University of Luxembourg

multilingual. personalized. connected.

Risk management in data protection: a share perspective of DPO & CISO of the University of Luxembourg

Agenda

UNIVERSITÉ DU LUXEMBOURG

- Introduction
- Why are we presenting together
- Why our coordination is key?
- How is our coordination organised?
- The Data Protection Officer and the Chief Information Security Officer cooperation
- Similarities within our methodology
- Case Study: A Data Breach Incident
- What about data protection impact assessment collaboration?
- Example of DPO & CISO collaboration regarding a DPIA
- Conclusion

Introduction

Sandrine Munoz

Data Protection Officer of the University of Luxembourg since 2016
Lawyer working in research and education with data protection mission
Linkedin
sandrine.munoz@uni.lu

Introduction

Laurent Weber

Chief Information Security Officer of the University of Luxembourg since 2023
Board member of RESTENA

https://www.linkedin.com/in/laur3nt/
laurent.weber@uni.lu

Why We Are Presenting Together

Collaboration in Data Protection & cybersecurity

- ✓ Data Protection & cybersecurity are interconnected and require joint efforts from all actors within the organization.
- ✓ By working together, we can effectively address the multifaceted challenges of data protection and cybersecurity.
- ✓ Data Protection & Information Security: There is no personal data protection without information security. Personal data is a key aspect of information security.

Key Objectives

- ✓ Demonstrate how our coordinated efforts have created a data protection & security framework.
- ✓ Highlight the synergy between the CISO and DPO roles in protecting data and ensuring compliance.
- ✓ Show how this collaborative approach enhances overall data protection & security and promotes a culture of awareness across the University.

Why our Coordination is Key?

Legal Requirement : Art.32 GDPR requires security of personal data processing

Pragmatically 2 officers having risk detection & management in their DNA

- Practical Impacts
- Prevent from Data breaches
- Protects the University's reputation
- Ensures compliance with Regulatory requirements

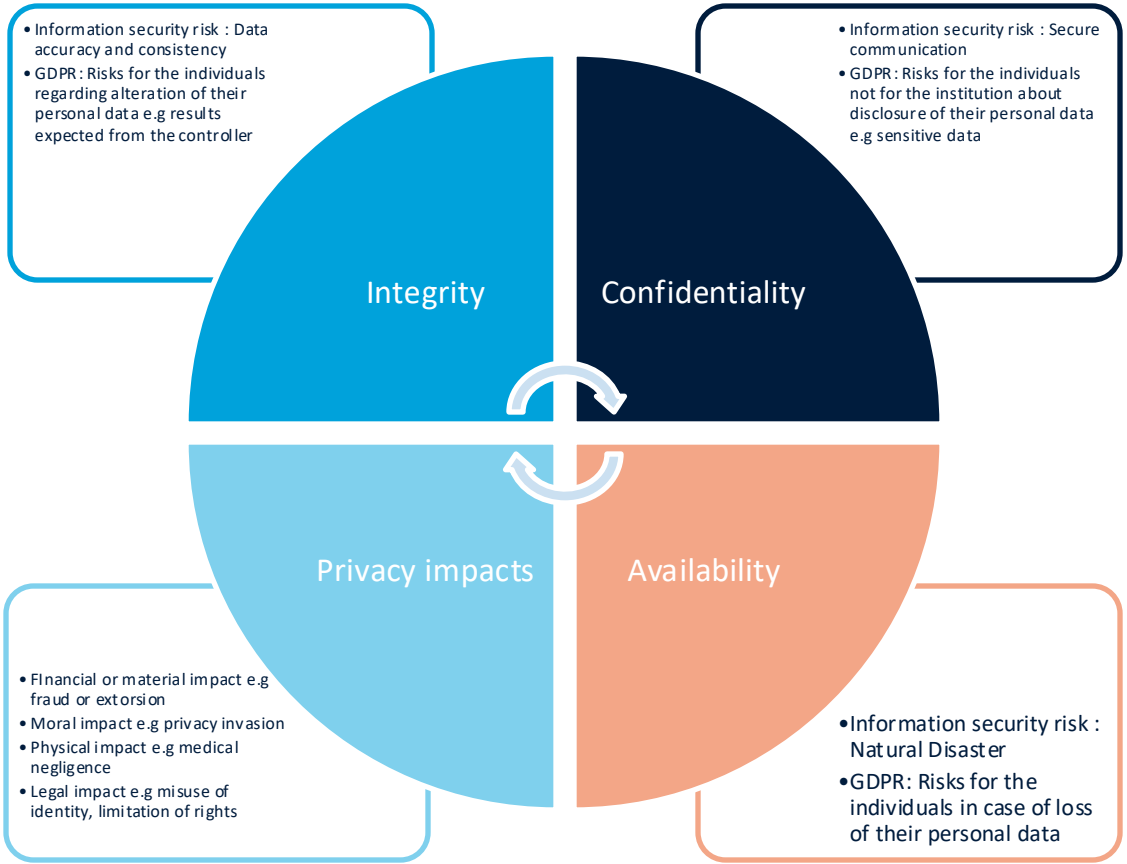
How is our Coordination Organized?

The Data Protection Officer and the Chief Information Security Officer cooperation

What are our main areas of collaboration?

