AI, Data Protection & Quantum What We Must Pay Attention To

Alain Herrmann, Commissioner
Commission nationale pour la Protection des Données

Data Privacy Day 2026 | 28 January 2026

DATA PRIVACY DAY 2026

AI, Data Protection & Quantum: What We Must Pay Attention To

AI and quantum technologies are not just new tools; they are quietly reshaping the assumptions on which data protection has relied for decades.

Data Privacy Day 2026

A strategic perspective beyond compliance

Understanding deeper technological transformations

Reshaping the foundations of data protection

Introduction: Why This Discussion Matters

AI is already embedded in everyday operations, whilst quantum technologies are approaching faster than many organisations anticipate.

AI systems are now operational realities

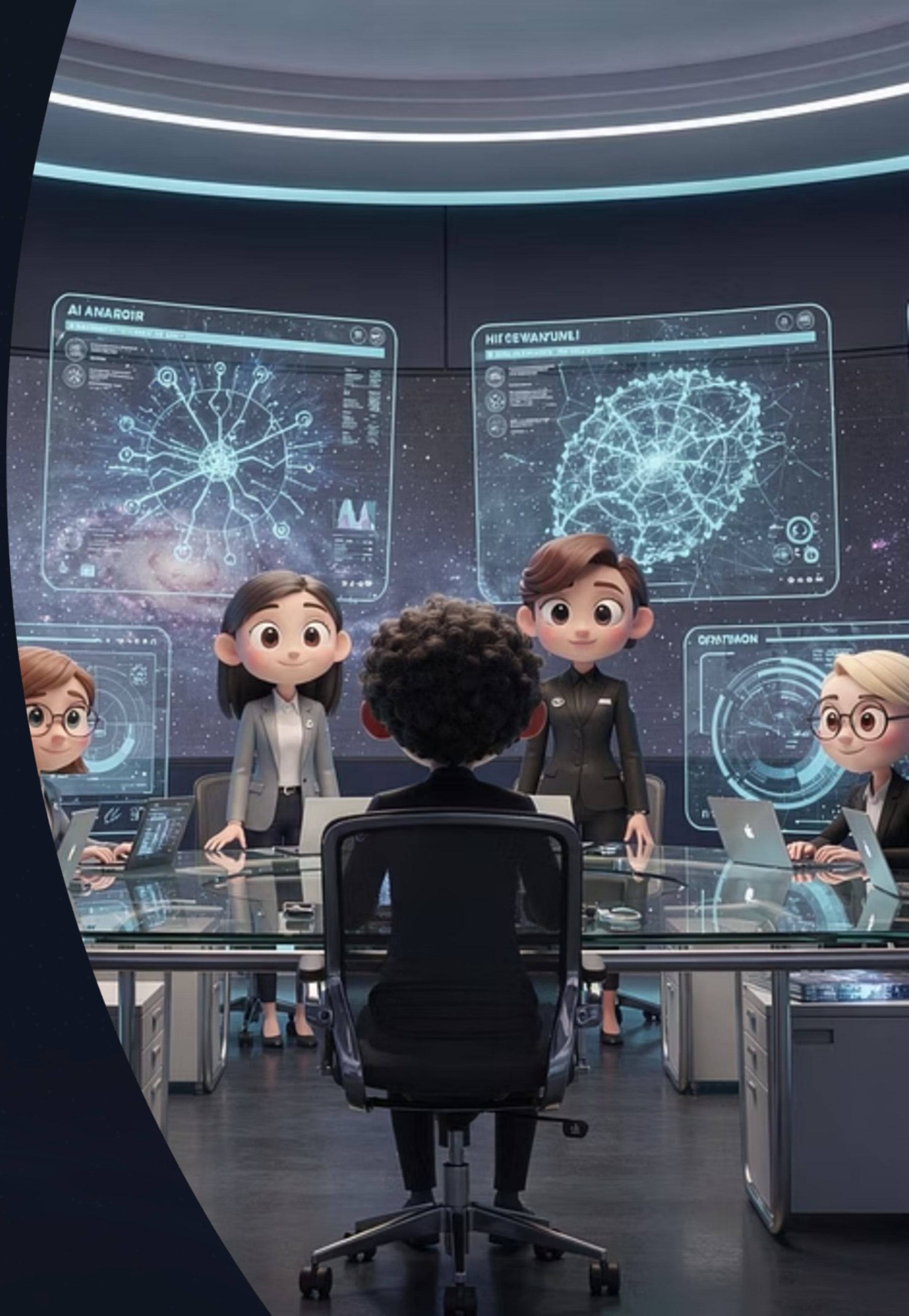
No longer emerging technology, but embedded infrastructure

Quantum computing challenges long-standing assumptions

Approaching faster than organisations anticipate

Core data-protection concepts are under pressure

Foundational principles require re-examination



Objective of This Talk

This presentation is not about listing obligations, but about identifying where attention, governance and anticipation must evolve.

