eu-LISA Industry Roundtable

GOING TO THE CLOUD

Why it matters for the EU public sector and how to make it work

belgium24.eu

11-12 June, Antwerp, Belgium

be EU
belgium24.eu

eu-LISA
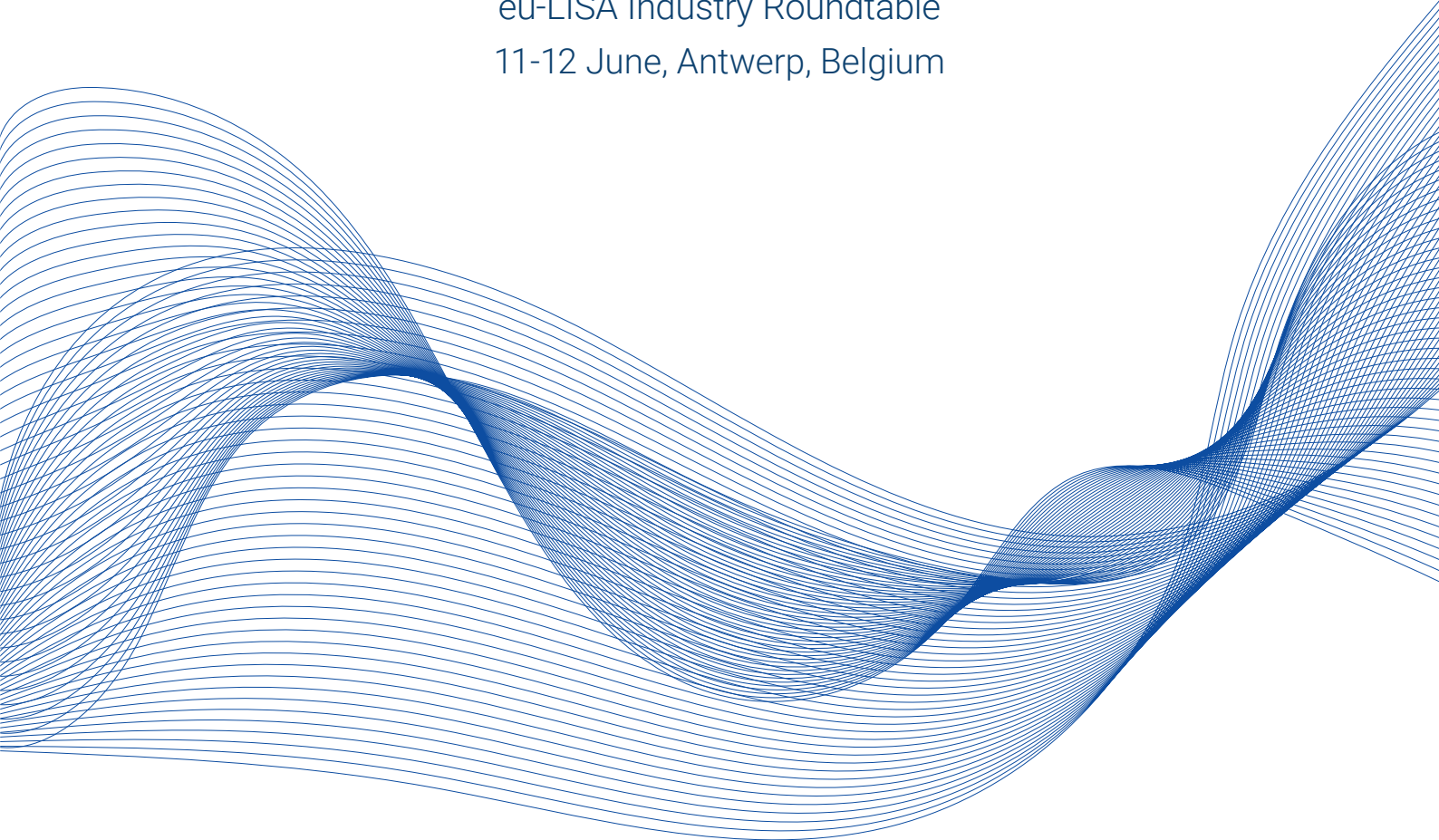Justice and Home Affairs Agencies Network

JHAAN
Presidency

Going to the cloud

Why it matters for the EU public sector and how to make it work

eu-LISA Industry Roundtable

11-12 June, Antwerp, Belgium

Contents

Executive summary

The eu-LISA Industry Roundtable 'Going to the cloud: why it matters for the EU public sector and how to make it work' was held in Antwerp, Belgium, and streamed online. The event, organised in collaboration with the Belgian Presidency of the Council of the EU, spanned 2 full days from 11 to 12 June 2024. The forum served as an opportunity for stakeholders to engage in the evolving discourse on cloud technologies and their transformative impact on public sector authorities operating in the area of freedom, security and justice across the European Union. The Roundtable was an engaging event, with over 320 attendees from 34 different countries.

The agenda of the event was carefully crafted to address the multifaceted challenges and opportunities presented by cloud adoption in the public sector. Topics such as security, privacy, sovereignty, interoperability and the different cloud adoption models were thoroughly examined.

Day one of the event set the tone with opening remarks delivered by the representative of the Belgian Presidency of the Council of the EU and eu-LISA's Executive Director, and a keynote presentation provided by the Ukrainian Deputy Minister for Digital Transformation that addressed the strategic importance of cloud technologies. It proceeded with a series of sessions, beginning with 'Setting the scene', which provided a foundational understanding of the cloud landscape. This was followed by a panel discussion featuring industry experts who offered diverse perspectives on the topic. The day concluded with an exploration of 'Cloud sovereignty: the Hyperscalers' perspective', giving participants insights into the views and approaches of leading cloud service providers.

The second day continued the dialogue with three focused sessions. 'Cloud security and privacy' delved into the core challenges and best practices to protect data in the cloud. This was succeeded by a session on 'Sovereign cloud adoption models and their interoperability', examining how the public sector can leverage different cloud models while ensuring seamless integration. The final session, 'The sovereign cloud as an enabler of innovation and digital transformation,' highlighted how cloud technologies are pivotal in driving innovation and modernising public services. The event concluded with final remarks given by the Head of Unit of eu-LISA's organising team, which encapsulated the insights and collaborative spirit of the discussions.

The main objective of the event was for participants to gain a clearer understanding of the EU's position on cloud technologies, and the advantages and limitations of various cloud services, and to share practical experiences from different public organisations, as well as to provide a common forum for the exchange of ideas among stakeholders and expansion of professional networks.

