

The Data Privacy Chronicle

Edition # 1 - AI Governance starts with data protection and your DPO

The Data Privacy Chronicle is a sequence of pragmatic newsletters mainly designed for Data Protection Officer (“DPOs”), privacy leaders and their respective organisations. The aim is simple: to provide you with practical insights, powered by our experience as data protection lawyers and DPO-as-a-Service providers, on emerging topics that shape your role and to help you navigate the growing complexity of regulatory frameworks in the digital era.

Our first edition tackles a very “trendy” topic: **AI Governance and the DPO’s role.**

1. Introduction

AI tools are already here. Whether through recruitment platforms screening CVs, customer service chatbots, fraud detection systems or internal analytics dashboards, most organisations in Luxembourg and abroad are already relying on Artificial Intelligence (“AI”) in one way or another. Very often, these tools are adopted quickly – but questions remain: *is your AI Governance ready? and do you have a full grasp of the legal and regulatory aspects at hand?*

The timing of this chronicle could not be more relevant:

- The EU AI Act has been adopted and is continuing to gradually apply over the coming months. It introduces a risk-based regulatory framework, classifying AI systems according to their potential impact (from minimal risk to unacceptable risk).
- While waiting for its full application, the GDPR remains more relevant than ever. Indeed, many of the AI-related issues (from defining a lawful basis for the processing of personal data, to respecting principles of minimisation and transparency) are already covered by GDPR obligations, which were deliberately designed to be technology-neutral.

For DPOs and privacy leaders, this means that *your role is already central in AI projects*. Beyond ensuring compliance, you are expected (or at least should be expected) to act as a strategic partner, guiding your organisation to use AI responsibly while avoiding legal, ethical, and reputational pitfalls.

2. Benefits of AI design and use

When discussing AI, risks often dominate the (legal) conversation. Yet, for organisations operating in Luxembourg and beyond, the potential benefits of AI are real. Properly designed and implemented, AI systems and AI agents can bring significant advantages in terms of data management and actually strengthen compliance frameworks, hence supporting the DPO's mission (regardless of the improvement of products and/or services).

For instance, AI can enhance data security by identifying unusual patterns and detecting anomalies that might otherwise go unnoticed, allowing companies to anticipate potential data breaches before they escalate. It also offers the ability to process large volumes of structured and unstructured data at speeds that no human team could ever match, an invaluable asset for sectors like financial services, healthcare, or retail.

When deployed responsibly, AI may even contribute to better data governance. Automated classification and organisation of personal data can facilitate accuracy and minimisation, two GDPR principles that are notoriously challenging.

Similarly, AI can provide strategic insights to organisations with strong governance, helping to anticipate compliance risks or operational inefficiencies. In this context, risk management ceases to be a mere "box-ticking" exercise and instead becomes a genuine driver of resilience and trust.

In other words, when designed responsibly and under close supervision, AI can be a valuable ally to the DPO and privacy experts within companies. But these benefits must always be weighed against the inherent challenges, which will be explored in the next section.

3. Challenges of AI design and use

While the benefits of Artificial Intelligence are obvious, the challenges are equally significant. For DPOs, they translate into daily issues on how to balance innovation with compliance and risks, and how to make sure that the promises of AI do not evolve into legal or reputational threats for the organisation.

AI systems are, at their core, tools built on algorithms and data. This means they inevitably carry inherent limitations: biases in training sets, hallucinations, or misinterpretations of context. A system that performs well in one environment can fail dramatically in another, simply because it cannot grasp sector-specific nuances or company-specific realities, hence human supervision remains essential.

The reliance of AI on large datasets also poses complex challenges. High-performing models often require significant volumes of personal data, raising immediate concerns under the GDPR: which lawful basis applies, how minimisation can be respected in practice, and how long training data may be retained. These questions are not theoretical because they lie at the heart of AI deployment and can expose organisations to regulatory scrutiny.

Moreover, the underlying data is often processed and/or hosted abroad, potentially triggering the application of foreign (and potentially contradicting) laws, in particular when regulatory obligations apply such as for the banking and insurance sectors with strict professional secrecy requirements.

Transparency is another weak point. Many AI systems, especially generative ones, operate as black boxes. Explaining to individuals how their data is used, or how a specific output was generated, is often impossible in practice, resulting in potential opacity claims and trust issues.

