YOUR GDPR
COMPLIANCE
PARTNER

10th Anniversary MGSI

DPO & Controllers:
Clearing Misunderstandings for Optimal Compliance

Mélanie Gagnon, CIPP/E, CIPM, CISA
CEO, MGSI

DPO Forum Luxembourg
13 February 2025

www.mgsi.lu

Disclaimers

1. **Content**
   The information in this presentation reflects the opinions and experiences of multiple Data Protection Officers (DPOs) and does not exclusively represent MGSI's position. It is provided for informational purposes only and does not constitute official advices.

2. **Reproduction Prohibited**
   This presentation is protected by copyright. Any reproduction, commercial distribution or modification, in whole or in part, is strictly prohibited without prior written authorization from MGSI.

3. **Internal Use Permitted Under Conditions**
   This document may be used for internal purposes only, provided it remains intact, without modification or removal of MGSI logos, trademarks, or references.

4. **Legal Compliance Disclaimer**
   This presentation is provided for informational purposes only and does not replace legal consultation. Each organization is responsible for its own GDPR compliance and must conduct its own analyses and compliance efforts.

Privacy Landscape 2025

Recent survey – Key Findings from ISACA

🔴 **45%** believe privacy budget is underfunded (up from **41**% in 2024).

🔻 **54%** expect privacy budgets to decrease further in 2025

🔐 **Only 38%** are confident in their organisation's ability to safeguard sensitive data.

⚠️ **Only 24%** of organisations always practice Privacy by Design.

Source: ISACA, January 2025
Press Releases 2025 Privacy budgets set to decrease in 2025 new research from ISACA reveals

Regulatory Overload: Building on a Fragile GDPR Foundation

NIS2

DORA

AI Act

Controllers' Facing Difficult Decisions

- How to do more with less?
- Compliance cuts: which block will make it collapse?

Changes are mandatory!

What key changes?

Demystify DPO's role: A Compliance Partner, Not a Barrier

Planning & workload management

Assess tools: avoid "100% GDPR compliant" myths.

Repeating the same approach will lead to failure. Change is not optional.

DPOs: The Most Misunderstood Role in Compliance!

How some people see the DPO…

- DPOs don't wake up thinking, "How can I ruin a project today?"
- DPOs are not evil… they don't punish controllers!

No DPO enjoys announcing bad news.

- They prefer early involvement to help mitigate risks **before** they escalate into crises.

DPOs: The Most Misunderstood Role in Compliance!

Common Reactions to the DPO:

- *We need to **move fast—no time** for compliance!*
- *"The DPO is **slowing us down**."*
- *DPOs are just **obstacles** to innovation.*
- *"No time, **we'll take the risk**."*
- *"The DPO is **not on our side**—let's not inform her/him."*

DPOs: The Most Misunderstood Role in Compliance!

Impacts & Risks

- Teams that don’t understand or take the DPO’s role seriously and keep postponing meetings
- They don’t have time or won’t make time for compliance.
- DPOs are often pressured to put business interests before compliance.
- Some companies appoint a DPO just to "tick the box" rather than empower the DPO to drive compliance.
- Without early involvement, the DPO spends time fixing problems rather than preventing them.

DPOs are no Harry Potter, they don’t have magic wands—if you involve them too late, compliance disasters are almost inevitable.

DPOs: The Most Misunderstood Role in Compliance!

Actual Role of the DPO

Article 39 : Tasks of the DPO (among others)

- To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR.
- To monitor compliance with GDPR.

- Beyond audits, the DPO serves as a compliance facilitator, risk advisor, and strategic guide—helping businesses navigate GDPR challenges proactively.
- The DPO provides guidance, not guarantees—compliance remains the controller's responsibility!

DPOs: The Most Misunderstood Role in Compliance!

Possible Solutions ➢ Actions from the DPO's side

Attitude of the DPO

- Own their role—compliance leadership requires confidence.
- DPO is not Designated Pleasing Officer!
- The DPO is not here to please everyone —her/his job is to ensure compliance, not win popularity contests.
- Be consistent and unwavering in compliance recommendations.
- Stay firm—compliance is not optional, even when unpopular.

DPOs: The Most Misunderstood Role in Compliance!

