dastra

What data protection did teach us about AI governance

DPO Forum
2nd of October 2025
Brussels

Welcome

Paul-Emmanuel Bidault

Co-founder & CEO of Dastra, data privacy & AI governance platform

Expertise in personal data governance software

Experience in data governance and risk management consulting

dastra

AGENDA

01 Introduction & context

02 What data protection did teach us

03 What data protection did NOT teach us

04 Example: a “DPIA-like” for an LLM

dastra

Data Protection and AI Governance

Data is today the fuel of AI: if poorly protected, it exposes us; if of poor quality, it is costly; if well governed, it becomes the best lever to reduce costs and secure controls!

A CHALLENGE…

Data protection is a critical issue:

- Data volumes are exploding: transactions, controlled documents, ESG data, IT logs, third-party reports, etc.
- Data quality is often insufficient: duplicates, incomplete documents, non-standardized data, etc.
- The risk of sanctions for incomplete or biased data exists and is growing with new regulations and obligations (such as the AI Act).

… AND A LEVER

Among the most frequently identified use cases:

- Process automation (especially for controls)
- Contract analysis (compliance gaps)
- Regulatory monitoring
- Risk forecasting/prevention (e.g., fraud patterns or deviant behavior)
- Setting up a chatbot (a dynamic knowledge base that “thinks”)
- Risk scoring for third-party due diligence

dastra

The Major Challenges for DPOs

Data Protection Officers face several key challenges that are reshaping their practices and internal positioning:

A COMPLEX AND VARIED FIELD	A CONSTANT RISK TO SECURE	THE NEED FOR URGENCY	NOT SLOWING DOWN THE BUSINESS
Regulations are becoming increasingly demanding and cover an ever-wider range of topics: data compliance, customer protection, cybersecurity, AI, anti-money laundering, and even sustainable finance.	The maturity of certain technologies and their growing use expose organizations to increasing cyber and fraud risks.	Regulations evolve very quickly, requiring an almost instantaneous capacity to adapt.	Controls must not overburden business processes or harm the customer experience.

To best address these major challenges, the Data Protection Officers we meet are facing a need for transformation that integrates organizational, process, tooling, and skills dimensions.

dastra

Why AI Governance Now?

Widespread adoption, diffuse risks, *and the binding timeline of* ***the AI Act,*** *with obligations phased in through 2026.*

May 2024
Official approval

Q3 2024
Entry into force

Q1 2025
- **Prohibited AI practices**
- **AI literacy requirements**

Q3 2025
New GPAI (General-Purpose AI) models

Q3 2026
General Date of Application
- **AI systems with transparency-related risks**
- **New high-risk AI systems listed in Annex III**
- **Existing high-risk AI systems listed in Annex III** that are significantly modified after the general application date (Q3 2026)

Q3 2027
GPAI models placed on the market before the 12-month implementation period (Q3 2025)

Q3 2027
- **New high-risk AI systems listed in Annex I**
- **Existing high-risk AI systems listed in Annex I** that have undergone significant modifications after the general application date (Q3 2026)

Q3 2030
High-risk AI systems used by public authorities, placed on the market before the general application date (Q3 2026) and not significantly modified

