



Predsednica Republike Slovenije

NATAŠA PIRC MUSAR

**Speech of the President of the Republic of Slovenia
Nataša Pirc Musar
EDEN conference**

The Hague, 16th of September, 2024

Ladies and gentlemen, esteemed colleagues, distinguished guests,

It is with great pleasure and a deep sense of responsibility that I address you today at this year's Europol Data Protection Experts Network Conference (EDEN 2024). This event, as many of you know, is not just a conference; it is a beacon for the data protection community, bringing together professionals, law enforcement officials, regulators, academics and representatives from the private sector and NGOs. It is a gathering that reflects the diverse and interconnected world we live in, where the protection of personal data is no longer just a legal requirement but a fundamental aspect of our shared values and a cornerstone of democracy.

First and foremost, I want to express my sincere gratitude to the organizers of this conference, in particular, the Data Protection Officer, Daniel Drewer. Your work in creating this space for dialogue and collaboration is invaluable. In a world where the pace of technological advancement often outstrips our ability to fully comprehend its implications, the importance of these discussions cannot be overstated.

I would also like to acknowledge and express my appreciation for my fellow keynote speakers:

- *Ms Catherine De Bolle, the Executive Director of Europol;*
- *Mr Wojciech Rafał Wiewiórowski, the European Data Protection Supervisor;*

- and Mr Olivier Onidi, the Deputy Director-General for Migration and Home Affairs in the European Commission.

Each of you brings a wealth of knowledge and a unique perspective to this conference. Your contributions to the field of data protection and cybersecurity in law enforcement have been instrumental in shaping the robust frameworks we have today.

As I stand before you today, I am struck by how deeply my professional journey has been intertwined with the evolution of data protection in Europe. From my time as the Information Commissioner of the Republic of Slovenia to serving as the Chairperson and co-chairperson of the Joint Supervisory Body of Europol, to working as an attorney specialized in data protection law, and now, as President of Slovenia, data protection has been a consistent and vital thread in the fabric of my career.

When I reflect on these roles, I am reminded of the critical importance of data protection in our society. As Information Commissioner, my task was to safeguard the privacy of Slovenian citizens, ensuring that their personal data was handled with the care and respect it deserves. This role taught me the value of transparency, accountability and the need for robust legal frameworks to protect individual rights.

In my role as the Chairperson of the Joint Supervisory Body of Europol, I encountered the complexities of ensuring privacy and security at the European level. This position brought with it the challenge of overseeing an organization that plays a crucial role in maintaining the safety of our societies while ensuring that fundamental rights are not compromised in the process. It was here that I truly understood the intricate dance between safeguarding individual freedoms and ensuring collective security.

Now, as President of Slovenia, I carry these lessons with me every day. My commitment to data protection has not wavered; in fact, it has deepened. The responsibilities of Head of State have given me a broader perspective on the role of data protection in governance. It is not just about protecting data; it is about protecting trust. Trust in our institutions, trust in our laws and trust in the future we are building for the next generation.

Throughout my career, I have witnessed first-hand the transformative power of data protection. It is not merely a technical or legal issue; it is a matter of principle. Our commitment to protecting personal data reflects our commitment to human dignity and individual autonomy. It is a commitment that must be upheld, regardless of the challenges we face. If anywhere, this is especially true in the area of law enforcement.

As Head of State, I am acutely aware that security and the protection of personal privacy are both essential and interdependent. As new technologies emerge and society evolves, our approach must adapt, but our commitment to safeguarding the fundamental rights of our citizens remains steadfast. Data protection is a cornerstone of these rights and must be upheld with the utmost integrity, ensuring that both security and privacy are fully realized in our efforts.

Let us now turn our attention to the evolution of data protection in Europe—a journey that has been as challenging as it has been rewarding. When I served as the Chairperson of the Joint Supervisory Body of Europol, the landscape of data protection was markedly different from what we see today. The JSB was tasked with overseeing Europol's compliance with data protection regulations at a time when the digital age was still in its formative years.

Back then, we were laying the groundwork for what would eventually become a comprehensive and cohesive data protection framework across Europe. The transition from the Joint Supervisory Body to the European Data Protection Supervisor (EDPS) marked a significant milestone in this journey. This shift not only centralised oversight but also strengthened the mechanisms for protecting personal data across the European Union.

