunities and challenges of data management, Mr Keber invited the participants to discuss how technology can better serve European citizens through secure and interoperable digital services in the area of freedom, security and justice.

Key points from his address include the following.

Data as a strategic asset for Europe.

Mr Keber explained that data has become a strategic asset for public governance and policymaking. Drawing on the experience of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) with the European Union (EU) Entry/Exit System (EES), he noted the current demand from policymakers for reliable and good-quality data and statistics, and stressed that the agency's role goes beyond operating Europe's most critical large-scale IT systems, as eu-LISA is key to the effective use of data across the European justice and home affairs (JHA) landscape.

Addressing the growth and complexity of data.

His opening remarks drew attention to the significant increase in both the volume and the complexity of the data managed across Europe's digital ecosystem, which require highly resilient and scalable infrastructures. Data is also becoming increasingly interconnected, creating opportunities for more effective services while requiring robust governance, quality and reliability. Ensuring secure and trustworthy data architectures, he argued, is essential for maintaining confidence among citizens, EU Member States and institutional stakeholders.

Unlocking innovation through interoperability and emerging technologies.

He noted the importance of interoperability to enable cooperation across organisations, systems and national borders. The ability to exchange and use information effectively allows public authorities to deliver coordinated and efficient services. Looking ahead, Mr Keber pointed to the growing role of data analytics and artificial intelligence (AI), while stressing that technological innovation must be accompanied by transparency, accountability and solutions that are developed enough to operate at the European level.

> *Our approach to data management today will influence, as it already does, the capabilities of European digital services tomorrow.*

Louise Jevens



Louise Jevens;
Chief Information Officer;
Department of Justice, Home Affairs and Migration;
Ireland

Representing the Irish Presidency of the Council of the European Union, Louise Jevens emphasised the Presidency's motto, 'there is no strength without unity', in highlighting the importance of cooperation, effective data governance and digital innovation for a safer, more effective and more trusted EU.

Key points from her address include the following.

Data management as the foundation of digital transformation.

Ms Jevens emphasised that, as European public administrations are becoming increasingly digital, connected and data driven, effective data management is more important than ever. Beyond simply collecting information, organisations must ensure that data is secure, accessible, reliable and properly governed throughout its life cycle.

Drawing on Ireland's efforts to better connect information in the criminal justice system, she highlighted how improved data integration and quality can enhance operational effectiveness and policymaking. These initiatives demonstrate how well-managed and interconnected data can strengthen analytical capabilities, improve evidence-based decisions and ultimately lead to better outcomes for both public administrations and citizens.

A vision for Europe's digital future.

Looking ahead, Ms Jevens stressed that emerging technologies such as AI offer significant opportunities to improve public services and support decision-making. She reaffirmed the importance of strengthening the EU's digital infrastructure, partnership and shared responsibility, ensuring that digital progress strengthens public trust and remains aligned with European values when addressing common challenges in migration, security and cross-border collaboration.

> *Put simply, trustworthy outcomes require trustworthy data.*

Key insights and areas for action from the opening remarks

Data as a strategic asset for public administration.

Data management is no longer solely a technical function but a strategic capability that underpins policymaking, operational effectiveness and public service delivery. Public institutions must invest in data quality, governance and accessibility to support evidence-based decision-making and respond to increasingly complex policy challenges.

Trust and governance as foundations for digital transformation.

Secure, reliable and trustworthy digital systems require strong governance frameworks, compliance-by-design approaches, robust cybersecurity and clear accountability mechanisms. Building and maintaining trust among citizens, Member States and institutions must remain a core principle of all digital initiatives.

Interoperability and collaboration for a connected Europe.

The growing interconnectedness of European systems demands seamless information sharing across institutions, sectors and national borders. Strengthening interoperability, common standards and cross-border cooperation is essential for improving migration management, security, justice cooperation and the delivery of public services.

Preparing data foundations for AI and emerging technologies.

AI and advanced analytics can enhance decision-making and service delivery. However, these technologies depend on high-quality, well-governed and trustworthy data. Public administrations must strengthen data governance frameworks while ensuring transparency, ethical safeguards and respect for fundamental rights.

Partnership as the key enabler of Europe's digital future.

Europe's digital challenges and ambitions can be addressed only through close cooperation between Member States, EU institutions, agencies, academia and industry. Knowledge sharing, collective problem-solving and coordinated action are essential to building resilient, scalable and citizen-centred digital services that deliver lasting public value.

02

Session I

Setting the scene and sharing experience: Member States and Institutions

Marc Sulon



Marc Sulon;
Head of Interoperability and Digitalisation Unit;
Directorate-General for Migration and Home Affairs;
European Commission

Insights from the Directorate-General for Migration and Home Affairs

Marc Sulon opened the first session by reflecting on the significant progress made in Europe's large-scale IT ecosystem over the past decade. He emphasised how the systems have evolved into an increasingly interconnected digital architecture, creating new opportunities for cooperation, information sharing and operational support across migration, border management and internal security domains.

Key points from his address include the following.

Unlocking the value of data.

Mr Sulon stressed that the next challenge is to maximise the value of the information the systems contain. The focus is shifting from system deployment to the effective use of data, ensuring that information can support evidence-based policymaking, operational planning and strategic decision-making across the EU.

Interoperability as a catalyst for better and proactive decision-making.

The development of interoperable systems and linked data enables authorities to connect information across databases, improving identity management, fraud detection and access to critical information. Mr Sulon stressed the need to adopt more advanced analytical capabilities so that patterns, emerging risks and operational trends can be identified earlier.

New large-scale IT systems.