Day 1

- Opening remarks

- Keynote presentation

- Session I | Setting the scene

- Panel discussion

- Session II | Cloud sovereignty:
The hyperscalers' perspective

- Close of the meeting

DAY 1

01 Opening remarks

Agnès Diallo

**Executive Director,
eu-LISA**

The event was opened by the Executive Director of eu-LISA, Ms Agnès Diallo, setting the stage for the event's discussions by sharing eu-LISA's vision of leveraging technology to serve its mission effectively. She welcomed attendees, expressing her satisfaction at the continued tradition of the Industry Roundtable and its significance in fostering collaborative discussions on pivotal topics such as cloud technology. Ms Diallo highlighted eu-LISA's mission as a technological bridge bringing policy into reality, emphasising the agency's reliance on effective collaboration with the industry, the European Commission and Member States to enhancetechnological capabilities. The Director underscored the agency's expansive role across Europe, managing large-scale IT systems that supported the implementation of security, border management and migration policies, and facilitated collaboration in the justice domain. She cited the Schengen Information System (SIS), the Entry/Exit System (EES) and the European Travel Information and Authorization System (ETIAS) as examples of eu LISA's commitment to operational excellence and innovation. Reflecting on the theme of cloud technology, she acknowledged the critical operational challenges faced by eu-LISA, including the need for robust infrastructure to support the vast scale of data and transactions processed by the agency's systems. She addressed the legal and security considerations inherent in managing such systems, particularly focusing on the importance of finding the right balance between cloud and on-premise infrastructure. The speech also touched upon the evolving landscape of digitalisation, noting the accelerated timelines for deploying new systems and the increasing infrastructure costs. She emphasised the importance of agility, security and the need for innovative solutions to meet these challenges. Ms Diallo concluded her remarks by reiterating the value of the Industry Roundtable as a forum for sharing knowledge, addressing common challenges and exploring solutions that benefit the broader EU public sector community.

"

Until recently, the availability of sovereign cloud solutions that meet our specific needs and fit within existing constraints has been very limited. However, we believe that the cloud brings many strategic opportunities. This Industry Roundtable is an opportunity to learn more about this topic, to discover what the industry has to offer, and to gain inspiration from public sector organisations already using the cloud.

Philippe Rosseel

Director Internal Support and International Relations Federal Public Services Home Affairs – Belgium

Mr Philippe Rosseel, Director of Internal Support and International Relations of the Belgian Federal Public Services, Home Affairs, took the stage with a sense of pride, both as an Antwerp native and as a representative of the Belgian Presidency of the Council of the EU. Mr Rosseel provided an insightful overview of the cloud computing landscape within the EU public sector, highlighting the evolution from traditional data centre models to contemporary cloud-first strategies. He cited the Belgian federal government's proactive steps towards a comprehensive cloud strategy by 2025, aimed at enhancing infrastructure flexibility, security and scalability to improve government service quality. Mr Rosseel addressed the pivotal challenges of data protection, artificial intelligence (AI) and cybersecurity, underscoring the necessity for compliance with stringent EU regulations. He drew attention to the anticipated growth in sovereign cloud services, reflecting the public sector's demand for greater control over its data. Rosseel emphasised the importance of diversification in cloud strategies to mitigate the risks of dependency on external cloud providers, which could affect national sovereignty and the vitality of local ICT industries. With a forward-looking approach, Mr Rosseel expressed the public sector's need to carefully evaluate cloud adoption models, considering the balance of costs, risks and market assurances for data security and sovereignty. In conclusion, Mr Rosseel extended gratitude to the organisers for assembling a balanced and comprehensive agenda, and called for a collaborative approach to harness the potential of cloud technologies to enhance government services, safeguard sovereignty and ensure robust infrastructure for critical applications, setting a collaborative tone for the discussions to follow.

"

Cloud adoption can bring flexibility, security, and scalability of the infrastructures used, as well as strong improvements in the quality of government services. We want to deploy modern applications that offer modern user experiences. Yet, using the cloud also brings along a number of challenges to address.

Keynote presentation

Georgii Dubynskyi

Online intervention

Deputy Minister, Ministry of Digital Transformation of Ukraine

Mr Georgii Dubynskyi, Deputy Minister of Digital Transformation of Ukraine, delivered a compelling keynote presentation, sharing Ukraine's strategic shift to cloud technologies amidst the challenges of an ongoing war and the associated cyber threats. Mr Dubynskyi outlined the proactive measures taken by Ukraine's Ministry of Digital Transformation, established in 2019, to not only digitise but fundamentally reform and enhance public services. He emphasised the ministry's ambitious goals, including widespread internet coverage, digital skills development and the complete digitisation of public services. Mr Dubynskyi recounted the significant increase in cyber-attacks against Ukraine, highlighting in particular the massive distributed denial-of-service (DDoS) attack preceding the full-scale invasion of their territory by Russia. In response, Ukraine embarked on a digital migration, transitioning critical data to cloud services to safeguard against physical and cyber threats. This move was facilitated by legislative changes that allowed for the transfer of state information resources to cloud infrastructures, ensuring continuity of government functions even in the face of direct attacks on data centres. The Deputy Minister provided concrete examples of cloud adoption, such as the electronic document management system hosted on Microsoft Azure and the backup of the national health service database on Oracle Cloud. He also noted the pivotal role of Amazon Web Services in providing substantial cloud storage to secure backups of Ukrainian registries. Mr Dubynskyi highlighted the Diia application, a government mobile app that has been instrumental in maintaining access to public services during the war. The app's success underscored the importance of digital resilience, which encompasses the robustness of physical infrastructure, data and services. Looking forward, Mr Dubynskyi discussed Ukraine's national cloud programme aimed at modernising digital infrastructure, promoting cloud-first policies and creating a transparent market for IT solutions. The programme's objectives include developing a cloud design for Ukraine, ensuring security and compliance, and supporting cloud transformation and data migration. To conclude, Mr Dubynskyi expressed Ukraine's readiness to collaborate and share its cloud migration experiences, contributing to a broader European cloud strategy and reinforcing digital resilience on a continental scale. Ukraine's cloud transformation journey – despite being shaped by the ongoing war - offered valuable insights into the power of cloud technology in ensuring the continuity and advancement of digital government operations.

In addition to safety, cloud provides Ukraine with agility, scalability and security. The government is modernizing digital infrastructure to create a transparent market for IT solutions and cloud service. We need to keep our government running, our economy afloat and our people safe and cloud technologies help reach these objectives.

03

Setting the scene

Laura Balke

**Policy Officer, Cloud
and Software Unit, DG CNECT,
European Commission**

Ms Laura Balke, Policy Officer at DG CNECT, European Commission, deputising for the Deputy Head of the Cloud and Software Unit, Mr Manuel Mateo Goyet, provided a comprehensive overview of the European Union's cloud policy and its trajectory. She focused on four pivotal questions: the current state of the European cloud market, its future direction, the actions taken so far, and the next steps. Ms Balke highlighted the exponential growth of the European cloud market since 2017. She mentioned the dominance of major players such as Amazon Web Services, Microsoft Azure and Google Cloud, and the relatively small market presence of European-origin providers. The presentation addressed the uneven adoption of cloud services across Europe, with discrepancies between large and small companies and among Member States. Ms Balke noted that the rise of AI is expected to drive demand for more advanced cloud capabilities. Looking ahead, Ms Balke discussed the EU's Digital Decade policy programme, which sets ambitious targets for cloud service adoption and the deployment of edge computing nodes across the Union. She emphasised the need to bridge the digital divide and ensure access to low-latency computing power throughout Europe. She outlined the regulatory landscape, including the Data Act's provisions to combat vendor lock-in and promote interoperability, as well as the Digital Markets Act's role in addressing market power abuses. She also touched on security and the importance of unlawful data access prevention and the Commission's efforts to publish standard contractual clauses to aid authorities procuring cloud services and facilitate compliance with the Data Act. Investments in cloud and edge computing infrastructure were highlighted, including the significant role in funding public sector digitalisation of the Important Projects of Common European Interest (IPCEI) and the Recovery and Resilience Facility (RRF). Lastly, Ms Balke underscored the collaborative nature of the road ahead, involving industry compliance, Member State enforcement and the Commission's effective implementation of policies. She expressed optimism about the collective journey towards the future of cloud policy in the EU.