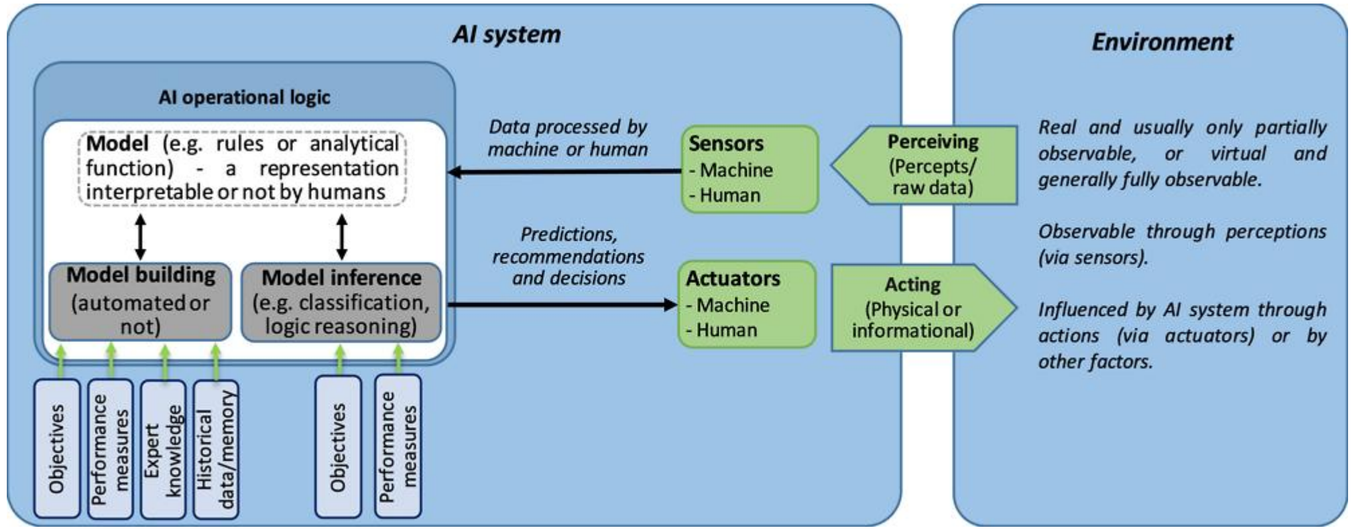
End of 2030
- **AI systems** that are components of a **large-scale IT system** as defined in Annex X, deployed within 36 months following entry into force (Q3 2027)

dastra

What is an AI system?

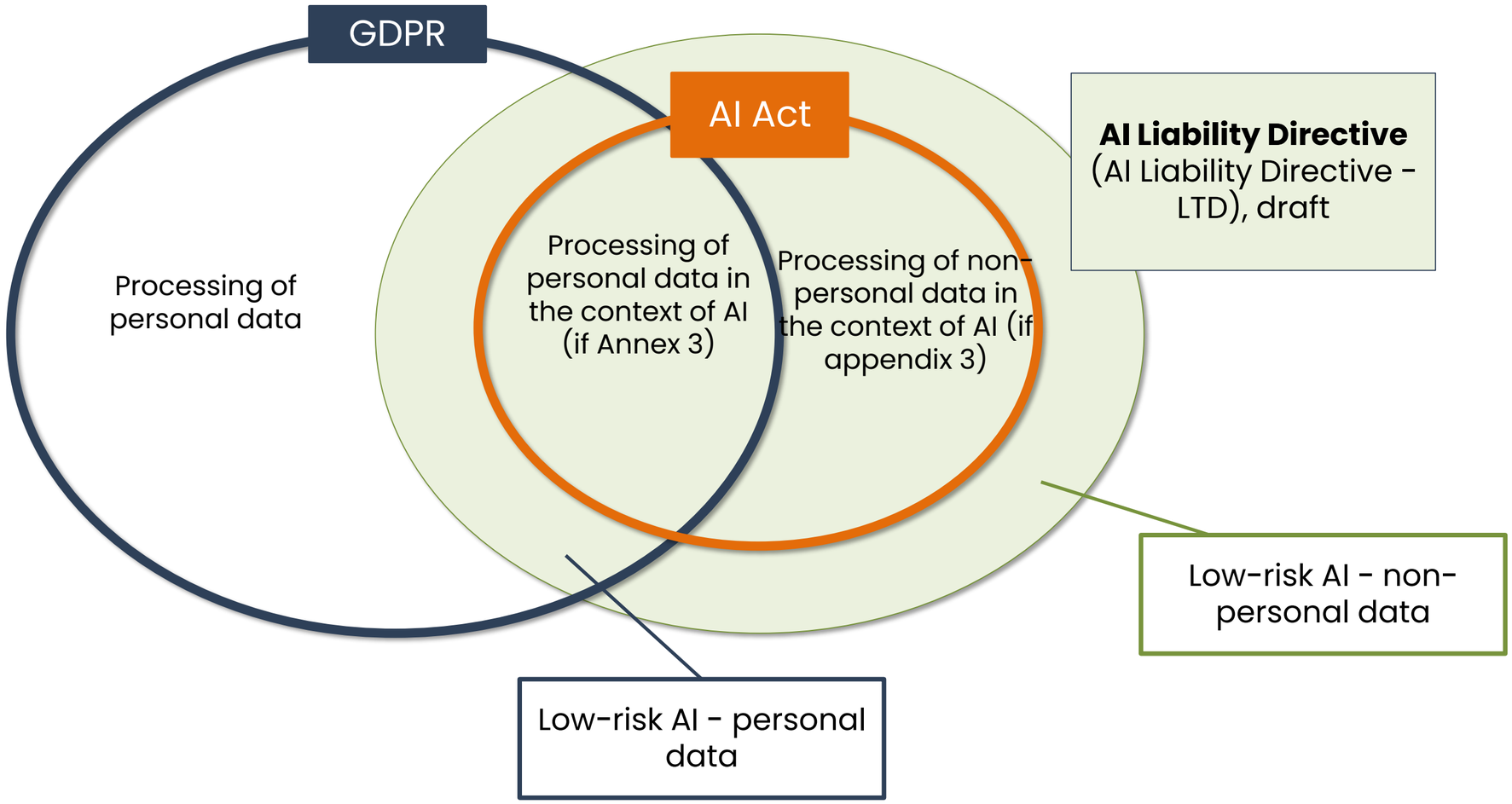
> *An **automated system** that is designed to operate at different levels of autonomy and can demonstrate adaptability after deployment, and **which**, for explicit or implicit purposes, **infers** from the inputs it receives **how to generate outputs** such as predictions, content, recommendations or decisions that can influence physical or virtual environments.*