Provide a clear sense of direction

Navigate the evolving landscape strategically

Highlight concrete points of attention

Focus on what truly matters

Share a supervisory authority's medium-term perspective

Forward-looking insights for decision-makers

Two Regulatory Frameworks, Two Distinct Logics

Organisations now operate under two major regulatory regimes that intersect, but do not overlap perfectly.

AI Act and GDPR apply simultaneously

Parallel regulatory obligations

Complementary objectives, different structures

Distinct but interconnected frameworks

Coherence is required to navigate both

Strategic alignment essential

GDPR vs AI Act: Different Foundations

The GDPR and the AI Act are built on different conceptual starting points.

GDPR

Personal data and risks to individuals

Roles: controller and processor

AI Act

AI systems and systemic risks

Roles: provider and deployer

A New Reality: Multiple Roles at the Same Time

The same organisation may hold several regulatory roles, often without fully realising it.

One organisation, multiple responsibilities

Navigating complex regulatory identities

Controller under GDPR, deployer under AI Act

Simultaneous obligations across frameworks

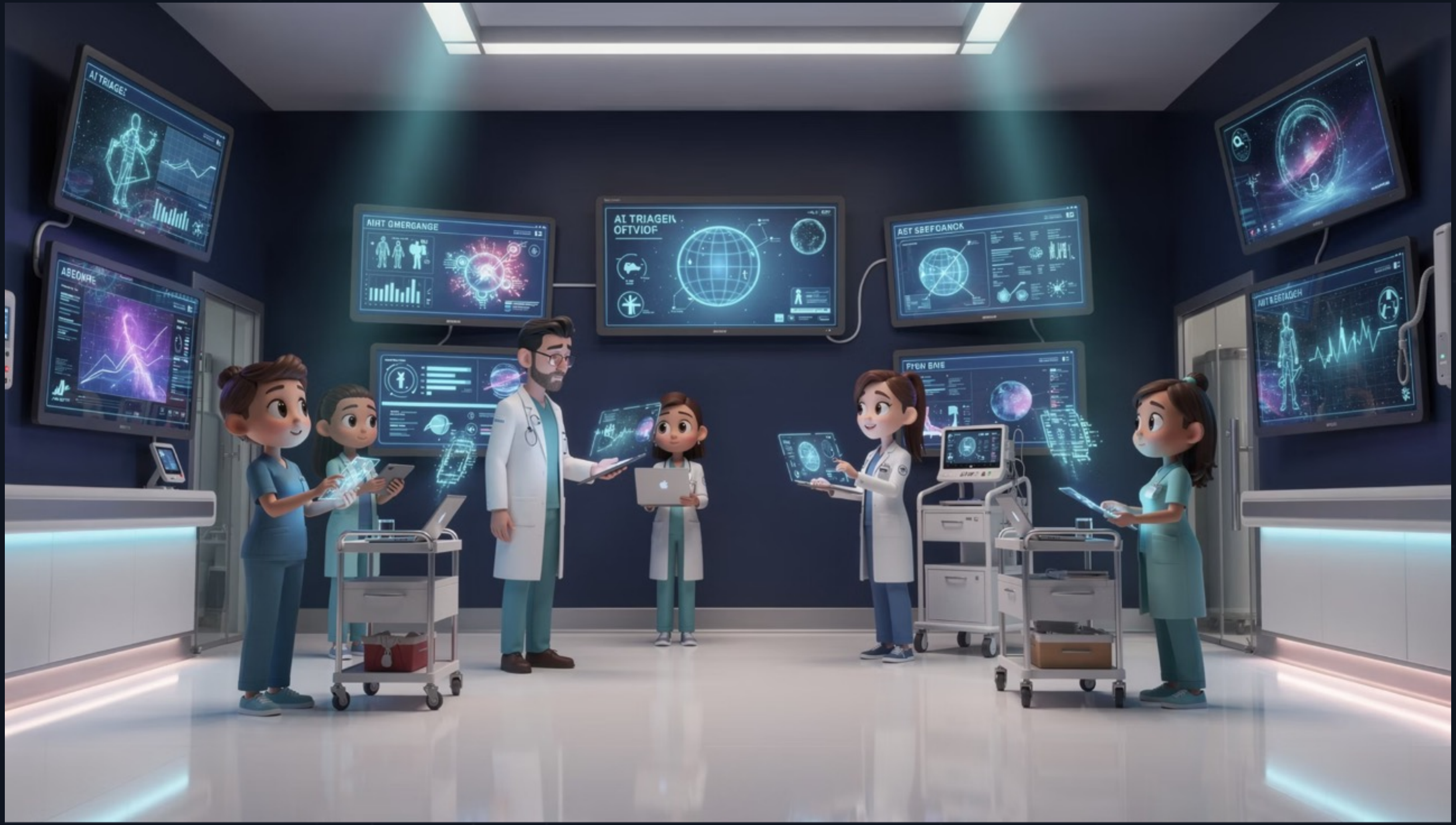
Accountability becomes fragmented

Clarity requires deliberate mapping

Case Study

Example: AI in a Public Hospital

A concrete example illustrates how complexity quickly arises in real-world deployments.



1

AI system used for emergency triage

Deployed in critical care environment

2

Hospital acts as controller and deployer

Multiple regulatory identities simultaneously

3

Third-party models and multiple data sources

Complex supply chain and data flows

4

Accountability is no longer straightforward

Requires careful governance mapping

Mapping Roles Is a Governance Issue

Correctly identifying roles is not a legal formality; it is a governance necessity.

Not a one-off classification exercise

Requires ongoing attention and review

A living process that evolves over time

Adapts as systems and contexts change

Poor mapping leads to unclear accountability

Creates gaps in responsibility and oversight

Compliance efforts become fragmented

Inefficiency and blind spots emerge

Strategic Risk

Beyond Compliance: Systemic Risks

Some of the most significant risks are not purely regulatory; they are systemic.

Risks extend beyond formal non-compliance

Broader societal and operational implications

AI can reproduce or amplify inequalities

Systemic bias embedded in systems

Effects often become visible only at scale

Emergent risks require anticipation

Observed Risks in Europe

These risks are not hypothetical; they are already visible in Europe.