Mr Sulon spoke about the successful launch of the EES in October 2025 and the new European Asylum Dactyloscopy Database (Eurodac) in June 2026 (with the European Search Portal and the Common Identity Repository – both interoperability components), and he also gave an overview of future capabilities. He referenced the European Travel Information and Authorisation System (ETIAS), the Multiple-Identity Detector (interoperability component) and the Central Repository for Reporting and Statistics (CRRS).

Quality, governance and sovereignty are essential.

The growing use of interconnected data and AI requires strong governance, high-quality information and strict respect for legal and data protection requirements. Mr Sulon emphasised the importance of maintaining European control over sensitive data and critical infrastructures while working closely with industry organisations to develop secure and compliant solutions.

Peter Lindlacher



Peter Lindlacher;
Head of the Data and Analytics Services Division;
European Central Bank

Moving up the Data Maturity Staircase: From Silos to Sovereignty

Peter Lindlacher shared the European Central Bank's (ECB's) experience in transforming its data ecosystem to support analytics, policymaking and innovation. Making reference to the evolution of the ECB's data platforms, he demonstrated how strong governance, scalable infrastructures, AI readiness and digital sovereignty have become essential components of modern data management.

Key points from his address include the following.

Transforming fragmented data into a trusted foundation for decision-making.

Mr Lindlacher described how the ECB addressed a fragmented data landscape by creating centralised platforms that provide a common, governed environment for storing, accessing and analysing information. This transformation has improved consistency, reduced duplication and enabled users to focus on generating insights.

Scaling data and analytics capabilities for the future.

The migration to cloud-based platforms has significantly expanded analytical capacity, supporting thousands of users and accelerating data science initiatives. This, coupled with Apache Iceberg, enables more sophisticated analytics and increases the role of AI in supporting policy and supervisory activities. Mr Lindlacher highlighted the need for auditability and reproducibility that ensure data remains reliable and reusable.

Balancing innovation with digital sovereignty.

A major focus of the ECB's next phase is ensuring that critical European data and analytical capabilities remain under European control. With the new analytics and data platform, the ECB and national central banks are creating a shared ecosystem designed around sovereignty, collaboration and secure access to data.

Shared European data infrastructure as a strategic capability.

Mr Lindlacher stressed that the future of data management lies not only in technology but also in collective action. Building common platforms, shared standards and interoperable capabilities across European institutions will strengthen resilience, improve collaboration and support Europe's long-term strategic autonomy in the digital sector.

> *The broader question for every European institution is the same: which critical capabilities must remain under European control and what are we prepared to do together to secure them?*

Georgios Stavropoulos and Eleftheria Katsoura



Georgios Stavropoulos;
Research Associate;
Centre for Research & Technology;
Hellas Information Technologies Institute



Eleftheria Katsoura;
Research Associate,
Centre for Research & Technology;
Hellas Information Technologies Institute

Engineering Trust into Data: High-Assurance Data for Identity & Border Systems

Georgios Stavropoulos and Eleftheria Katsoura presented a data-centric perspective on digital systems, focusing on the complete data life cycle and the practical implementation of privacy-preserving technologies within the Horizon Europe Einstein project.

Key points from their address include the following.

Embedding trust, privacy and compliance throughout the data life cycle.

Mr Stavropoulos stressed that data management extends far beyond storage and access, covering the entire life cycle from data collection and processing to retention and deletion. Privacy, trust, security and regulatory compliance should be integrated into system design from the beginning, ensuring that every stage of data handling remains trustworthy and compliant.

Privacy-enhancing technologies enable secure innovation.

Privacy-enhancing technologies (federated learning, homomorphic encryption, biometric template protection, etc.) can strengthen security and trust without limiting functionality. These approaches allow organisations to share, analyse and use data while reducing the exposure of sensitive information and maintaining user control over personal data.

Human oversight and responsible AI in high-risk systems.

AI should support, not replace, human decision-making in identity and border management systems. The speakers noted the importance of transparency, explainability, bias testing, robustness assessments and continuous monitoring to ensure that AI remains aligned with fundamental rights and EU regulations such as the EU Artificial Intelligence Act.

The Einstein project as a testbed for secure and interoperable solutions.

Ms Katsoura demonstrated how these principles have been applied in the Einstein project, in which six interoperable applications were developed, supporting border management, document verification, biometric checks and digital identity management processes. The project shows the importance of balancing interoperability, security, privacy and operational effectiveness while preparing future solutions for Europe's evolving digital ecosystem.

> *Do not design these systems based on when a regulation will become applicable. Build the privacy, the trust, by design.*

Key insights and areas for action from session I

Moving from data collection to data exploitation.

The priority is shifting from building and connecting systems to extracting meaningful value and using data more effectively to support evidence-based policymaking and operational decision-making.

Data quality as the foundation of interoperability and trust.

The effectiveness and trustworthiness of interoperable systems, analytics platforms and AI solutions depend on the quality, consistency and reliability of the underlying data. Common standards, quality controls and strong validation processes are essential to ensure trustworthy outcomes.

Embedding governance, privacy, and compliance by design.

Data protection, security and regulatory compliance must be integrated throughout the entire data life cycle. Organisations should adopt privacy-by-design approaches, clear governance frameworks and robust oversight mechanisms to ensure that innovation remains aligned with legal requirements and fundamental rights.

Building trusted foundations for artificial intelligence.

AI, machine learning and predictive analytics offer significant opportunities to improve operational effectiveness and support more proactive decision-making. However, successful adoption requires well-governed, high-quality data, explainable and auditable models, human oversight, and safeguards against bias and misuse.