Possible Solutions? ➢ Actions from the DPO's side

What should the Controller expect from the DPO? (Article 39)

- Loyalty – The DPO is a compliance ally, not a whistleblower. Their role is to inform, to conduct audit, to guide, not punish.
- The Hard Truth – The DPO must provide an honest and objective assessment of compliance risks.

More importantly… Compliance is a two-way street—what do DPOs need from Controllers?"

DPOs: The Most Misunderstood Role in Compliance!

Possible Solutions ➢ Actions from the Controller's side

1) **Shifting the controller's mindset**: from seeing the **DPO** as a regulatory burden to recognizing them as a **strategic ally**.

The way the entire company perceives the DPO is directly shaped by the Controller's vision and actions!

While compliance is the Controller's responsibility, their approach and decisions have a direct impact on the DPO's ability to fulfill their role effectively. **A Controller who actively engages with the DPO** and takes informed actions not only facilitates their collaboration but also **reinforces the company's overall GDPR compliance.**

DPOs: The Most Misunderstood Role in Compliance!

Possible Solutions ➢ Actions from the Controller's side

2) **Respect and Empower the DPO's Position. Controllers and processors must:**

- **Support** the DPO in performing their tasks.
- **Involve the DPO** properly and in a timely manner in all personal data protection issues.
- **Ensure independence:** the DPO must not receive any instructions regarding the performance of those tasks.

DPOs: The Most Misunderstood Role in Compliance!

Possible Solutions ➢ Actions from the Controller's side

COMMUNICATION IS THE KEY!

Without top-level endorsement, teams and management will inevitably see DPOs as an obstacle.

1) **Establish clear communication and messaging across the company**
   - **Privacy is a priority in this company.**
2) **Notify all employees when a new DPO is appointed or remind them of the DPO's role**
   - The DPO will contact teams regarding specific compliance matters.
   - It is crucial to respond promptly.
   - If the DPO requests a meeting, it is important to attend.

DPOs: The Most Misunderstood Role in Compliance!

Key Takeaway:

Compliance is a shared responsibility, not just the DPO's burden.

Clear communication and proactive engagement from controllers ensure smoother processes and reduce regulatory risks.

- The DPO is **not the enemy**—they are a strategic ally in building a **compliant and sustainable business.**
- **Involve them early, communicate their role clearly, and integrate compliance into business strategy.**

Planning & Workload Management

Current Situation

- Business most probably won't **increase their budgets for privacy**
- The same expectations are **placed on the DPO, but with a reduced budget**

Problem: Overloading Compliance Resources

- Launch of multiple projects simultaneously - while the DPO is only appointed for one or two days a week (or even less), internal teams struggle to keep up.
- From a business perspective, this may seem efficient; however, from a compliance standpoint, it significantly increases risk.

Key Risks of Overloading the DPO

- Critical privacy reviews get rushed or skipped.
- DPIAs are often delayed or poorly executed.

Planning & Workload Management

Possible Solutions: Smart Planning & Risk Anticipation

- Align compliance efforts with project timelines: Ensure the DPO has sufficient time to provide meaningful input.
- Prioritize high-risk projects to allocate resources efficiently.
- Share the list of upcoming projects early with the DPO.
- Identify high-risk projects, especially those requiring a DPIA, before critical development stages.

Key Message:

Efficient project planning is not just a business priority—it's a compliance necessity.

Processors claiming their tool is… GDPR Compliant. Or even better… 100% GDPR Compliant?

Myth or Reality?