Ex. A credit scoring system, autonomous driving system…



Conceptual view of an AI System
Source: OECD

Link between GDPR & AI Act (1/2)



+ Other laws containing provisions specific to AI :

- Data Services Act (DSA)
- Product Liability Directive (PLD)
- Unfair Commercial Practices Directive (UCPD)
- Platform Work Directive (brouillon)

Link between GDPR & AI Act (2/2)

ARTICLE 22 GDPR

Decisions producing legal effects or affecting an individual in a similar and significant way

Personal data + automated decision making (ADM) only

Personal data + AI + ADM only

Personal and non-personal data + AI to make recommendations or predictions

AI ACT – Appendix III

AI systems presenting a health and safety risk or a risk of negative impact on fundamental rights

High-risk AI:

- AI used as a product security component
- Real-time biometric authentication
- Critical infrastructures
- Access to education
- Recruitment, promotion and dismissal decisions
- Access to essential services
- Law enforcement, immigration, justice, asylum

Decisions Producing Legal Effects	• Decisions affecting the legal status of individuals • Decisions affecting accrued legal entitlements of a person • Decisions affecting legal rights of individuals • Decisions affecting public rights — e.g., liberty, citizenship, social security • Decisions affecting an individual's contractual rights • Decisions affecting a person's private rights of ownership
Decisions Producing Similarly Significant Effects *Some of these examples may also fall within the category of legal effects depending on the applicable legal regime and the specific decision in question*	• Decisions affecting an individual's eligibility and access to essential services — e.g., health, education, banking, insurance • Decisions affecting a person's admission to a country, their citizenship, residence or immigration status • Decisions affecting school and university admissions • Decisions based on educational or other test scoring – e.g., university admissions, employment aptitudes • Decision to categorise an individual in a certain tax bracket or apply tax deductions • Decision to promote or pay a bonus to an individual • Decisions affecting an individual's access to energy services and determination of tariffs

DPO FORUM dastra

AGENDA

01 Introduction & context

02 What data protection did teach us for AI governance

03 What data protection did NOT teach us for AI governance

04 Example: a “DPIA-like” for an LLM

dastra

What Data Protection Has Taught Us in 4 Dimensions

What privacy has taught us can be broken down into 4 key dimensions that we can now apply to AI:

Principles

- What it is: Values & guiding rules.
- Examples (privacy): Transparency, minimization, accountability, by design.
- To retain for AI: AI by design, explainability, usage boundaries.

Organization

- What it is: Roles, responsibilities, governance.
- Examples (privacy): Controller/Processor, DPO, sponsors.
- To retain for AI: Cross-functional governance, model/data owners, AI lead.

Processes

- What it is: Workflows & repeatable decisions.
- Examples (privacy): Records, DPIAs, incident management.
- To retain for AI: System mapping, risk assessments, continuous monitoring.

Tooling

- What it is: Artifacts & tools to act and demonstrate compliance.
- Examples (privacy): Records, DPIA templates, rights management portals.
- To retain for AI: AI register, model/data cards, test benches, logs & dashboards.