Balancing innovation, sovereignty and collaboration.

Europe's ability to leverage its growing data assets depends on maintaining control over critical infrastructures, data platforms and analytical capabilities while fostering collaboration between Member States, EU institutions, agencies, academia and industry.

03

Session II

Data governance and compliance by design

Theofanis Syrigos



Theofanis Syrigos; Head of Programme and Solutions Management Unit; eu-LISA

Data Governance Model

Theofanis Syrigos presented the governance framework underpinning eu-LISA's large-scale IT systems, highlighting the legal, organisational and operational mechanisms that ensure data is managed securely, consistently and in accordance with EU legislation.

Key points from his address include the following.

Data governance is driven by legal mandate and shared oversight.

Mr Syrigos emphasised that eu-LISA's systems are developed, operated and managed strictly within a legislative framework defined by the EU co-legislators (the Council and the Parliament), and the governance structure ensures they remain aligned with policy objectives, regulatory requirements and operational needs.

Data protection by design and by default.

A core message was that data protection is embedded into every stage of system design and operation. System-specific regulations define what data can be processed, who can access it, retention periods, security requirements, and the purposes for which information can be used.

Clear separation between data controllers and data processor.

Mr Syrigos highlighted the governance distinction: Member States act as data controllers, as they are responsible for the data they enter into EU JHA systems and for decisions based on that information. eu-LISA, by contrast, acts as the data processor, managing the underlying technical infrastructure while ensuring compliance with the legal and operational requirements.

The CRRS as a strategic tool for policy and operational insights.

Introducing the CRRS, Mr Syrigos explained the purpose of the system, namely how anonymised data from multiple EU JHA systems can be aggregated to generate statistics, analytical reports and cross-system insights.

> *Data protection and security measures are not just an add-on feature.*

Bart Dekempe



Bart Dekempe;
Associate Partner;
IBM

CRRS: Delivering Trusted, Auditable Data

Bart Dekempe provided an in-depth overview of the CRRS, focusing on the data governance capabilities that enable information to be trusted, of high quality and actionable. He highlighted how data governance, quality, lineage and sovereignty are essential for transforming raw data into reliable insights that can support decision-making across the EU JHA sector.

Key points from his address include the following.

Transforming raw data into trusted information.

Mr Dekempe explained that the CRRS is designed to convert data originating from multiple EU JHA systems into a reliable source of information for end users. The platform transforms raw operational data into high-quality datasets that can be confidently used by policymakers, analysts and operational practitioners.

Data governance creates confidence in decision-making.

Effective governance ensures a 'single version of the truth'. Through metadata management, intelligent cataloguing, access controls and policy enforcement, the CRRS helps users understand the meaning, ownership and quality of the data they are using.

Data quality and lineage ensure transparency and accountability.

Mr Dekempe highlighted the importance of automated data quality controls and end-to-end data lineage. The CRRS enables information to be traced back to its original source, every transformation applied to it to be understood and its quality to be assessed throughout the process, which strengthens trust in reports and other analytical outputs while supporting transparency, auditability and compliance.

Sovereignty and open standards by design.

A recurring theme was the importance of maintaining full control over European data. The CRRS has been designed as an on-premises solution running within eu-LISA's infrastructure and built on open-source technologies and open data standards. This approach guarantees that data remains under the control of eu-LISA and its stakeholders.

Nicolae Paladi



Nicolae Paladi;
Chief Executive Officer;
Canary Bit

Scalable Compliance by Design: Security Automation with Trusted Execution Environments

Nicolae Paladi explored the growing importance of privacy-enhancing technologies in protecting sensitive data throughout its entire life cycle. Using the analogy of Hans Christian Andersen's 'The Emperor's new clothes', he argued that, while organisations have become proficient at protecting data at rest and in transit, the protection of data while it is being processed remains one of the most significant challenges in modern digital services.

Key points from his address include the following.

Protection of data in use remains a critical gap.

Mr Paladi highlighted that, while encryption and cybersecurity measures have become standard for data protection, data often remains exposed during processing. Achieving true end-to-end privacy necessitates addressing this gap with technologies designed to secure information while it is actively being used.

Confidential computing enables verifiable trust.

A central theme was the use of confidential computing and trusted execution environments, which create isolated processing environments that prevent infrastructure operators, cloud providers and other processes from accessing sensitive data.

Privacy and compliance can be translated into technical controls.

Mr Paladi emphasised that trust should be based on verifiable evidence. Remote attestation means that compliance requirements and security policies can be encoded into technical controls, allowing organisations to automatically verify whether infrastructure meets specific legal, security and operational requirements before sensitive data is processed.

Privacy-enhancing technologies support General Data Protection Regulation (GDPR) compliance and data sovereignty.

Drawing on a project carried out with the support of the Swedish Authority for Privacy Protection, Volvo Group and Ericsson, and using a regulatory sandbox, Mr Paladi demonstrated how confidential computing can support GDPR principles such as data protection by design and using appropriate technical safeguards.

> *There is an old proverb: trust but verify. We turned it around; verify, then trust.*

Key insights and areas for action from session II

Governance must be embedded across the entire data life cycle.

Effective data management requires clear governance structures that define roles, responsibilities, ownership, access rights and accountability throughout the data life cycle, ensuring that data is managed consistently across interconnected systems while remaining aligned with legal mandates, operational requirements and policy objectives.

Data protection and privacy must be built into system design.

Data protection cannot be treated as an additional layer applied after implementation. Privacy-by-design and data-protection-by-default principles must guide the architecture, operation and evolution of digital systems from the outset. As data sharing and interoperability increase, organisations must continue to strengthen safeguards through privacy-enhancing technologies, trusted execution environments, open standards and sovereign infrastructures.