—

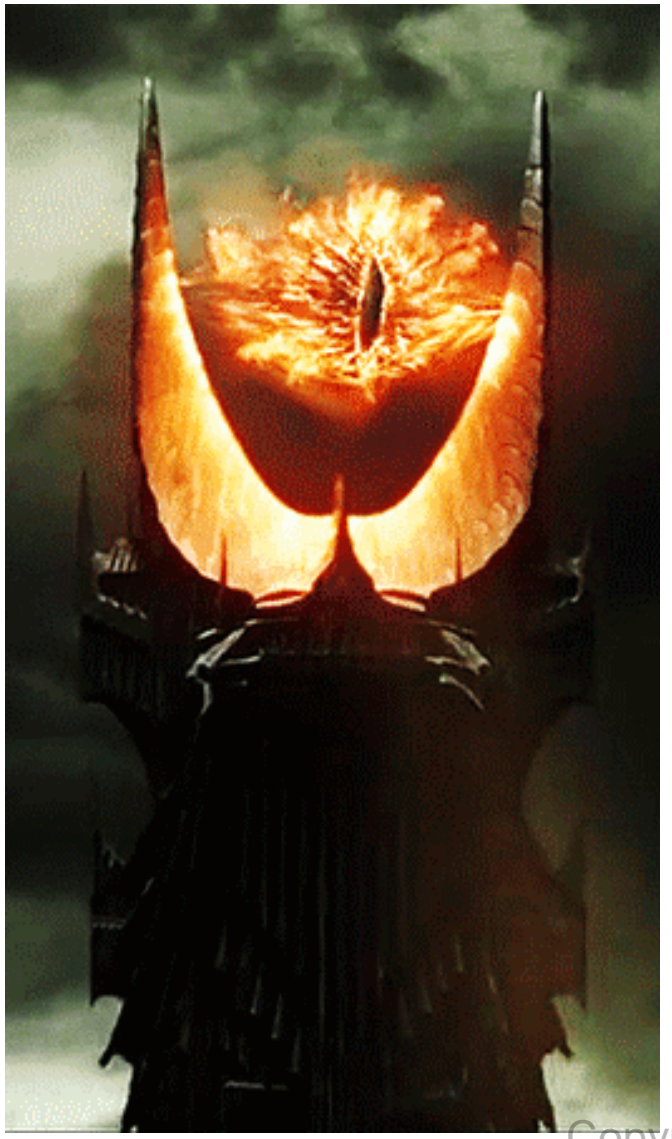
HOW

Developer or processor see their tool

100% GDPR Compliant Tool? Really?