"

The Data Act seeks to open up space in the European cloud market and allow providers to distinguish themselves on the basis of their performance and their pricing, preventing lock-in practices. It does not regulate data flows, but it prevents unlawful data access, by enforcing that providers take reasonable measures to prevent potentially unlawful transfer of EU data to non-EU/EEA authorities.

Uku Särekanno

**Deputy Executive Director
for Information Management
and Processes, Frontex**

Mr Uku Särekanno, Deputy Executive Director for Information Management and Processes at Frontex, shared insights on the agency's adoption of cloud computing and its critical role in supporting its expansive operations. He began by stating the multiple and very diverse choices public institutions face with cloud computing, emphasising the need for speed and efficiency in operational support. Mr Särekanno provided an overview of Frontex's core areas of operation, including situational awareness, border management support, migrant return operations and facilitation of Schengen entry and pre-controls. He highlighted the agency's reliance on ICT systems to deliver these functions effectively, particularly in managing the complexity of their operations across numerous locations and joint operations throughout Europe. Frontex's adoption of cloud computing was driven by the necessity for a shorter time to market for their services, flexibility, scalability and the ability to adapt to changing business needs. Mr Särekanno detailed the agency's use of cloud services such as Office 365, Microsoft Intune, Azure DevOps and Azure Storage services, which have been instrumental in managing a vast number of devices deployed at border crossing points and supporting the development process. Despite the significant use of cloud services, Mr Särekanno noted that Frontex maintains a cautious approach, with critical applications and sensitive information still managed within its own data centre. He discussed the challenges faced by the agency, including compliance with the EU data protection framework, the dominance of major market players such as Microsoft, and the need for continuous risk assessment and data classification. Mr Särekanno concluded by acknowledging the need to find the right balance between marketing promises and security realities. He argued for a more active use of cloud services within public administration, emphasising the importance of proper risk assessments and a coordinated effort among EU institutions and agencies to negotiate favourable terms with cloud service providers.

Frontex has been using cloud technology in its operations for some years, albeit to a limited extent. The cloud's flexibility, scalability, and adaptability could be critical in meeting the ever-evolving operational needs, maintaining cost effectiveness. Moreover, the adoption of cloud services can enhance workplace attractiveness and significantly bolster resilience against cyber threats.

04

Panel discussion

Panel moderator:
Joris Vankeerberghen,
Head of the Smart Hosting
Platforms Sector, eu-LISA

Panellists:
Laura Balke, Policy Officer
Cloud and Software Unit,
DG CNECT, European
Commission

Uku Särekanno, Deputy
Executive Director for
Information Management
and Processes, Frontex

Jakub Mayer, Acting Head of
Digital Solutions Operations
Department, eu-LISA

In the panel discussion, the speakers explored the drivers for cloud adoption, the importance of compliance and security, the strategies to avoid vendor lock-in and the impact of recent policy initiatives on EU data sovereignty and cybersecurity. One key takeaway from the discussion was that cloud adoption is driven by the need for agility, scalability and faster time-to-market for services, as emphasised by Mr Uku Särekanno. Mr Särekanno also noted Frontex's role in providing operational support to the Member States and the potential of its cloud strategy to help Frontex with this mission. Mr Jakub Mayer agreed and expressed eu-LISA's view on the need for differentiated and specific security requirements for sensitive data that limit the scope within which cloud services can be considered. The panellists spoke on the importance of ensuring compliance with the EU regulations and the challenges. Ms Laura Balke highlighted the impact of the Data Act and the Digital Markets Act, which will enter into force in September 2025, on reducing egress charges and other customer 'lock-in' practices. Addressing vendor lock-in involves assessing applications and services suitable for the cloud, with a cautious approach to those containing sensitive data. Mr Särekanno stressed the importance of effective enforcement of cloud-related legislation to ensure security, while not restricting the potential benefits of the cloud. Moreover, Ms Balke discussed the importance given to sovereignty and cybersecurity concerns in the Data Act, which dictates a cautious approach to cloud adoption for sensitive large-scale IT systems, yet encourages the emergence of a 'market for trust'. Mr Mayer described eu-LISA's thorough assessment process for identifying opportunities for cloud use while maintaining data security and control. The panellists discussed recent trends, such as increased investment on digital services and the need for operational efficiency. They also noted the potential impact of AI on the demand for cloud services and its implications for data protection. Mr Särekanno highlighted the pressing need for agencies to outsource technological operations to the market while emphasising Frontex's commitment to proactively adopting new technologies. This approach was driven by Frontex's imperative to be more adaptive in delivering in its field of operations, which may involve taking greater risks than a typical agency. However, he underscored that Frontex maintains a steadfast focus on security throughout this process. Ms Balke stressed the importance of the establishment of cloud rules for the advancement of AI and mentioned that the European Commission was currently focusing on writing a compendium of rules that would provide guidance and procurement criteria to facilitate cloud adoption within the EU institutions. The panel concluded with questions from the audience, addressing topics such as agility in cloud adoption, end-user adoption and the Commission's consideration of specific technologies to facilitate transitions between cloud service providers. Overall, the panel provided insights into the complex landscape of cloud adoption within the EU public sector, emphasising the balance between leveraging cloud benefits and maintaining security, compliance and sovereignty standards.

05

Cloud sovereignty: The hyperscalers' perspective

Jean-Christophe Chauvet

—

Supporting public institutions in cloud adoption

Director Presales and Bid Management OVHcloud

Mr Jean-Christophe Chauvet from OVHcloud started his presentation by explaining how the company had been instrumental in aiding public organisations with their cloud migration strategies. He began by providing an overview of OVHcloud's global presence, with 32 data centres across 10 countries and its commitment to sustainability, as evidenced by their leading power usage effectiveness (PUE) and water usage effectiveness (WUE) indicators. Chauvet outlined the reasons why organisations opt for OVHcloud, including a vast ecosystem of partnerships, a comprehensive range of cloud services and a simple pricing structure that ensures predictability in costs. He emphasised OVHcloud's sustainability efforts, integrated model allowing for recycling of datacentre components, and the company's goal to be carbon neutral by 2030. The company was committed to data sovereignty, ensuring that clients had control over their data, immunity to extraterritorial laws and ethical management of data without unauthorised use or movement, with practices designed to be on the safe side of evolving regulations, such as the General Data Protection Regulation and the upcoming Data Act. Mr Chauvet shared three case studies demonstrating OVHcloud's role in facilitating public sector cloud adoption. The first case involved the Ministry of the Interior of France, where OVHcloud provided a flexible and agile cloud platform that significantly reduced application development time. The second case highlighted the French unemployment agency's need to manage peak demand, which was addressed by utilising cloud services for scalability and disaster recovery. The third case, involving the Ministry of Defence of France, showcased the use of a highly secure and available SecNumCloud platform to manage the vast data generated by maritime space monitoring. In conclusion, Mr Chauvet reflected on the challenges and the importance of building trust and confidence between cloud service providers and public organisations. He stressed the need for engagement on both sides to ensure successful cloud adoption, offering OVHcloud's experience as a testament to the potential of cloud services to meet the complex demands of the public sector.