Bias in employment and predictive policing

Documented cases across member states

Uneven performance across languages and cultures

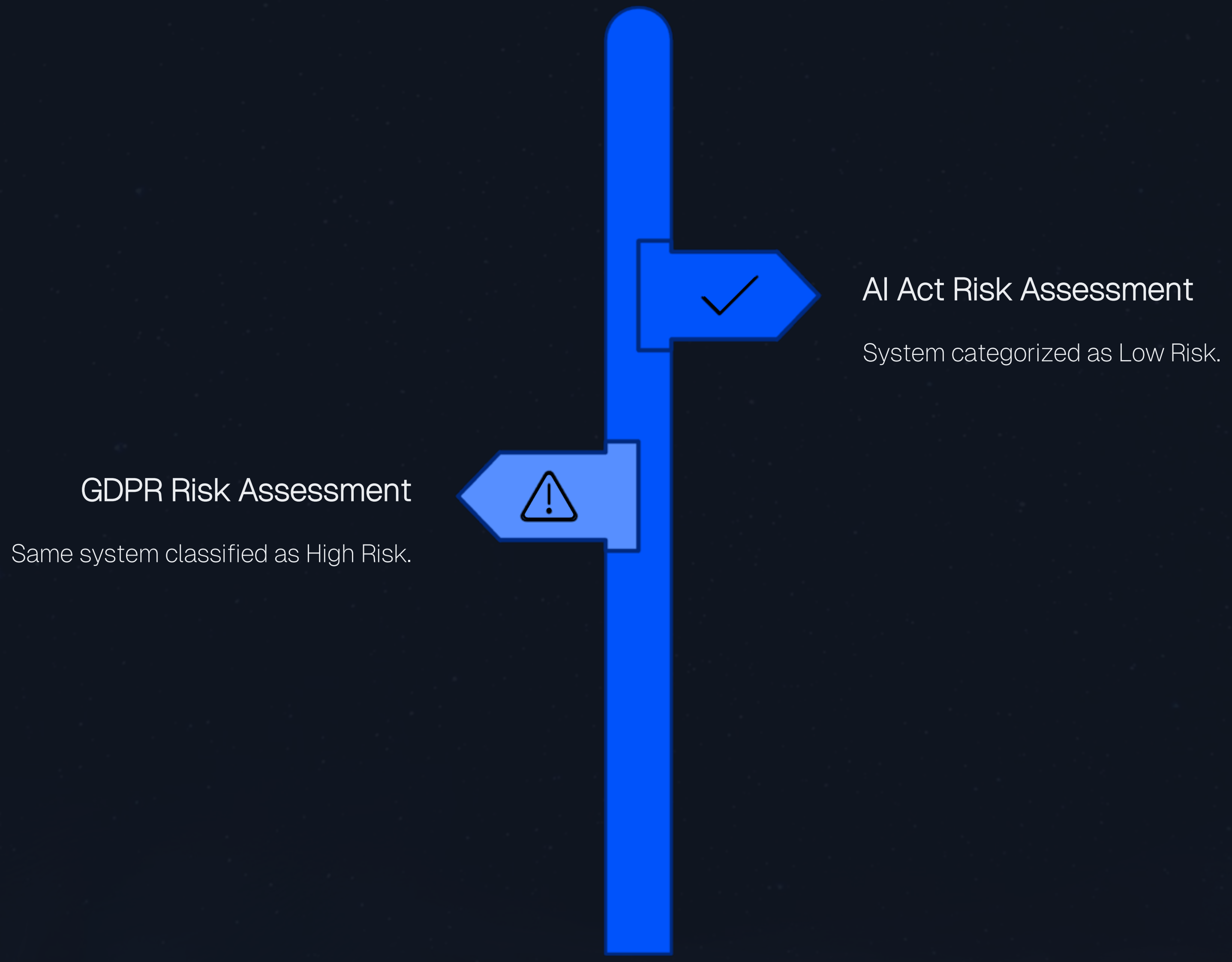
Disparate impact on different populations

Real systems using European data

Operational deployments with measurable effects

Risk Categorisation: A Potential Misalignment

Risk assessments under the AI Act and the GDPR do not always lead to the same conclusions.



✓ AI Act Risk Assessment

System categorized as Low Risk.

⚠ GDPR Risk Assessment

Same system classified as High Risk.