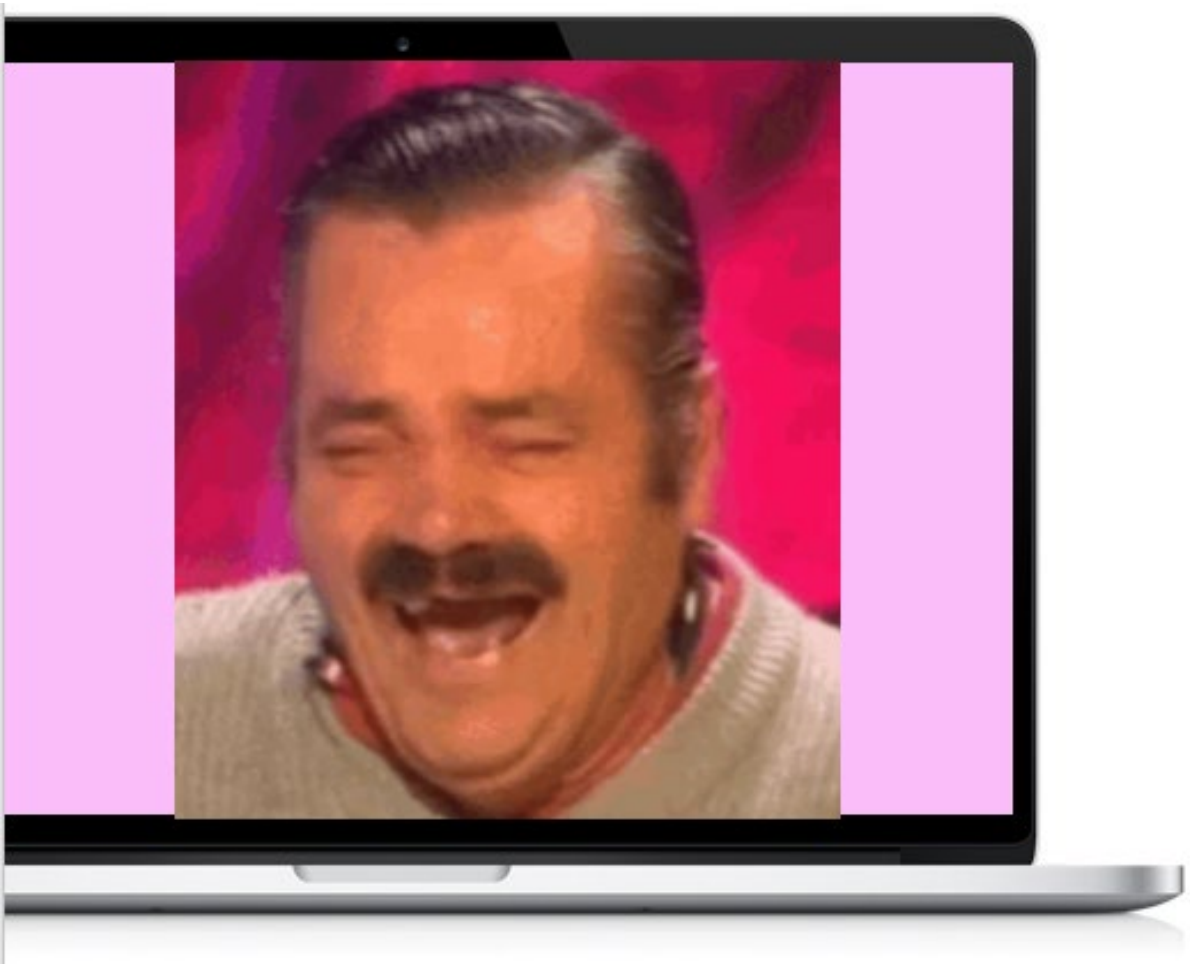
HOW Controllers see the tool

100% GDPR Compliant Tool? Really?



HOW
The CNPD sees the tool

100% GDPR Compliant Tool? Really?



HOW
DPOs see
the tool

100% GDPR Compliant Tool? Not That Simple!
The Tool Helps, But Compliance Rest with the Controller!

100% GDPR compliant… Even if that is true… who knows ☺

- **One thing is for sure: it is not the tool that is compliant. The tool is designed to help the controller meet the GDPR requirements (security, access rights, data minimization, masking data, data subject's rights, etc.)**

- **The Controller remains fully responsible for ensuring GDPR compliance when using the tool.**
- Key legal obligations include:
  - **Article 5(2) & 24(1) GDPR** – Compliance demonstration & technical/organizational measures.
  - **Article 25 GDPR** – Privacy by design & default
  - **Article 28 GDPR** – Data Processing Agreement (DPA) required.
  - **Article 32 GDPR** – IT-security risk assessment.
  - **Article 35 (DPIA)**
    - The tool's **DPIA** only covers the tool itself, not its implementation.
    - **The Controller must conduct its own DPIA** to assess risks and ensure compliance

Conclusion – Key Takeaways

01 The DPO is a strategic ally, not a regulatory burden.

02 Privacy budgets are shrinking, yet compliance requirements are increasing.

03 Misconceptions about the DPO's role lead to inefficient processes and compliance risks.

04 Overloading the DPO results in rushed privacy reviews, skipped DPIAs, and potential regulatory penalties.

05 Tools claiming 100% GDPR compliance do not absolve controllers from their legal obligations

Conclusion – Key Recommendations

- **Early Involvement of the DPO:** Integrate them at the beginning of projects to anticipate compliance risks.
- **Strategic Workload Planning:** Align compliance efforts with project timelines to avoid bottlenecks.
- **Controller Accountability:** Remember that GDPR compliance remains the responsibility of the controller, not the tool.
- **Clear Internal Communication:** Reinforce the DPO's role and encourage teams to engage proactively.
- **Proper Resource Allocation:** Ensure sufficient budget and staffing for privacy and compliance teams.

A well-supported DPO is essential to proactive compliance and building a culture of privacy and security.

YOUR GDPR COMPLIANCE PARTNER

Have questions?

Need GDPR expertise?

We're here to help!

📩 Contact: Mélanie Gagnon, CIPP/E, CIPM, CISA
📧 Email: melanie.gagnon@mgsi.lu
📞 Phone: +352 28 89 27 00
🌐 Website: www.mgsi.lu
🔗 LinkedIn MGSI
🔗 LinkedIn Mélanie Gagnon

10th Anniversary MGSI

YOUR GDPR COMPLIANCE PARTNER

Simplify your compliance with tailored support!

Happy Anniversary MGSI!

Celebrating 10 years of expertise in data protection & information security!

OUR SERVICES

- GDPR Compliance Audit
- External DPO
- Governance & Operational Support
- Compliance in Projects (Privacy by Design)
- DPIA Implementation
- Security & Risk Management
- IAPP Certification (AIGP, CIPP/E, CIPM) & GDPR Training