Trusted data requires strong quality, lineage and transparency mechanisms.

Reliable reporting, analytics and policymaking depend on high-quality data that can be traced back to its source and verified throughout its life cycle. Automated data quality controls, metadata management, data lineage and auditability are critical capabilities for ensuring confidence in data-driven decisions and creating a single, trusted source of information.

Unlocking the value of data through secure analytics and reporting.

Platforms such as the CRRS demonstrate the potential of aggregating information across systems to generate insights that cannot be obtained from individual datasets alone. Advanced reporting and analytics capabilities can enhance operational monitoring, support evidence-based policymaking, identify cross-system trends and enable more informed strategic decisions across the JHA sector.

04

Session III

Secure and scalable data architectures for the public sector

Joris Vankeerberghen



Joris Vankeerberghen; Head of the Smart Hosting Platform Services Sector; eu-LISA

The Foundation of Data Management: The eu-LISA Platform Journey

Joris Vankeerberghen presented eu-LISA's approach to modernising the infrastructure foundation that supports EU large-scale IT systems and developing that infrastructure into shared, scalable and secure hosting platforms designed to accelerate delivery, support interoperability and provide resilient foundations for future digital services.

Key points from his address include the following.

From fragmented infrastructure to shared platforms.

Mr Vankeerberghen highlighted how early EU JHA IT systems were deployed on isolated infrastructures, which created operational complexity, slowed innovation and made scaling difficult. To address these challenges, eu-LISA developed its smart hosting platform model, providing a common infrastructure capable of supporting multiple systems while maintaining the necessary separation and security controls.

Building secure, cloud-native foundations.

By consolidating core services through a hybrid multi-cloud set-up, introducing computing, storage, networking, observability, backup and recovery into shared platforms, eu-LISA can deploy new capabilities efficiently and ensure that security, resilience and regulatory requirements are met.

Transforming the operating model through collaboration.

eu-LISA has shifted towards closer collaboration within the agency by adopting Agile methodologies as well as development and security operations practices (DevSecOps), which help reduce delays, improve knowledge retention and ensure security and compliance through the development life cycle.

Preparing the platform for sovereign cloud and AI capabilities.

Looking ahead, eu-LISA is extending its platform strategy to include sovereign cloud services, advanced cost management practices, multi-institutional hosting opportunities and AI capabilities. These developments aim to strengthen digital sovereignty, improve operational efficiency and provide a secure foundation while maintaining compliance and governance standards.

> *What is data management without the infrastructure and the services on which it is hosted?*

Ingrid Romjin



Ingrid Romjin;
Chief Executive Officer and Founder;
Falqon Systems

Securing Critical Communication Networks: Quantum Secure Communication for Europe

Ingrid Romjin explored how quantum-secured communication networks can help protect critical infrastructure and sensitive data against future cyber threats. She highlighted the growing urgency of preparing for the arrival of cryptographic quantum computers and demonstrated how quantum key distribution and quantum networking technologies can be deployed today to strengthen the long-term security of European communication networks.

Key points from her address include the following.

Quantum computing creates a new cybersecurity challenge.

Ms Romijn explained that, while quantum computing has the potential to deliver significant scientific and technological advances, it poses a major challenge to today's encryption methods. Quantum computers are expected to break many of the cryptographic algorithms currently used to protect digital communications, making preparation a priority today.

Quantum-secured communications provide long-term protection.

Using quantum key distribution, organisations can establish highly secure communication networks. Using quantum entanglement and physics, organisations can establish cryptographic keys with strong protection against eavesdropping and future quantum-enabled attacks.

Defence-in-depth through quantum and post-quantum security.

Ms Romijn stressed that quantum security should complement existing cybersecurity measures. Quantum networking technologies can be combined with post-quantum cryptography and traditional encryption approaches to create layered protection.

Real-world deployments demonstrate technology readiness.

She showcased several operational deployments, including projects in the Port of Rotterdam and a cross-border quantum network connecting Belgium and Luxembourg. These demonstrate that quantum-secured communication is no longer a purely experimental concept but an emerging operational capability.

> *"The time to start looking into quantum secure networks is really now.*

Jonny McCandless



Jonny McCandless;
Senior Solutions Architect;
Elastic

Federated Insights, Sovereign Data: A Zero-Trust Data Mesh for the Public Sector

Jonny McCandless explored how data mesh architectures can help public sector organisations overcome growing challenges related to data fragmentation, scalability, security and AI adoption. He argued that organisations should adopt distributed models that allow data to remain under the control of its owners while still being accessible for analytics, collaboration and decision-making.

Key points from his address include the following.

Moving beyond data silos with a data mesh approach.

Mr McCandless explained that organisations increasingly struggle with data spread across multiple systems, formats, locations and tools. Data mesh approaches offer an alternative by allowing data to remain where it is created while making it accessible through a common layer of services and search capabilities.

Embedding zero-trust security into data sharing.

A key message was that data sharing should not necessitate relinquishing control. By implementing security at the source of the data, organisations can define precisely what information is accessible, to whom and under what conditions.

Real-time access enables better decisions.

Rather than relying on periodic data transfers and central repositories, data mesh models enable near-real-time access to information. This reduces delays, improves situational awareness and allows organisations to make more informed decisions based on the most current data available across multiple systems and domains.

Strong data foundations are essential for responsible AI.

Mr McCandless highlighted the role of AI as a force multiplier for organisations managing large volumes of information. However, successful AI adoption depends on trusted, high-quality and up-to-date data. Distributed data architectures combined with responsible AI governance, auditability and access controls can support sovereign AI solutions tailored to the public sector.