"

OVHcloud's approach emphasizes control over data and freedom to move between providers without extra charges, reflecting our foundational belief in data sovereignty and ethical management.

Pieter Kestelyn

Microsoft cloud for sovereignty

**Senior Cloud Solutions
Architect, Microsoft**

Mr Pieter Kestelyn, Senior Cloud Solutions Architect for Microsoft, presented Microsoft's approach to supporting public institutions in their cloud adoption journey, focusing on the Microsoft Cloud for Sovereignty. Mr Kestelyn provided an overview of Microsoft's global cloud infrastructure, emphasising the company's commitment to sustainability and describing the innovative water-cooling technology that significantly reduces its data centres' carbon footprint. Mr Kestelyn highlighted the importance of data sovereignty, control and privacy, which are central to Microsoft's cloud offerings, ensuring clients have full ownership and control over their data. He discussed the drivers of digital transformation, such as the need for new services, cost savings and increased productivity. Hyperscale clouds such as Microsoft Azure enable significant innovation and agility, allowing for rapid experimentation and deployment of new technologies, particularly in AI and cybersecurity. Addressing concerns about data control and privacy, Mr Kestelyn introduced 'Microsoft cloud for sovereignty', which is built on top of Microsoft's hyperscale cloud and offers additional controls to meet sovereignty requirements. He detailed the three pillars of the solution: regulatory compliance tooling, consistent application of sovereign guardrails and guidance documentation for deploying workloads in compliance with regulatory standards. Mr Kestelyn explained the layered structure of Microsoft Cloud for Sovereignty, with its foundation in Microsoft's extensive data centre network and EU data boundary. The solution provides public cloud capabilities, compliance transparency and a portfolio of sovereign controls, including confidential computing and customer-managed keys for encryption. He concluded by outlining the service offering within the Microsoft Cloud for Sovereignty, which includes sovereign landing zones, sovereignty baseline policy initiatives, transparency logs, automated workload templates and extensive technical documentation.

"

Microsoft's cloud sovereignty helps ensure compliance with future regulatory changes using sovereign guardrails and provides public sector customers with a future-proof solution that helps reduce the risk perception associated with cloud adoption.

Mustafa Isik

AWS digital sovereignty: More control and choice without compromise

Chief Technologist for Sovereign Cloud Amazon Web Services

Mr Mustafa Isik, delivered a presentation focusing on the concept of digital sovereignty, the complexity of digital sovereignty, a range of concerns from security to data residency, and how Amazon Web Services (AWS) is addressing these through various initiatives and technological advancements. Mr Isik highlighted AWS's significant commitment to Europe, including EUR 215 billion in investment since 2010, a workforce of 220 000 employees and the development of key AWS technologies in European cities such as Dresden and Berlin. He shared his experience with ARD's Bayerische Rundfunk, where he led the transition to cloud services, underscoring the relevance of AWS's services to European entities. Furthermore, the presentation outlined the main pillars of digital sovereignty concerns: data residency and security, operator access restrictions, resiliency and survivability, and independence and transparency. AWS's approach to sovereignty was described as 'sovereign by design', with a range of technical measures, operational controls and contractual protections to ensure security and compliance. Mr Isik introduced the AWS Nitro system, a foundational security technology, which provides confidential computing by isolating customer workloads from the underlying hypervisor. AWS's commitment to security is further demonstrated by over 133 security and compliance attestations. AWS European Sovereign Cloud is an AWS region designed to cater to the specific digital sovereignty requirements of the European Union. The first such region will be located in Brandenburg, Germany and will feature three availability zones. It represented a significant investment of EUR 7.8 billion over 15 years and was intended to offer the same level of service as the global AWS Cloud, but with data residency, operations and metadata kept within the EU. Mr Isik concluded by emphasising AWS's dedication to providing advanced sovereignty controls and features without compromising the quality of the cloud services offered. He stated that the European Sovereign Cloud would not be a lesser version of AWS's global offerings but would maintain the same standards of innovation and service.

"

The European Sovereign Cloud will maintain the standards and engineering achieved in the USA's model but its infrastructure is going to be operated solely by AWS personnel that is resident in the EU, has EU work permits, and only while that personnel is located in a member state of the European Union.

Damien Rilliard

Meeting cloud sovereignty expectations: sharing lessons learned

**Senior Director EMEA
Sovereignty Lead Oracle**

Mr Damien Rilliard, Senior Director of EMEA (Europe, Middle East and Africa) Sovereignty Lead at Oracle, presented a comprehensive view of digital sovereignty from Oracle's perspective, emphasising that it was not a 'one-size-fits-all' concept. Recognising that definitions of sovereignty vary widely, depending on who you ask, Mr Rilliard pointed out the importance of understanding an organisation's specific sovereignty goals, which are influenced by the type of data, workloads and applicable regulations. Mr Rilliard underscored the distinction between cybersecurity and sovereignty, stressing that cybersecurity measures alone cannot ensure sovereignty in the cloud. He introduced the Oracle Cloud Infrastructure (OCI) approach to sovereignty, which included six key principles: location, isolation, access management, encryption, data access requests and contractual guarantees. Oracle acknowledged the need for flexibility and offered a range of cloud solutions, from fully connected public clouds to disconnected, air-gapped clouds that could be operated within a customer's own data centre. Mr Rilliard detailed the Oracle EU Sovereign Cloud, which had been operational for 12 months and provided a fully isolated, EU-dedicated cloud environment with organisational, technical and contractual controls to ensure data remained within the EU. Oracle's sovereign cloud solution was backed by contracts, including a Data Processing Agreement (DPA) that guaranteed no data transfer outside of the EU and no reliance on subcontractors. Mr Rilliard concluded with an invitation to explore further resources, including a white paper on Oracle's Sovereign Cloud principles. Overall, the presentation highlighted Oracle's comprehensive approach to addressing the complex challenges of digital sovereignty for governments and the public and private sectors across the EMEA region, showcasing Oracle's commitment to offering tailored cloud solutions that aligned with the diverse sovereignty requirements of different entities.

"

One size does not fit all. Oracle can establish special legal entities, alone or through partners, along with contractual and operational business practices to meet local sovereignty needs.