Generative AI often produces outputs in a polished and convincing style, even when factually inaccurate. This creates a false sense of certainty and can lead to premature reliance on the system without adequate human oversight, potentially generating significant liability in case of material error

Focus: accountability and documentation

For DPOs and privacy experts, one recurring theme is *accountability*. Even if the AI Act introduces new obligations, GDPR principles remain fully relevant today. This means that organisations must document:

- which AI tools are being used or developed;
- what (personal) data they rely on;
- the legal basis for processing such data;
- the safeguards applied (pseudonymisation, encryption, access restrictions);
- and how risks have been assessed and mitigated.

This documentation is not just a compliance exercise. It is a practical way to create traceability, facilitate internal and external communication, and build trust with regulators, clients, and employees.

4. Recommendations for organisations and their DPOs / privacy leaders

So how can organisations and DPOs move from identifying risks to actively managing them?

We believe that the key is to adopt a structured approach, ensuring that AI projects are not only innovative but also compliant and trustworthy. Below are practical recommendations and a checklist for the organisations and their DPOs to consider, based on our own experience.

DPO Checklist

1. Be a pragmatic enabler

Position yourself at the start of every AI initiative. Whether it is the adoption of an external tool or the development of an in-house model, the DPO must be at the table early to influence design choices and avoid costly retrofits. The key is to draw a balance between regulatory obligations and business interests so that the organisation can take informed decisions.

2. Strengthen AI literacy

The AI Act formally requires organisations to promote “AI literacy” among internal staff (including C-levels) and any other relevant person (customers, service providers, etc). The training must build on both the potential and the risks of AI. The DPO is usually perfectly positioned to act as a bridge, ensuring that key considerations (including those related to data protection) are included in all training modules.

3. Map and document AI use and risks

Maintain a clear inventory of AI tools and projects within your organisation. For each system, document:

- its purpose and scope;
- the type of (personal) data it processes;
- the legal basis;
- retention policies;
- any vendor dependencies.

Identify specific risks as well and document how you handle them.

This mapping and documentation will serve as your accountability backbone.

4. Vendor management

Many organisations will rely on external providers for AI solutions. DPOs should:

- assess vendors before procurement (due diligence);
- review contractual clauses (data use, transparency obligations, audit rights, liability allocation, international data transfer and potential consequences);
- ensure ongoing monitoring of compliance.

5. Draft internal AI policies

It is essential for organisations to adopt internal policies on AI use. These should define acceptable uses, review processes, documentation requirements, and escalation mechanisms. They will also serve as a reference point for staff.

6. Review and update regularly

AI projects evolve quickly. Schedule regular reviews (technical, legal, and organisational) to assess changes, retrain models if necessary, and update documentation. This continuous monitoring is essential to remain aligned with applicable legislation.

By following these steps, DPOs can help their organisations embrace AI responsibly, while protecting individuals' rights and reducing regulatory and reputational risks.

5. Conclusion

AI is not just a buzzword, it is already reshaping how organisations (and users) operate. While its promises are significant, its challenges are equally real. For companies, the difference between an AI project that creates value and one that creates liability often comes down to one element: governance.

Based on our experience, a proper governance often starts with key actors, including DPOs and privacy leaders, who will make sure that awareness is raised about risks, suggest ways to lower them, ensuring compliance with existing rules and promoting a culture of accountability. By positioning yourself as an early player and enabler in AI projects, you can help your organisation strike the right balance between innovation and trust.

The road ahead is complex due to the numerous EU regulations already in force. Preparing now is therefore not optional but rather a strategic necessity to remain relevant today and in the long run.

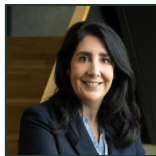
HOW WE CAN HELP

At **Stellan Partners**, our Technologies, Data & IP team assists clients in navigating these challenges by:

- Acting as **external DPO** or supporting the existing DPO with AI-related projects;
- Drafting or reviewing **AI governance policies** and contractual frameworks with vendors;
- Helping to **identify, assess and document risks** while also helping to mitigate them by implementing recommended measures (technical, organisational and contractual measures);
- Providing **training and workshops** on AI and data protection (including to meet AI Literacy requirements);
- Guiding organisations through **compliance checks** and documentation requirements.

If you would like to discuss how AI (and related legislation) may impact your organisation and what steps you should take now, contact us.

Please contact the members of our Technologies, Data & IP team should you need any assistance.



Audrey Rustichelli

Deputy Managing Partner

New Technologies, Data & IP

audrey.rustichelli@stellanpartners.lu

T: +352 661 463 238

This newsletter has been prepared by Stellan Partners for general guidance only. Although the greatest care has been taken to ensure that the information contained therein are accurate on the date of publication, Stellan Partners does not accept any liability to any person for the information (or the use or reliance upon such information) which is provided in this handbook or incorporated into it by reference. On any specific matter, please contact us for appropriate advice. The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.