> *We aim to empower Europe's data mission.*

Derrick Struys



Derrick Struys;
Director of Data Services and Storage;
Hewlett Packard Enterprise

Setting Data Free Securely: AI's Challenge

Derrick Struys presented Hewlett Packard Enterprise's (HPE) vision for enabling secure, large-scale data management and AI readiness through data fabric technologies. Drawing on examples from financial services, telecommunications, biometrics, autonomous vehicles and public-sector data environments, he demonstrated how organisations can reduce data silos, improve access to information, and accelerate analytics and AI-driven innovation while maintaining governance and control.

Key points from his address include the following.

Connecting distributed data through a unified data fabric.

Mr Struys highlighted how HPE's data fabric approach seeks to create a global data namespace that connects multiple systems and repositories without requiring multiple copies. This enables organisations to work with data as a single resource while maintaining visibility, governance and control.

Reducing data duplication and accelerating innovation.

Mr Struys explained that data fabrics enable organisations to work directly with live datasets, creating logical rather than physical copies of information. This reduces storage requirements, improves consistency and dramatically shortens the time required to deploy analytics and AI workloads.

Supporting large-scale analytics and operational insights.

Data fabric architectures support real-time access to massive datasets and distributed infrastructures, enabling use cases ranging from fraud detection to biometric identity management, by providing high-performance access to massive datasets and enabling real-time queries across distributed infrastructures.

Governance, automation and self-service capabilities.

Beyond data access itself, Mr Struys emphasised the importance of governance, policy management, auditing and automation. Integrating data fabric technologies with cloud management platforms allows organisations to automate deployment, simplify operations, provide self-service access to resources and maintain governance over multi-cloud environments.

> *You need as much data as possible from your own environments to get even better results out of your machine learning systems or your AI.*



Guust Franssens (left);
Solution Engineer;
Microsoft

Florian Boigner (right);
Cloud Solution Architect;
Microsoft

Guust Franssens and Florian Boigner

Bridging On-Premises Data with Microsoft Fabric and Purview

Guust Franssens and Florian Boigner presented Microsoft's approach to balancing data sovereignty with the need for scalable analytics and AI capabilities. Using Microsoft Fabric as an example, they demonstrated how data can remain within trusted environments while still benefiting from advanced analytics, reporting and AI services.

Key points from their address include the following.

Enabling cloud analytics without moving sensitive data.

The speakers stressed that, by using a governed data access pattern, organisations can keep data within trusted on-premises or sovereign environments while creating secure references to that data from cloud-based analytics platforms.

Data sovereignty requires more than data residency.

A key message was that sovereignty extends beyond where data is stored. Organisations should adopt layered governance models that ensure control is maintained across all stages of data access and processing.

Governance must extend beyond the source data.

Even when source data remains under organisational control, analytical processes generate additional assets such as cached data, transformed datasets, dashboards, reports and AI outputs, and access controls, data protection measures and compliance obligations continue to apply.

Information protection enables secure collaboration and AI use.

Through data classification, sensitivity labels, customer-managed encryption keys and end-to-end governance controls, organisations can securely share, analyse and leverage data for analytics and AI while maintaining compliance and control.

> *Instead of moving data, we can point to data.*



Key insights and areas for action from session III

Modern digital services require shared, scalable and sovereign infrastructures.

As digital ecosystems become more interconnected, organisations must move beyond fragmented and system-specific infrastructures towards shared, cloud-native and scalable platforms. Future architectures should balance flexibility and innovation with security, compliance, operational resilience and digital sovereignty.

Data should be accessible without unnecessary movement.

There is a clear need to reduce large-scale data duplication and migration while still enabling analytics, reporting and collaboration. Approaches such as data meshes, data fabrics, governed access and federated architectures allow organisations to access, analyse and share information while maintaining ownership, control and governance where the data originates.

Security and trust must be embedded across infrastructure, data and communications.

Zero-trust principles, privacy-preserving controls, information protection mechanisms and secure-by-design infrastructure must be integrated throughout the entire technology stack. Organisations should prepare for emerging threats, including quantum-related risks, by investing in cryptographic protections and resilient communication architectures.

High-quality, well-governed data is the foundation for analytics and AI.

Advanced analytics, business intelligence and AI depend on secure access to trusted and well-governed data. Organisations should invest in common governance frameworks, metadata management, access controls and scalable data platforms that enable users to derive insights while maintaining transparency, accountability and compliance.

Digital sovereignty must enable rather than limit innovation.

The challenge for European organisations is to leverage cloud, analytics, AI and emerging technologies while retaining strategic control over critical data, infrastructures and decision-making processes. Achieving this balance will necessitate continued collaboration between public institutions and technology vendors to develop interoperable, secure and future-ready digital ecosystems.

CLOSING OF DAY 1

Day 2

Keynote presentation

Session IV | Solutions for data sharing

Session V | Data exploitation, analytics and AI readiness

Close of the event

DAY 2

05

Keynote presentation

Matthias Leese



Matthias Leese;
Assistant Professor;
Swiss Federal Institute of Technology Zurich

Data Management at Scale: Lessons from the Schengen Information System

Matthias Leese presented findings from a five-year research project on data quality in European law enforcement and border management systems, focusing on the Schengen Information System (SIS). His presentation examined the practical challenges of managing data at scale and highlighted the organisational, technical and human factors required to ensure that information remains meaningful, reliable and usable across European security networks.

Key points from his address include the following.

Preserving meaning across systems.