AI Act risk categories differ from GDPR assessments

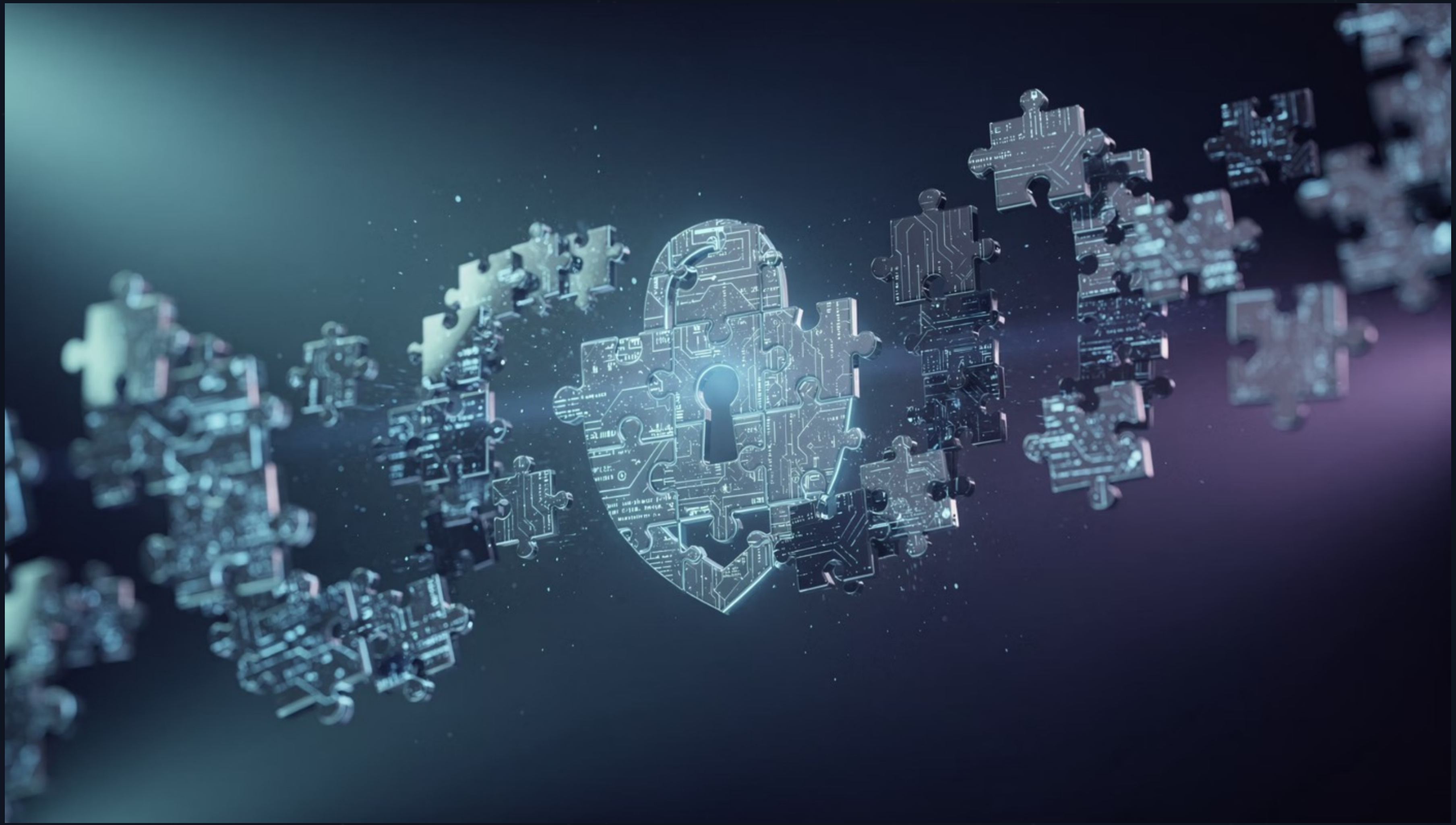
A system may be low-risk under the AI Act

Yet still high-risk under the GDPR

Technical Challenge

Inference and the Limits of Anonymisation

Modern AI systems can infer far more than what was explicitly collected.



Inference of data never directly provided

AI derives sensitive information from seemingly innocuous inputs

Mosaic effect challenges anonymisation

Combining datasets reveals identities

Risk depends on tools and auxiliary datasets

Context determines re-identification potential

Large Language Models: A New Risk Category

General-purpose AI systems introduce specific and documented data-protection risks.

1 **Possible memorisation of training data**

Models may retain and reproduce training examples

2 **Risk of regurgitating personal information**

Unintended disclosure through model outputs

3 **Membership inference attacks are feasible**

Adversaries can determine if data was used in training

Note: These are not theoretical concerns—they have been demonstrated in research and real-world deployments.

Looking Ahead

Quantum Technologies as a Stress Test

Quantum technologies challenge a silent pillar of data protection: trust in cryptography.

- Cryptographic assumptions may no longer hold

  Current encryption methods face quantum threats

- "Store now, decrypt later" is a real risk

  Today's encrypted data vulnerable to future quantum attacks

- Long-term confidentiality must be anticipated

  Strategic planning required now

- Trust will be a key digital asset

  Foundation of future data protection

The technologies reshaping data protection demand not alarm, but anticipation. The organisations that succeed will be those that recognise these shifts early, integrate governance thoughtfully, and build trust as a strategic capability.

Conclusion

After exploring regulatory evolutions, systemic risks and technological challenges, we return to essentials: trust and vigilance. Data protection and responsible adoption of AI and quantum technologies are long-term investments for our organisations and societies.

01

Synthesis

AI and quantum reshape the foundations of data protection.

02

Responsibility

Accurate role mapping and proactive risk anticipation are crucial.

03

Action

Implement integrated governance (GDPR + AI Act), strengthen DPIAs and build a culture of anticipation.

04

Vision

Digital trust will be the cornerstone of our economy—embrace these technologies while remaining rigorous on ethics and compliance.

The path forward requires vigilance, strategic thinking and a commitment to building systems worthy of public trust.

Alain Herrmann
Commissioner
CNPD
https://cnpd.lu