- Data breach
- Data protection impact assessment
- Controls
- Processes, policies & procedures

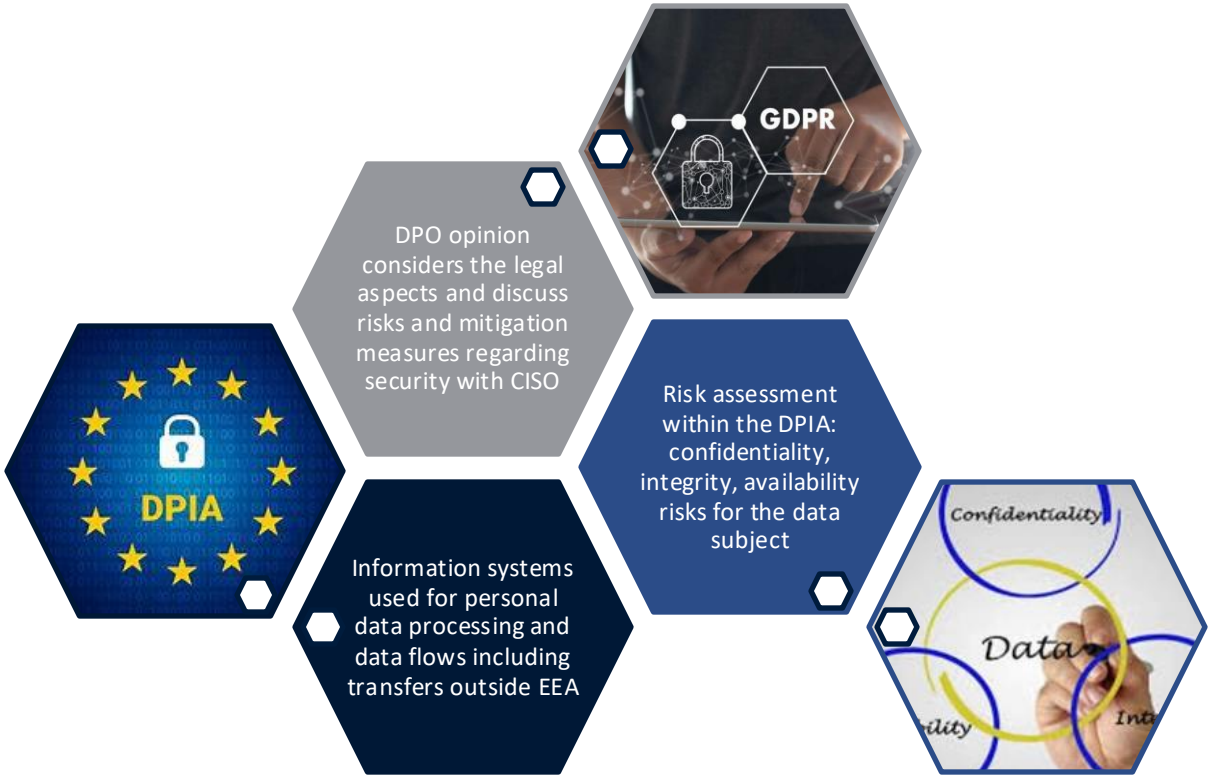
Similarities within our methodology



Case Study: A Data Breach Incident

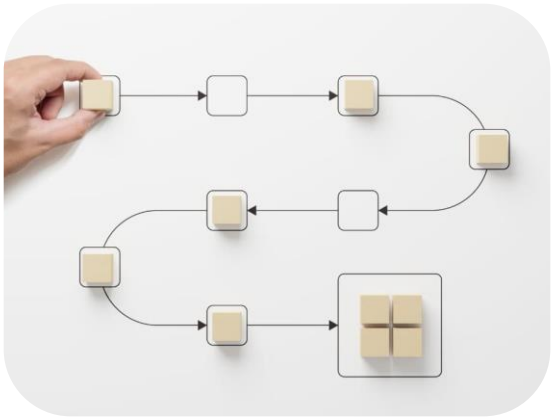
Detection and Initial Response	• **CISO:** ISO team detects the incident via security monitoring systems and immediately initiates the incident response plan. Together with the IT team, they block compromised accounts to prevent the attack from spreading. • **DPO:** DPO is informed of the incident and begins assessing the implications for data protection and regulatory compliance.
Impact Assessment	• **CISO:** Assesses the extent of the breach, identifies compromised systems and accounts, and affected data. Works with IT to understand how the attack occurred and how to remediate/ensure it doesn't happen again. • **DPO:** Assesses the risks to the rights and freedoms of individuals affected by the breach & consult the top management. Propose to the top management whether notification to data protection authorities and communication to affected individuals is necessary based on risk assessment
Notification and Communication	• **CISO:** Provides technical details about the incident and measures taken to contain it. Assists in preparing technical communications for internal stakeholders. • **DPO:** Notify to the CNPD and communicate to the person affected depending on the risk assessment validated by the top management
Lessons Learned	• Honest exchange between the CISO and DPO to analyse the incident management and discuss/document points for further improvement.

Example of DPO & CISO collaboration regarding a DPIA



Conclusion

Our collaboration is crucial for maintaining a robust data protection and security posture. By working together, we ensure that the University meets its legal obligations and protects the rights of individuals.



We continuously strive to improve our processes and stay ahead of emerging threats. This involves staying informed about the latest cybersecurity trends, GDPR guidance, conducting regular assessments, and implementing best practices.

Thank you for your attention. We are happy to answer any questions you may have.