Effective data management is not only about storing accurate records but also ensuring that information retains its meaning when shared across different legal, organisational and operational environments. Choices made during data entry can significantly influence how records are interpreted and used elsewhere.

Human expertise remains essential.

Although automated validation and quality-control mechanisms are critical, human judgement remains indispensable. Experts are needed to investigate anomalies, interpret context and resolve issues that technical rules alone cannot address.

Practical interoperability beyond data exchange.

Successful information sharing requires more than technical connectivity. Data must remain understandable and actionable when transferred between jurisdictions, making standards, support structures and cross-border cooperation vital components of large-scale systems.

AI readiness depends on context.

Mr Leese argued that AI-ready data require more than completeness and standardisation. Understanding data provenance, organisational practices and contextual factors is essential to ensure that AI applications can use information safely and effectively.

> *Good data management at scale means to preserve the meaning and also the usability of data as they move across technical, organisational, legal and operational contexts.*

06

Session IV

Solutions for data sharing

Coen Janssen and Gianfranco Cecconi



Coen Janssen;
Policy Officer;
Directorate-General for Communications Networks, Content and Technology;
European Commission



Gianfranco Cecconi;
Data Ecosystems and Sovereign Data Lead;
Capgemini

The Role of Data Spaces in the European Data Union Strategy

Coen Janssen and Gianfranco Cecconi showcased the strategic and practical development of European data spaces. Their joint presentation highlighted how trusted data-sharing frameworks, common standards and interoperability can support Europe's data economy, AI ambitions and digital sovereignty.

Key points from their address include the following.

From data policy to economic value.

Mr Janssen outlined the EU data union strategy, which seeks to increase access to high-quality data, simplify data-sharing rules and strengthen digital sovereignty. Data spaces were presented as a key mechanism for translating policy objectives into innovation, economic opportunities and AI-enabled services.

Data spaces as trusted sharing ecosystems.

Data spaces were described as federated environments that enable organisations to exchange data while maintaining control over access and usage. Effective data sharing depends not only on technology, but also on governance, trust frameworks and clear agreements between participants.

Formalising data-space standards.

European standardisation efforts are translating existing data-space specifications into formal standards, including trusted data transactions, data catalogues, semantic assets, governance frameworks and maturity models. Future work will address data quality metrics and data value chains.

Building foundational infrastructure.

Mr Cecconi compared data spaces to enabling infrastructure such as roads and power networks. The focus is on building the standards, software, best practices and governance foundations that allow organisations to develop new services and data-sharing solutions.

> *We don't build the road to admire the road. We build the road because we want something at the end, we want a service that is enabled by that.*

Darío García Coder



Darío García Coder;
Lead Architect and Technical Director;
Sopra Steria

Building the Interoperability Backbone for Sovereign European Data Spaces

Darío García Coder presented Simpl-Open, a middleware solution developed within the European Commission-funded Simpl programme. His presentation focused on how the platform supports the implementation of common European data spaces by providing a set of technical components and services for secure, interoperable and sovereign data sharing across sectors.

Key points from his address include the following.

A middleware for implementing data spaces.

Mr García Coder described Simpl-Open as a middleware designed to connect organisational infrastructures and enable data exchange within common European data spaces. It implements reference architectures and best practices developed through European data space initiatives.

Security, trust and data sovereignty.

A central objective of Simpl-Open is to establish trusted data sharing. The platform supports participant onboarding, identity management and secure point-to-point interactions, while allowing providers to define access policies, usage conditions and contractual terms.

Interoperability through configurable services.

Simpl-Open provides configurable processes that can be adapted to different sectoral requirements, while supporting organisational, semantic, technical and legal interoperability.

From proof of concept to operational deployment.

The Simpl programme is progressing from feasibility studies to proof-of-concept implementations across multiple common European data spaces. Mr García Coder also outlined the ongoing work to extend Simpl-Open through integration with the European High-performance Computing Joint Undertaking, infrastructure-sharing initiatives and mechanisms to support the long-term sustainability of data spaces.

> *"The goal is to provide the maximum control to the provider on how their data is used and consumed.*

Marc Christopher Schmidt and Daniel Arosa



Marc Christopher Schmidt;
Policymaker and Team Leader
eProcurement;
Directorate-General for
Internal Market, Industry,
Entrepreneurship and SMEs;
European Commission



Daniel Arosa;
Executive Manager;
NTT Data

Public Procurement Data Space (PPDS)

Marc Christopher Schmidt and Daniel Arosa talked about the Public Procurement Data Space (PPDS), an initiative designed to unlock the value of Europe's public procurement data through semantic interoperability and shared data infrastructure. Their presentation demonstrated how the PPDS addresses challenges in data quality, interoperability and analytics to improve transparency, policymaking and cross-border access to procurement information.

Key points from their address include the following.

Unlocking fragmented procurement data.

The public procurement market represents EUR 2.5 trillion annually, yet only around 20 % of procurement data is available through EU-level platforms. The PPDS addresses this gap by connecting Member State data sources and incorporating procurement data both above and below EU reporting thresholds.

Expanding visibility beyond EU reporting thresholds.

The PPDS aims to complement data from the EU platform Tenders Electronic Daily by incorporating procurement data below EU reporting thresholds, providing a more complete view of public procurement activity and supporting better analysis and policymaking.

Semantic interoperability through a common ontology.

A central feature of the PPDS is its use of the e-procurement ontology to harmonise procurement information from different national systems. Data is transformed into a common semantic model and stored in a searchable knowledge graph.

Building advanced analytics capabilities.