CLOSE
OF THE DAY

06

Closing remarks

Luca Zampaglione

———

Mr Luca Zampaglione, Acting Deputy Executive Director and Chief Security Officer at eu LISA, focused on cloud computing's role in enhancing eu-LISA's services. He delivered a clear message of support for cloud implementation within the agency, emphasising the importance of risk assessment prior to adoption to prevent new vulnerabilities and mitigate costs. He stressed his belief that it was a matter of time before most organisational processes were cloud-based, though he acknowledged legal restrictions that demand for data processing be conducted in-house. Highlighting the event's high attendance, both in-person and online, Mr Zampaglione interpreted this as a sign of the topic's widespread interest. He reiterated eu-LISA's role in transforming the visions of policymakers into reality through technology. He reflected on the takeaways from the day's discussions, starting with those from the Deputy Minister of Digital Transformation of Ukraine, who spoke about three types of resilience: data, infrastructure and IT services to those from the representatives from DG CNECT and Frontex, offering an institutional perspective on regulation and application of cloud services, especially in relation to cybersecurity and legal constraints on classified information. He stated that OVHcloud, Microsoft, AWS and Oracle presented the industry's standards for this technology. Mr Zampaglione noted the forthcoming EU regulation on information security, which would categorise information protection levels and could influence how cloud services were utilised for different data categories. In conclusion, Mr Zampaglione remained optimistic about the potential for classified information to eventually be managed in the cloud, despite the current challenges.

Acting Deputy Executive Director and Chief Security Officer, eu-LISA

"

———

eu-LISA is the digital heart of Schengen and with the use of cloud we could see the heart beat outside of its body for the first time.

Day 2

- **Session III** / Cloud security and privacy

- **Session IV** / Sovereign cloud adoption models and their interoperability

- **Session V** / The sovereign cloud as an enabler of innovation and digital transformation

- Close of the event

DAY 2

07

Cloud security and privacy

Eric Vetillard

———

Cybersecurity, sovereignty and certification: How do they mix?

Lead Certification Expert, The European Union Agency for Cybersecurity (ENISA)

Mr Eric Vetillard, Lead Certification Expert at ENISA, discussed the challenges and considerations involved in developing the European Union Cybersecurity Certification Scheme for Cloud Services (EUCS). He touched on the complexities of mixing sovereignty concerns with cybersecurity certification, likening it to oil and water due to their differing natures. Mr Vetillard began with several definitions to clarify the concepts involved: certification as a formal process involving third-party verification against requirements; cybersecurity as protection against cyber risks, including those to nations; and sovereignty as the ability of a state to remain independent and avoid interference. The EUCS aims to provide a certification scheme applicable to all cloud services, offering three levels of requirements corresponding to the levels defined in the Cybersecurity Act. He emphasised that while the EUCS can significantly contribute to cybersecurity, it is not expected to cover every specific risk for sophisticated use cases. Technical challenges to generate the EUCS included the selection of requirements, with the EUCS basing its three levels on Germany's Cloud Computing Compliance Criteria Catalogue (C5) to accommodate different evaluation methodologies. The EUCS also had to address the identity of each evaluation level and ensure that customers understand what security they are getting from their cloud service provider. The sovereignty discussion brought additional complexity; therefore, the EUCS does not enforce harmonised requirements around sovereignty. Mr Vetillard highlighted the difficulty of certifying aspects related to sovereignty, such as data storage and operations in the EU, technical measures such as encryption and company control. Mr Vetillard concluded by emphasising the strength of the EUCS approach in enforcing transparency and accuracy of information through the certification process. This approach strikes a balance between the practicalities of certification and the evolving nature of cybersecurity and sovereignty concerns.

"
———

The European Cybersecurity Certification Scheme will be based on the Cybersecurity Act and follow three main guiding principles: use-case based, transparency, and consistent evaluation.

Andre Engelbertz

Approaches towards a sovereign European cloud

Mr Andre Engelbertz, CTO of Cloud Services and VP Strategy at T-Systems, shared insights into T-Systems' approach to cloud services, emphasising the company's extensive experience and global reach. Mr Engelbertz highlighted T-Systems' four key service areas: advisory, digital enabler, managed services and infrastructure and security, which is integrated across all other areas. He also presented T-Systems' guiding principles, which includes sustainability, diversity, agility, security and sovereignty, the latter being the focal point of his presentation. Addressing sovereignty, Engelbertz outlined three distinct aspects: data sovereignty (control over data by its owner), operational sovereignty (control over the manipulation of infrastructure and the software stack) and technology sovereignty (independence from any technology provider, achievable through dual-vendor strategies and open-source solutions). He then discussed how T-Systems' offerings align with these sovereignty dimensions, contrasting them with the offerings of hyperscalers. While the hyperscalers provide flexibility and a broad feature ecosystem, they might have limitations in terms of operational sovereignty. T-Systems addresses this with offerings such as the sovereign controls on the Google Cloud Platform, the Open Telecom Cloud (OTC), private cloud solutions and the Open Sovereign Cloud, which is entirely based on open-source technology and operated out of Germany. Focusing on the OTC, Mr Engelbertz emphasised its compliance with the GDPR, addressing data and operational sovereignty and its reliable and secure infrastructure, backed by eight years of operation. Lastly, Engelbertz introduced the Future Cloud Infrastructure (FCI), T-Systems' private cloud offering, which is SAP certified and aligns well with regulated environments. FCI's multi-cloud connectivity platform makes it an ideal candidate for driving hybrid cloud scenarios by facilitating seamless integration with hyperscalers. Mr Engelbertz concluded by emphasising T-Systems' commitment to providing sovereign cloud solutions that can complement a multi-cloud strategy, offering a European-operated public cloud alternative with a robust feature set that caters to the sovereignty and regulatory needs of their clients.

CTO Cloud Services and VP Strategy T-Systems

T-System's Future Cloud Infrastructure combines ease of use of a public cloud, with more control, tenant separation, flexibility and cost predictability. Cloud solutions focused on operational, data, and technology sovereignty.

Rom Adams & Jose Rui Teixeira Nunes

A secured hybrid cloud experience

The joint presentation by Mr Rom Adams, AppDev Specialist Public Sector at Red Hat Inc, and Mr José Rui Teixeira Nunes, Solutions Architect at Amazon Web Services (AWS), focused on the secure hybrid cloud experience provided by their collaboration. Mr Adams began by discussing the common challenges organisations faced when deploying new platforms, emphasising the importance of security and compliance from the outset. He introduced the Red Hat Open Hybrid Cloud, which is founded on three pillars: a true platform for consistency, cloud-native development for streamlined deployment and full management automation for simplification. Central to the Red Hat approach is the OpenShift platform, which enables developers to work flexibly across various environments while maintaining security and compliance. Mr Adams highlighted ROSA (Red Hat OpenShift Service on AWS), which is a co-engineered solution between Red Hat and AWS, that allows for the rapid setup of a secure cloud environment. This solution helps organisations avoid the 'valley of death' of empty platforms by enabling them to quickly bootstrap a production-grade application environment. Mr Teixeira Nunes followed with a discussion on the infrastructure and services AWS offers that are integrated with ROSA, providing tools to build secure solutions that meet regulatory compliance. AWS services are designed to ensure data security and privacy, with customers maintaining full control over who accesses their data. Mr Teixeira Nunes provided examples of AWS infrastructure options, including dedicated local zones for specific customers or communities and AWS Outposts for on-premise cloud services. He also mentioned AWS's commitment to confidential computing with the Nitro system and the option for customers to manage encryption keys with the external key store. To validate AWS's claims on security and privacy, Mr Teixeira Nunes mentioned a number of third-party certifications. He then shared case studies of organisations that have achieved digital sovereignty through AWS, including a hospital in Germany, the Ukrainian government during the ongoing war and the Singapore government's Smart Nation Digital Government Group.