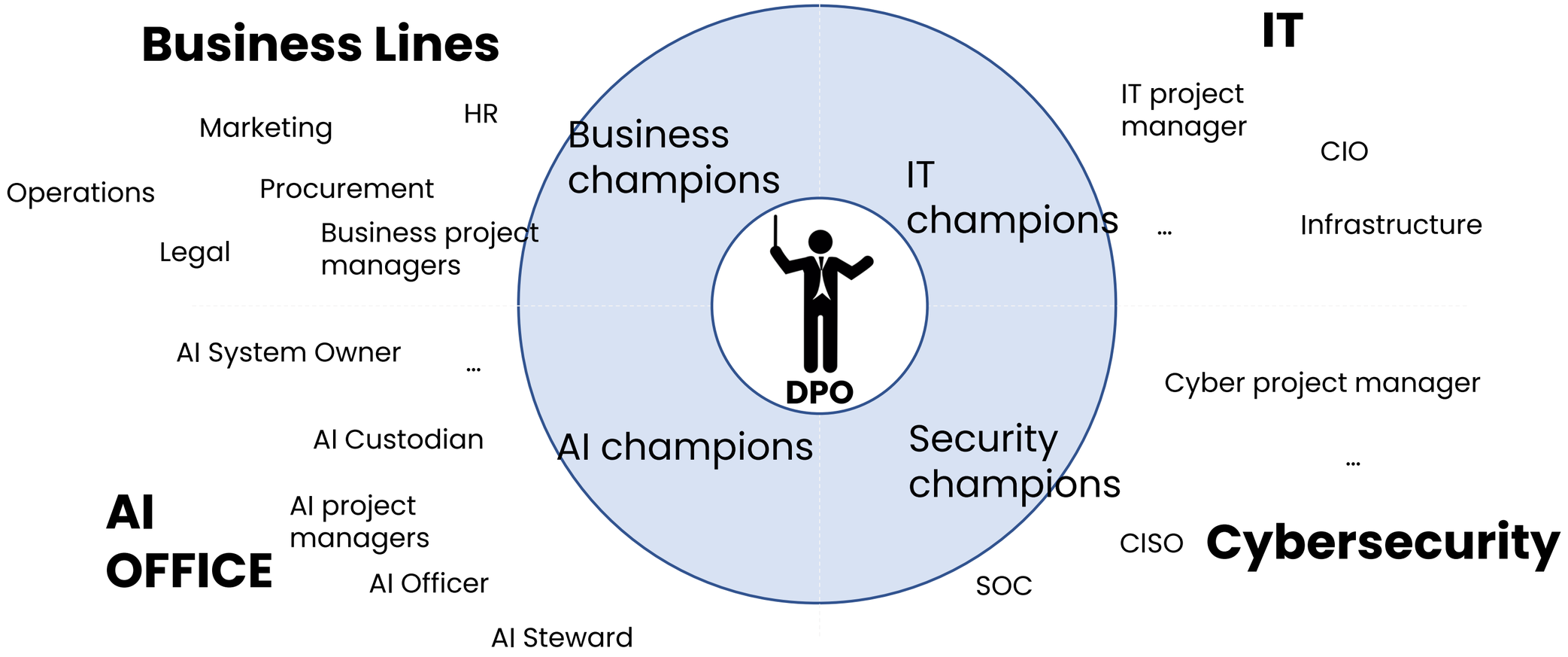
dastra

Principles: GDPR, Useful Reflexes for the AI Act

GDPR Principles		AI Act Principles
Transparency		Clear notices for AI (usage, limitations, contacts).
Minimization / Purpose limitation		Data & model capabilities limited to the intended purpose.
Accountability	⇔	*Evidence by default* (proof of choices, tests, trade-offs).
Privacy by design		AI by design: controls integrated from the start (HITL, safeguards, red teaming).
Security & Quality		Dataset traceability, version governance, bias/error review.
Risk-based approach		Classification of AI systems: prohibited, high-risk, limited, minimal.