Beyond data integration, the PPDS provides dashboards, data catalogues, query services and graph exploration tools. Future development will focus on enhanced analytics, AI integration, data enrichment and interoperability with other European data spaces through Simpl components.

> *Europe is rich in public procurement data, but we cannot really use it to our advantage.*

Frédéric Bellaiche



Frédéric Bellaiche;
Vice President of Technology and Research;
Dawex

Sensitive Data Spaces and Trusted Data Transactions

Frédéric Bellaiche examined the role of trusted data transactions and standards in enabling secure data sharing within sensitive environments. His presentation focused on the emerging European standardisation framework for data spaces and demonstrated how common trust, security and interoperability mechanisms can support data exchange in highly regulated sectors such as defence, health, aerospace and nuclear energy.

Key points from his address include the following.

Trusted data transactions as a regulatory foundation.

Mr Bellaiche highlighted the development of the Trusted Data Transaction standard, which defines the phases, roles and mechanisms required to establish trust in data exchanges. As a harmonised European standard linked to the Data Act, it can be audited, referenced in public tenders and used to support a presumption of conformity with regulatory requirements.

Trust throughout the data life cycle.

Trustworthiness must be ensured at every stage of a transaction, from rights publication and discovery to negotiation and data exchange. The standard introduces requirements for verified identities, trusted data product descriptions, usage contracts, access controls, traceability and secure transfer.

A common model for sensitive data spaces.

Although sectors such as defence, health, aerospace and nuclear energy have unique operational contexts, they share similar requirements. Common standards can provide a shared foundation across these sectors.

Security, sovereignty and interoperability.

Sensitive data spaces require additional safeguards. Trusted data transaction standards provide a common framework for sharing data while maintaining control over its use, access conditions and security requirements.

> *The trust layer is now standard. It's not a design choice that you have to make.*



Key insights and areas for action from session IV

Treat data spaces as strategic infrastructure.

Trusted data sharing requires long-term investment in standards, governance, interoperability and common technical foundations.

Standardise trust across organisational boundaries.

Trusted data transactions, common governance frameworks and shared rules are essential for enabling secure and scalable cross-border data sharing.

Maintain sovereignty while enabling data exchange.

Organisations must retain control over how data is accessed, used and shared, particularly in sensitive or regulated environments.

Make interoperability semantic as well as technical.

Common ontologies, shared vocabularies and agreed data models are critical to ensuring that data can be understood and reused across organisations and Member States.

Focus on outcomes, not data movement.

The objective of data sharing is to support better analytics, AI applications, policymaking and public services, rather than to exchange data for its own sake.

07

Session V

Data exploitation, analytics and AI readiness

Domenico Borla



Domenico Borla;
Head of AI Strategy and Governance;
Capgemini

The Model Travels to the Data

Domenico Borla discussed how public sector organisations can become AI ready when working with sensitive, distributed data that cannot be freely combined. He proposed an architecture that bridges data governance and AI governance by linking models and compliance checks to the data, rather than moving data to centralised AI systems.

Key points from his address include the following.

Bridging the gap between data governance and AI governance.

A key challenge public sector organisations face in adopting AI is the need to balance data sovereignty and security with the requirements for trustworthy and effective AI. Mr Borla proposed an approach in which data remains under the control of the data owner while AI models and validation checks are executed locally.

Federated analytics as an alternative to data centralisation.

The proposed architecture is based on the principle that raw data should not move. Models are trained where the data resides and only learned parameters or aggregated results are shared centrally.

Embedding AI readiness and trust into the process.

The model incorporates data-quality checks, bias assessments and explainability mechanisms at the local level. Data controllers evaluate the data quality and fairness of their own populations, while only summary information is shared.

A practical pathway for AI adoption.

Mr Borla proposed a phased approach, beginning with legal and compliance assessments, followed by pilot phases using synthetic data and later real-world testing with volunteer Member States. The objective is to demonstrate that AI-enabled analysis can be achieved without moving sensitive data and, at least during the pilot phase, without requiring a new legal basis.

> *We don't bring the data to the model. We bring the model to the data.*

Jose Rui Teixeira Nunes



Jose Rui Teixeira Nunes;
Solutions Architect;
Amazon Web Services

Revolutionising Fisheries Control with AI-Driven Data Automation

Jose Rui Teixeira Nunes presented on how the European Fisheries Control Agency (EFCA) transformed fisheries oversight through a modern data platform and AI-powered analytics. Using EFCA's Bluefin Tuna Data Platform and the interrogation requirements information system as examples, he demonstrated how AI can automate data processing, improve operational intelligence and enable data-driven decision-making within a resource-constrained EU agency.

Key points from his address include the following.

From manual processing to AI-powered ingestion.

EFCA previously relied on the manual processing of thousands of documents received in different formats, languages and alphabets. The Bluefin Tuna Data Platform introduced automated data ingestion using optical character recognition and large language models.

Accessible insights through self-service analytics.

The interrogation requirements information system platform enables inspectors and operational staff to generate visualisations and reports using natural language, without requiring specialist business intelligence expertise.

Building a collaborative data ecosystem.

The modern data architecture supports the integration of multiple data sources, including fisheries records, new onboard camera systems and satellite imagery. It also facilitates data sharing and collaboration with organisations such as the European Maritime Safety Agency, the European Border and Coast Guard Agency and Member State authorities.

AI delivers operational value when embedded into workflows.

Automated data extraction and near-real-time analytics helped EFCA reduce manual effort and improve situational awareness by identifying inconsistencies, data gaps and potential errors.