Rom Adams: AppDev Specialist Public Sector Red Hat Inc

Jose Rui Teixeira Nunes: Soltions Architect, Amazon Web Services

"

Most customers choose to run OpenShift on AWS because they want to keep existing tools and practices while leveraging investments in the AWS services portfolio. ROSA is the easiest and most convenient way to pay for and deploy fully supported and managed OpenShift clusters.

Darren McDonagh

The Nutanix cloud platform – the balance between cloud efficiency and sovereignty

Principal Solution Architect, Nutanix

Mr Darren McDonagh, Principal Solution Architect at Nutanix, presented the company's hybrid multi-cloud solution, emphasising Nutanix's capabilities in transforming on-premises hardware into hyper-converged solutions that offer the simplicity and services of the public cloud. Nutanix's software supports a wide range of workloads, including databases, virtual machines, containers and SAP, and can be deployed both on-premises and in public clouds such as AWS, Azure and Google Cloud. Mr McDonagh highlighted how Nutanix has assisted a number of EU agencies in transforming their private cloud infrastructures, providing the ease of a public cloud with the security of owning their data and hardware. He underscored the transformational nature of cloud computing, not just as a technology but as a business model that enables innovation and agility. He stressed the importance of a cloud operating model that allows organisations to build, operate, use and govern workloads in a hybrid multi cloud environment, delivering Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) to support all types of workloads, across various locations. Highlighting the complexity of today's cloud landscape, Mr McDonagh advocated a hybrid multi-cloud platform that provides a single skill set across all platforms, enabling the movement of applications between on-premises and cloud environments, as needed. Nutanix's solution aims to give organisations control over where to deploy workloads based on various factors such as data classification and regulatory requirements. Mr McDonagh provided examples of Nutanix's deployment and migration to the cloud for various entities, such as a German pension management company (HAPEV) and the European Commission's Directorate-General for Digital Services (DG DIGIT), both customers requiring secure and flexible hosting platforms. Nutanix's unified hybrid cloud is unique in the industry, offering a single operating model for all workloads and locations, with the ability to move workloads across environments without code changes. The company's software can optimise hosting in public clouds, resulting in cost savings and reduced risk, as the governance and security model remains consistent. In conclusion, Mr McDonagh emphasised Nutanix's capability to provide faster time to value, reduced risk during cloud migration and cost-effective solutions both on-premises and in the cloud.

"

Nutanix simplifies IT operations with a single software-defined cloud platform deployed on-premises or in the public cloud. This enables intelligent workload placement of your apps and data with zero code changes.

08

Session 4

Sovereign cloud adoption models and their interoperability

Stylianos Dolopikos, Ioannis Theodorakakos, & Christian Zahorski-Philippe

Migrating EMA's workloads to cloud

FROM LEFT TO RIGHT:

Christian Zahorski-Philippe: Head of Cloud Transformation Services for Public Sector, NTT DATA

Stylianos Dolopikos: Head of Cloud Acceleration Service, EMA

Ioannis Theodorakakos: Enterprise Network Architect, Cloud Acceleration Service, EMA

Mr Christian Zahorski-Philippe, Head of Cloud Transformation Services for the Public Sector from NTT DATA introduced the fireside chat with two representatives from one of their customers, the European Medicines Agency (EMA) – Mr Stylianos Dolopikos, Head of the Cloud Acceleration Service at EMA, and Mr Ioannis Theodorakakos, Enterprise Network Architect – to share their perspective on the cloud migration journey. They provided insight into the vision, challenges and lessons learned from EMA's cloud migration experience. They outlined the compelling events that drove EMA's cloud migration, such as the agency's relocation from London to Amsterdam and the termination of a data centre framework contract. EMA aimed to become a digital hub and accelerate innovation and digitalisation for its stakeholders, which include experts and pharmaceutical companies. They discussed the considerable scale of the migration effort, which involved over 1 000 virtual machines and 120 business applications, emphasising the need for service continuity throughout the process. During their discussion, they highlighted the challenges EMA faced due to its limited exposure to AWS and VMware cloud environments. Gaps that were addressed through extensive training programmes, technical workshops and partnerships with professional services. Governance was a key focus area from the beginning, with the implementation of AWS Control Tower and landing zone approaches to establish a strong foundation for cloud services. Technical challenges included migrating physical servers and replicating functionalities such as NTP (Network Time Protocol) network appliances, Oracle gateways, firewalls and VPN gateways to the cloud. The team utilised HCX (Hybrid Cloud Extension) software to extend their network from on-premises data centres to VMware cloud, maintaining IP address plans. They also stressed the importance of financial planning and cost management, advising that costs be calculated before migrating and that resources be powered off when not in use to optimise cloud expenses. Looking forward, EMA has begun the next phase of its digital transformation, focusing on application refactoring, modernisation and adopting DevOps principles and serverless computing to further innovate and support sustainability efforts.

"

The European Medicines Agency wanted to invest in becoming a full digital data driven agency and accelerate the innovation and digitalization for all of our stakeholders, to become a digital hub for the European regulatory network.

Antoine Duchaussoy

Moving to cloud in the EU: Practical solutions for critical applications

Solutions Engineering Manager, Thales

Mr Antoine Duchaussoy from Thales delivered a presentation on the challenges of cloud adoption for handling highly sensitive and classified data. Mr Duchaussoy's talk highlighted the unique challenges faced when merging cloud technology with the needs of sensitive and classified operations. As a Solutions Engineering Manager, he shared his experiences working in high-risk and sensitive environments such as Afghanistan, Mali and Iraq, where he had supported missions with NATO, the European Union, especially the European Defence Agency (EDA), the United Nations and the French Armed Forces. Thales, as described by Mr Duchaussoy, is not a conventional IT or cloud provider, but a company that specialises in trust across various domains, including sensing, transmitting and processing data for critical decision-making. He emphasised the company's expertise in creating secure, trustworthy environments in sensitive situations. Mr Duchaussoy talked about the limitations on cloud use in the defence and sensitive information sectors, citing restrictions due to data sensitivity, control and access challenges. He highlighted the need for secure communication and data handling, even in areas with poor connectivity such as Somalia, or when conducting remote military operations. To address these challenges, Thales introduced the TrustNest, which brings cloud-like features to users in restricted environments, and the Nexium Defence Cloud, a private cloud infrastructure that is hardened for classified information up to the EU 'Secret' level. This solution allows for cloud-like capabilities, such as orchestration and infrastructure as code, in environments where traditional cloud services are not feasible. Mr Duchaussoy pointed out the skills shortage in IT for such environments and how the 'GreenLake' offer from Hewlett Packard Enterprise (HPE) helps Thales to provide a pay-as-you-go model for hardware, mimicking cloud payment models. The presentation concluded with the message that there is no single cloud adoption model to fit all purposes and that organisations must consider their prerequisites and the level of trust that they can place in a solution.