The introduction of the General Data Protection Regulation (GDPR) and the EU Data Protection Regulation (EUDPR) in 2018 was a watershed moment, not just for Europe but for the world. The GDPR set a global benchmark for data protection, emphasising the importance of individual consent, transparency and accountability. It reinforced the idea that personal data belongs to the individual and that organizations must earn the right to use it.

The Law Enforcement Directive (LED) and the Europol Regulation (ER) further enhanced this framework, addressing the specific needs of law enforcement agencies while ensuring that fundamental rights are not compromised. These regulations have provided a robust legal basis for the processing of personal data in the context of law enforcement, taking into account both the need for security and the protection of individual freedoms.

Europe's leadership in data protection has not gone unnoticed. The principles enshrined in the GDPR, EUDPR, LED and the Europol Regulation have resonated far beyond our borders. Countries around the world have looked to Europe as a model for developing their own data protection laws, and this has led to a ripple effect of stronger privacy protections globally.

But with leadership comes responsibility. As we move forward, we must continue to uphold the values that have made Europe a leader in data protection. We must resist the temptation to compromise on these values in the face of new challenges. The digital landscape is constantly evolving, and with it, the threats to privacy and security are becoming more complex. But I firmly believe that these challenges also present opportunities—opportunities for innovation, for collaboration, and for reaffirming our commitment to the principles that guide us.

I am not going to repeat statements that already have been made on many occasions regarding the interplay between security and privacy. Let me just say clearly that we want and actually need both!

The complexity of data management in the digital age, however, adds another layer to this challenge. As organizations collect and process vast amounts of data, the risk of breaches, misuse and abuse grows. This is where the role of Data Protection Officers (DPOs) becomes crucial.

DPOs are the unsung heroes of the data protection world. They serve as the internal guardians of privacy within organizations, ensuring that data protection principles are upheld at every level. Their role is not just about compliance; it's about fostering a

culture of data protection, where every employee understands the importance of safeguarding personal data.

It is also important to reiterate the need for DPOs to maintain their independence within organizations. Independence is not a luxury; it is a necessity. Without it, DPOs would be unable to provide the critical oversight needed to ensure that data protection principles are upheld.

This independence does not mean isolation. On the contrary, DPOs should be fully integrated into their organizations' overall data protection strategy. They should have a seat at the table when decisions are made, and their voices should be heard loud and clear. This is how we can ensure that data protection is not just a checkbox exercise but a fundamental part of organizational culture.

But DPOs cannot operate in isolation. Collaboration is key to their success. Just as Data Protection Authorities (DPAs) collaborate to ensure consistent enforcement of data protection laws across Europe, DPOs must also collaborate with each other. Knowledge-sharing, exchange of best practices and mutual support are essential in enhancing the effectiveness of DPOs across Europe.

I strongly advocate for the strengthening of these networks of collaboration among DPOs. By working together, DPOs can address common challenges, share insights and develop innovative solutions that benefit the entire data protection community.

The EDEN Conference plays a vital role in fostering this culture of collaboration and engagement. By bringing together a diverse range of participants—law enforcement officials, regulators, NGOs, academics and private sector representatives—this conference provides a unique platform for dialogue and exchange on ongoing challenges and anticipated developments, such as the effect of AI on policing and the privacy of individuals.

The importance of this inclusive dialogue cannot be overstated. Data protection and cybersecurity in law enforcement are complex and multifaceted issues that require input from all sectors of society. By engaging with a broad spectrum of stakeholders,

we can develop more comprehensive and effective data protection strategies that take into account the needs and perspectives of all involved. And also, in this increasingly digital world, the opportunity to meet face-to-face and to catch up on old friendships, and to make new ones, cannot be overestimated.

I want to take this opportunity to emphasize the importance of continued and increased collaboration among all stakeholders in today's digital landscape. The challenges we face in data protection and cybersecurity are too complex and multifaceted to be tackled by any one sector alone. Governments, private enterprises, academia, civil society and international organizations each bring unique perspectives, resources and expertise to the table. By working together, we can pool our strengths and address these challenges more comprehensively and effectively.