> *The end users are not business intelligence experts. They can take insights from the data just by expressing what they need.*

Christian Spindeldreher



Christian Spindeldreher;
Data and Artificial Intelligence Strategist;
Dell Technologies

Presentation: Dell Technologies

Christian Spindeldreher shared lessons learned from Dell's internal AI transformation and the development of its AI-ready data architecture. He described the critical role of data management, governance and security in enabling trustworthy AI, demonstrating how data platforms, semantic technologies and governance frameworks underpin effective AI.

Key points from his address include the following.

Data readiness as the foundation for AI.

Mr Spindeldreher emphasised that technical AI capabilities alone are insufficient unless fragmented data sources, data quality issues and governance requirements are addressed.

Combining data fabric, data mesh and data products.

Following the integration between Dell and EMC, Dell introduced a new data architecture to connect information stored across multiple systems and business units. Data products provide a single access point for users, making information easier to find and share while ensuring appropriate governance and security.

Semantic layers for explainable and trustworthy AI.

To support explainable and reliable AI, Dell introduced a semantic or knowledge layer. This layer provides contextual information that grounds AI outputs and improves the retrieval and use of enterprise knowledge.

AI is redefining the cyber-threat landscape.

The presentation stressed the importance of human-in-the-loop decision-making, AI life cycle management and cybersecurity. As AI expands the attack surface, organisations must establish robust governance, monitoring and recovery capabilities to protect data integrity, privacy and operational resilience.

> *Human in the loop is a central consideration for how we deal with AI in a decision process.*

Dennis Diefenbach



Dennis Diefenbach;
Chief Executive Officer;
The QA Company

Unlocking Enterprise Data with Large Language Models & Model Context Protocol (MCP)

Dennis Diefenbach concluded the session by presenting the Model Context Protocol (MCP) and its role in enabling agentic AI within secure and sovereign environments. Drawing on examples from the European Parliament, Eurostat and the Publications Office, he demonstrated how the MCP allows AI systems to interact with data sources and applications, making advanced AI capabilities accessible across organisations while maintaining control over deployment and governance.

Key points from his address include the following.

The MCP as a standard for agentic AI.

Mr Diefenbach described the MCP as an emerging standard that connects large language models with external applications and data sources. Comparable to a universal connector for AI, it allows AI systems to retrieve information, interact with software and perform tasks beyond the capabilities of stand-alone language models.

Turning organisational data into accessible knowledge.

Using a Eurostat example, Mr Diefenbach showed how the MCP enables non-technical users to query structured databases in natural language.

Bringing AI to existing systems and workflows.

Examples based on EUR-Lex and Microsoft Word demonstrated how the MCP can be integrated with existing applications without requiring major modifications.

Sovereign and secure AI deployment.

The QA Company develops solutions that run on premises and under organisational control, enabling institutions to adopt AI while meeting governance, compliance and data protection requirements.

> *MCP (Model Content Protocol) is generally seen as the USB-C for AI.*

Key insights and areas for action from session V

AI readiness starts with data readiness.

Effective AI implementation depends on high-quality, well-governed and accessible data. Data fragmentation, poor-quality data and inconsistent governance remain major barriers to the adoption of AI technologies.

Balance AI innovation with sovereignty and trust.

Public-sector organisations must enable AI while maintaining control over sensitive data. Federated approaches, local validation and human oversight provide practical ways to reconcile innovation with security and compliance.

Make data and AI accessible to operational users.

Natural-language interfaces, AI-powered analytics and automated reporting can broaden access to data, allowing non-specialists to generate insights and support decision-making.

Embed governance, security and cybersecurity by design.

Trustworthy AI requires governance throughout the life cycle, including data quality controls, explainability, human-in-the-loop decision-making and resilience against emerging AI-related cyber threats.

CLOSE OF THE EVENT

08

Closing remarks

Philippe Harant



Philippe Harant;
Head of Strategy, Capabilities and Coordination Unit;
eu-LISA

Philippe Harant closed the 2026 Industry Roundtable by reflecting on the key themes and lessons learned from the two-day event. Drawing on discussions about data governance, analytics, interoperability and AI, he highlighted the growing strategic importance of trust, data quality and digital sovereignty in managing Europe's large-scale information systems.

Key points from his address include the following.

Trust as the foundation of digital transformation.

Trust emerged as a recurring theme throughout the event. Security, data protection, fairness, explainability and auditability were identified as essential safeguards for data-driven services and AI-enabled systems.

Data quality as the basis for interoperability and AI.

Ensuring data quality at the point of capture is critical. In interoperable environments, poor-quality data can propagate across systems, affecting analytics, decision-making and AI applications.

Digital sovereignty and control over data.

Digital sovereignty extends beyond preventing unauthorised access to data. Organisations must also ensure continued access to their own strategic information assets and digital infrastructure.

Data as a strategic asset.

Mr Harant highlighted a growing shift from viewing data management as a by-product of operating large-scale IT systems to recognising data as a strategic asset. The demand for accurate statistics and data-driven insights is increasing across Member States and EU institutions and agencies.

A growing platform for collaboration and knowledge exchange.

The Industry Roundtable attracted record in-person participation from EU institutions, Member States, industry organisations and academics. Mr Harant emphasised its value as a forum for sharing experience, discussing common challenges and exploring future approaches to data management.

> *Zero trust by design is in fact what creates trust.*

CN: EL-01-26-024-EN-N
ISBN: 978-92-95237-30-8
ISSN: 2600-2728
doi: 10.2857/3416282

Copyright: © European Union Agency for
the Operational Management of Large-Scale IT Systems
in the Area of Freedom, Security and Justice. 2026
Images of waves: © Ahmad Araf/adobestock.com