"

More than just a single cloud approach, sovereign clouds require consideration of multiple cloud adoption models driven by data sensitivity, use cases and performance.

Renato Nascimento & Lukas Casier

Accenture offering for the management of hybrid and multi-cloud environments

FROM LEFT TO RIGHT:

Lukas Casier: Cloud Advisory Senior Manager, Accenture

Renato Nascimento: Sales Director for EU institutions, Accenture

Mr Renato Nascimento and Mr Lukas Casier from Accenture gave a joint presentation on the potential and challenges of hybrid cloud adoption for the European institutions, bodies and agencies. Mr Nascimento started the presentation by introducing Accenture's significant investment in cloud domains and experience in aiding clients' transition to cloud services. He detailed the current cloud environment landscape, citing a Flexera report that indicated that a majority of entities are adopting a multi-cloud approach, with many striving to transition from legacy systems to private and public cloud solutions. He emphasised the need to combine agility, performance and governance in the cloud domain, highlighting Accenture's approach to addressing these challenges through what they call the Cloud Continuum Control Plane. Mr Casier continued the presentation by discussing the importance of developing a hybrid cloud and data strategy tailored to the benefits institutions aim to realise. He highlighted that public clouds offer extensive innovation opportunities and that solving sovereignty challenges in public cloud environments can maximise value for the European institutions. Mr Casier introduced the concept of landing zones: pre-configured environments installed on public cloud accounts to ensure compliance with security standards and organisational policies. He emphasised Accenture's development of landing zone products across major cloud providers and their successful implementation in some of Europe's largest institutions. The presentation concluded with an outline of the Cloud Continuum Control Plane and how it integrates capabilities across public and private clouds to manage complexity, increase cost efficiency and enforce security and compliance, delivering tangible value for clients' cloud management needs. Messrs Nascimento and Casier concluded by stating that Accenture's approach can bring tangible value to the EU agencies such as eu-LISA, addressing their unique concerns and leveraging on lessons learned from years of experience in the field.

"

Public cloud offers the richest service catalogues to support innovation, so if you're able to solve the sovereignty challenge you can also maximize the value potential for any European institution.

Colin Taylor

————

Edge-to-cloud sovereignty, on your terms – sovereignty and interoperability enablers of public sector cloud adoption

Hybrid Cloud Strategist, Hewlett Packard Enterprise

Mr Colin Taylor from Hewlett Packard Enterprise (HPE) discussed HPE's approach to cloud services, focusing on hybrid cloud strategies in particular. Mr Taylor's presentation offered an insight into HPE's perspective on cloud adoption and the evolving landscape of cloud services. He shared HPE's journey from an infrastructure company to one that offers cloud services where customers need them, including in their own data centres. This strategic direction was supported by significant investments to better understand the cloud model's appeal. Emphasising the importance of trust in cloud service providers, Mr Taylor discussed the concept of 'poly cloud' as opposed to 'multi cloud', suggesting that no single provider can meet all needs, and that the future will likely involve a mix of different cloud services from various providers, including niche players. Mr Taylor also touched upon the importance of sovereignty, data control and the ability to trust the people operating cloud platforms. He suggested that a greater number of European companies should become providers of cloud services to create a healthier and more balanced market. Mr Taylor covered the distribution of workloads across different cloud environments, the challenges faced by businesses and IT leaders when managing hybrid cloud infrastructures and the concept of HPE's GreenLake cloud for private cloud enterprise. In his conclusion, Taylor emphasised the need for partnerships and collaboration with trusted service providers. He advocated using open-source tools and avoiding vendor lock-in by not relying solely on a provider's native tooling.

"

————

Poly-cloud is the notion that you're not ever going to get everything from a single provider, different providers meet different needs. HP Enterprise is interoperable, giving you the ability to integrate HPE and non-HPE components.

09

Session 5

The sovereign cloud as an enabler of innovation and digital transformation

Alejandro Fernández Muñoz

Spain's justice journey to the cloud: Strategy and example use cases

Area Manager, Ministry of the Presidency, Justice and Parliamentary Relations, Spain

Mr Alejandro Fernández Muñoz from the Ministry of the Presidency, Justice and Parliamentary Relations of Spain, discussed Spain's approach to cloud implementation in the public sector, particularly within the Ministry of Justice. He emphasised the need to adopt cloud technologies wisely and outlined strategies for integrating cloud services while maintaining data sovereignty and security. Mr Fernández Muñoz provided an overview of the digital transformation efforts within the Spanish justice system, which served a large number of internal and external users and had initiated numerous AI and RPA (Robotic Process Automation) projects. The Spanish Ministry's digital agenda focuses on harnessing new technologies for economic growth and social cohesion, with a strategic emphasis on infrastructure, citizen skills and public sector digitalisation, delivering secure, efficient and reliable technologies with autonomy and control over data. This includes a hybrid cloud approach, combining state clouds, public clouds and private clouds for public administrations and universities. A significant effort is also underway to consolidate data centres into fewer, larger facilities. The Spanish Ministry of Justice's approach to new developments is primarily on premise, with cloud migration limited to applications requiring cloud-specific capabilities. The Ministry is also exploring IT on-demand data centres, hybrid multi-cloud and software as a service, emphasising the importance of a Cloud Centre of Excellence to guide the process. Mr Fernández Muñoz discussed the establishment of a landing zone, a pre-configured environment in cloud data centres, created in partnership with Amazon Web Services. This facilitates scalable, secure and compliant cloud deployments. Additionally, he highlighted successful cloud projects within the Ministry, such as a digital virtual desktop for remote court hearings, low-code applications for rapid development and AI projects for transcription and legal text simplification. The presentation concluded with an affirmation of the Spanish Ministry's commitment to cloud technologies, provided that they are implemented wisely and securely, with infrastructure made available by the government itself to ensure sovereignty and control.

"

With a hybrid multi-cloud solution we hope to achieve more secure, efficient, and reliable technological infrastructures for the provision of digital public services while safeguarding the country's strategic autonomy, security, and control over data

Akira Ito

Accelerating safe and secure data exchange with Fujitsu Data e-Trust

Senior Research Manager, Fujitsu

Mr Akira Ito from Fujitsu presented Fujitsu's Data e-Trust platform for accelerating safe and secure data exchange. He explained how various EU-Japan cooperation agreements on data exchange have created an environment conducive to secure personal data exchange, data flow for non-personal data and data flow with trust. Fujitsu's Data e Trust, commercially available in Japan, is being explored for the European market to enable data sovereignty through a secure data platform. Mr Ito detailed Data e-Trust's concept, which facilitates collaboration with distributed personal and corporate data, allowing data linkage across organisations and providing governance in data ownership and disclosure. It allows individual data owners to grant data access consent and ensures tamper-free management of data trails. To support Data e-Trust, Fujitsu offers advanced technologies that enable interoperability and support data exchange between the EU and Japan. Mr Ito introduced IDYX (Identity Exchange) and CDL (Chain Data Lineage), technologies that support trust in data exchange and the origin and trail of data, respectively. These facilitate secure certificate conversion between the EU and Japan data spaces, and interconnectivity with various blockchain platforms. He compared Data e-Trust to standard blockchain systems, highlighting how Data e-Trust provides separated databases with concepts of data ownership and data sovereignty, unlike blockchain's public and immutable ledgers. Lastly, he presented use cases of this technology, such as trusted learning information with Kwansei Gakuin University and carbon neutrality efforts with the Green Digital Consortium in Japan.