Cross-sector collaboration enriches the discourse, bringing in diverse perspectives and expertise that are crucial for understanding and solving the nuanced problems we face. For example, the technical expertise of the private sector can complement the regulatory knowledge of governmental bodies, while academic research can provide insights into emerging threats and innovative solutions. This collaborative approach allows us to see the bigger picture and to develop solutions that are not only effective but also sustainable in the long term.

In a world where data knows no borders, our efforts to protect it must also be borderless. This means fostering international cooperation, where countries work together to harmonise data protection standards and share best practices. It also involves interdisciplinary collaboration, where experts from fields as varied as law, technology, ethics and sociology come together to address the multifaceted nature of data protection challenges. Only by embracing this comprehensive and cooperative approach can we hope to create a digital landscape that is secure, resilient and respectful of individual rights. And EDEN is the perfect place to do this!

As I conclude, I want to return to where I began—my personal journey from serving as the Information Commissioner of Slovenia to my current role as President of Slovenia. This journey has been shaped by my commitment to data protection, a commitment that has only grown stronger with time.

My experience has taught me that data protection is not just about safeguarding information; it is about safeguarding trust. It is about ensuring that individuals can trust that their personal data will be handled with care and respect. It is about ensuring that our institutions can be trusted to protect the rights and freedoms of our citizens.

This is a journey that can take you anywhere, even to the Presidential Palace. It is a testament to the importance and relevance of data protection in today's world. For those of you who are dedicated to this field, know that your work is not only valuable but also transformative. You are shaping the future of privacy, security and governance in the digital age.

To those in the audience who are just starting their careers in data protection, let me say this: Your expertise can open doors to significant leadership roles. The skills and knowledge you gain in this field are not only applicable to data protection but also to broader issues of governance, ethics and human rights. You are the future leaders who will continue to drive the evolution of data protection, and I have no doubt that you will rise to the challenge.

I want to particularly encourage the young women in the audience who are pursuing or considering careers in data protection. The technology and cybersecurity fields have historically been male-dominated, but your voices and perspectives are vital to achieving true gender balance and diversity in this field. Your contributions will shape the policies and practices that protect our rights in the digital age. As you gain expertise and experience, you will be well-positioned to take on leadership roles that influence not only data protection but also the broader landscape of digital governance and ethics.

Remember, your journey in this field is not just about advancing your career—it's about breaking down barriers, setting new standards and inspiring the next generation of women to follow in your footsteps. The challenges ahead are significant, but so are the opportunities. With your passion, dedication and unique insights, you have the power to drive meaningful change and lead us towards a more inclusive and equitable digital future.

As we move forward, I encourage all of you to continue advancing data protection in a way that respects individual privacy and promotes trust in our institutions. The work you do is not easy, but it is essential. Together, we can build a future where data protection is not just a legal obligation but a core value that underpins our society. This is a collective responsibility that we all share, and your dedication to this mission is what will ensure that our digital future remains secure and respectful of individual rights.

Responsible use of personal data is the key to sustainable growth, to a world where we can enjoy all the privileges of the digital millennium, not at the expense of our human rights and freedoms.

It is of utmost importance that we keep this in mind at all stages of development of AI technologies, and of its future uses, especially when used by states and law enforcement, due to their unique position of power.

In fact, as the title of this conference suggests — “Data Protection and Cybersecurity as Law Enforcement Core Business” — it is clear that these principles are now central to the very mission of law enforcement. Protecting data and ensuring cybersecurity are not just auxiliary tasks; they are integral to maintaining the safety, security and trust that our societies rely on. These principles must be woven into the fabric of every decision and action within law enforcement agencies. By embedding data protection and cybersecurity at the core of your work, you not only fulfill your legal obligations but also strengthen the trust that the public places in your institutions.

I want to extend my deepest gratitude for the opportunity to speak with you today. I am confident that the insights and collaborations fostered during this conference will play a crucial role in advancing our shared goals. Unfortunately, due to other pressing commitments in my role as President, I must take my leave and cannot stay for the remainder of the conference.

I wish you all a productive and inspiring conference, and I look forward to seeing the innovations and collaborations that will emerge from your discussions. Thank you once

again, and I trust that today's dialogue will contribute to the ongoing strengthening of our data protection and cybersecurity frameworks.

Thank you.