"

Fujitsu developed Data e-Trust a secure data platform for data sovereignty. It enables data linkage across organizations, and it provides governance in data ownership and disclosure. An individual data owner can grant consent for their own data, it affords additional credential for certificate, and it enables tamper-free management of data trails.

Stephan Scheers & Laurent Plichart

Why observability and AI will help your cloud adoption?

FROM LEFT TO RIGHT:

Stephan Scheers: Account Executive, Dynatrace

Laurent Plichart: Solutions Engineer, Dynatrace

The presentation by Mr Stephan Scheers, Account Executive, and Mr Laurent Plichart, Solutions Engineer, from Dynatrace, began by highlighting the importance of observability and artificial intelligence in cloud adoption. They emphasised the complexity of cloud migration and the need for a strategy, observability and automation to drive adoption and migration to the cloud. They showcased Dynatrace's observability platform with artificial intelligence at its core, providing end-to-end visibility and automatic problem detection and root cause analysis. The platform aims to streamline troubleshooting, reduce alert storms and provide a single source of truth for the development, security and operations teams. It also offers application security and vulnerability detection, protection and automated response, addressing the security aspects of cloud environments. The speakers presented real use-cases, including a European agency (undisclosed) and the European Commission, where Dynatrace's observability and AI capabilities led to significant improvements in troubleshooting, productivity and efficiency. The speakers also addressed concerns about AI training and emphasised that Dynatrace's AI is decentralised, working on the user's own server without the need for centralised data analysis. Overall, the presentation highlighted the critical role of observability and AI in cloud adoption, showcasing Dynatrace's capabilities in streamlining troubleshooting, improving security and optimising cloud environments. The success stories shared underscored the tangible benefits of adopting Dynatrace's observability platform with artificial intelligence for public sector organisations.

"

Dynatrace integrates Cloud-Based legacy modernization with hyper-modal decentralized Artificial Intelligence. Observability and artificial intelligence will help in cloud adoption by allowing users to access the data and problem solve by using natural language.

CLOSE OF THE EVENT

10

Closing remarks

Philippe Harant

———

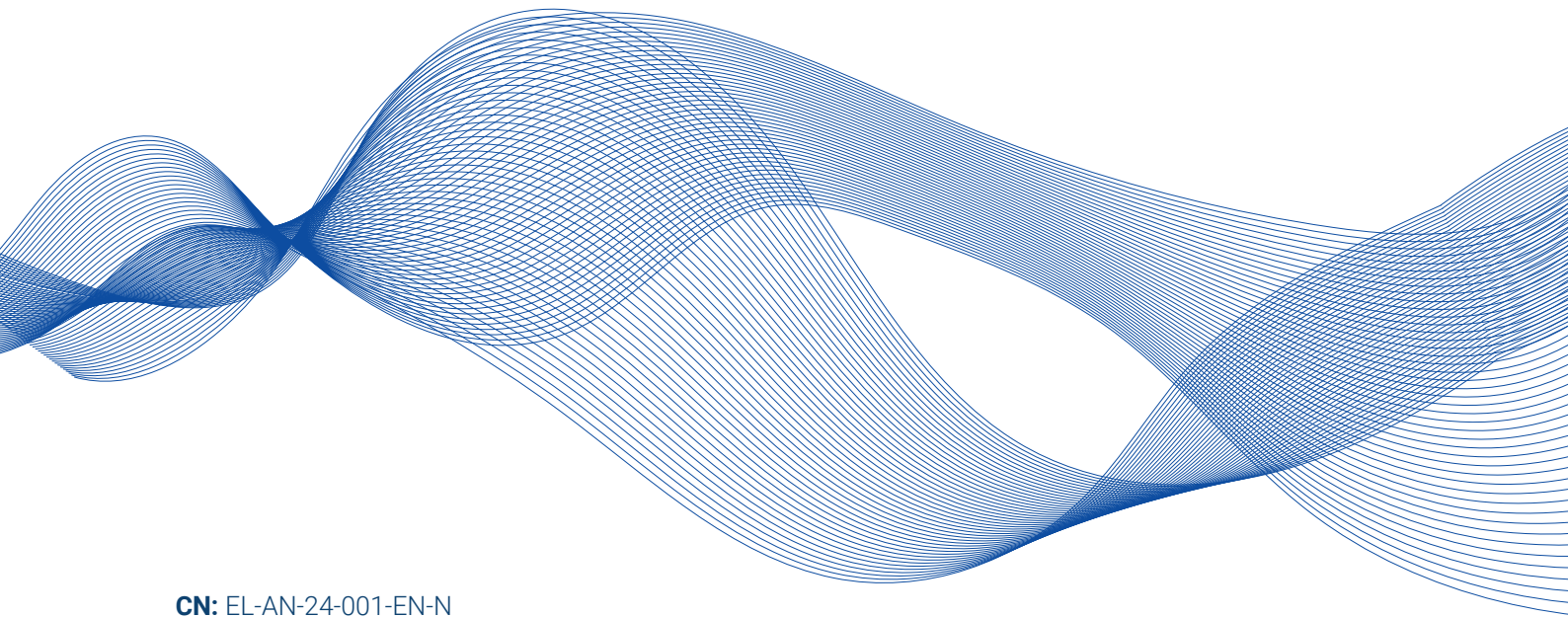**Head of the Strategy, Capabilities and Coordination Unit, eu-LISA**

Mr Philippe Harant, Head of the Strategy, Capabilities and Coordination Unit at eu-LISA, concluded the Industry Roundtable by thanking all the speakers for their rich and insightful contributions. He highlighted the significant participation from industry, Member States the European Commission, and the EU agencies and the numerous proposals submitted by the industry, indicating a strong interest in cloud technologies, in particular in the sovereign cloud. Mr Harant summarised the main takeaways from the discussions, noting that the consensus is not on whether to move to the cloud but how to do so, considering the cloud as a necessity for many public sector organisations. The variety of cloud solutions, including hyperscalers and hybrid solutions, were discussed, emphasising the need to balance innovation with security and sovereignty. Security emerged as a key concern as well as solutions to support it, such as security by design, zero trust and certification, all of which were mentioned as important considerations for cloud adoption. Mr Harant expressed the value of the Industry Roundtable in fostering dialogue between industry, Member States and the EU to address needs and co-design innovative solutions. He thanked the team behind the event for their professionalism and dedication, and the Belgian Presidency representatives for their support. Lastly, he announced the 10th anniversary of the Industry Roundtable, inviting attendees to the next Industry Roundtable event which will take place in Budapest on 12 13 November 2024, organised in cooperation with the Hungarian Presidency of the EU Council.

"

———

The question is not anymore whether or not to go to the cloud but how to go to the cloud.