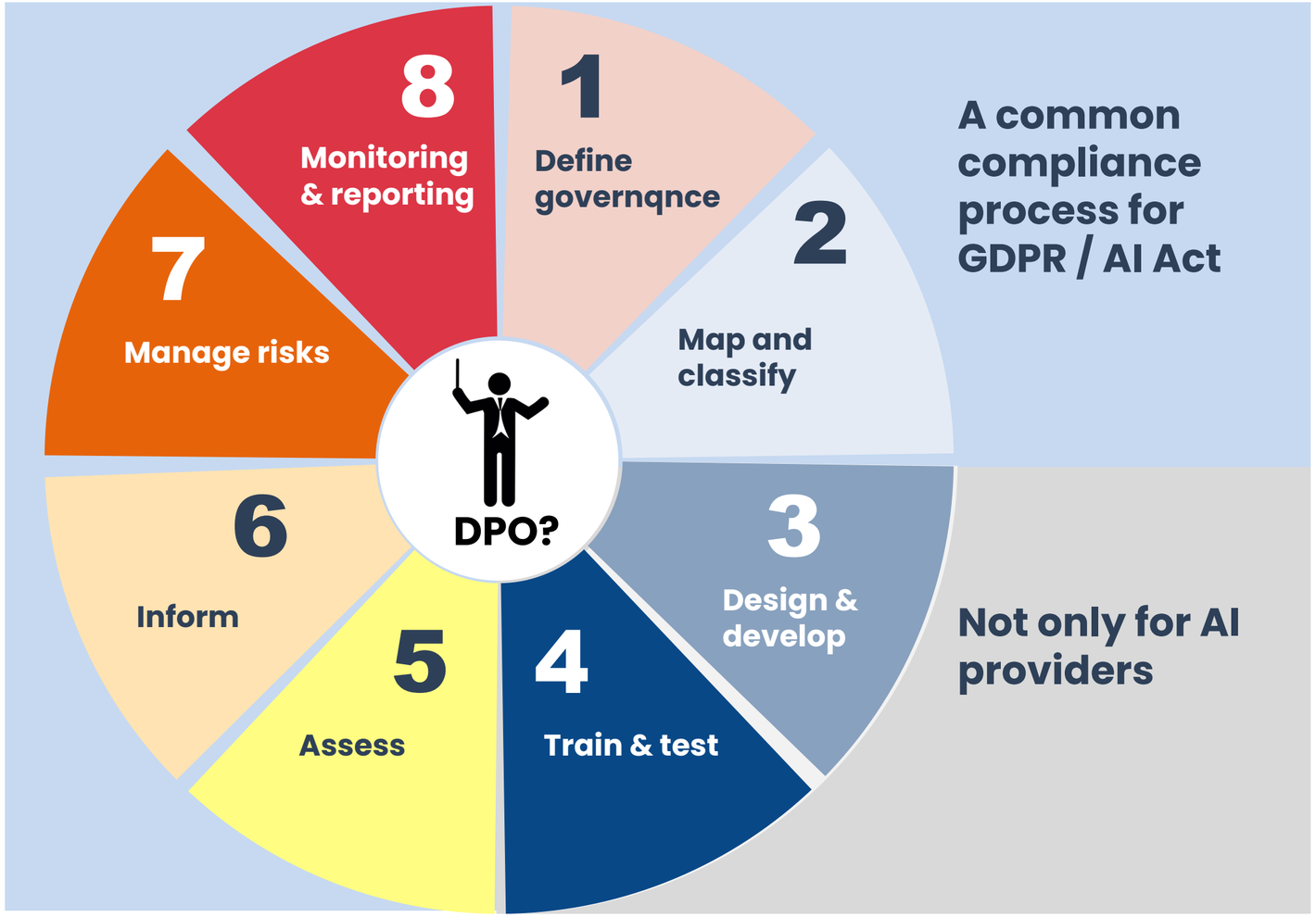
dastra

Organization: the DPO, a Natural Player Already Embedded in the AI Governance Ecosystem



Processes: Operational Lessons from GDPR Useful for the AI Act

- **Anticipate:** Compliance by design / by default (AI review already at scoping stage).
- **Document to demonstrate:** Decisions, metrics, test results → evidence pipeline.
- **Integrate into processes:** Clear RACI (product, data, legal), validation before go-live.
- **Measure:** Governance KPIs (coverage of mapping/assessments, detection time, incidents resolved).
- **Train & align:** AI literacy, concrete examples, dedicated Q&A channel.



The "compliance wheel"

dastra

Tooling: Already Functional GDPR Tools

GDPR tools		AI Act Artifacts
Records of processing activities & documentation		Core register of AI systems (use, model, data, owners, risks, controls, monitoring).
DPIAs & assessments		*AI-specific DPIA-like assessments (FRAIA, bias, security, copyright, explainability).*
Lawful basis	⇔	AI usage policies & user notices (user information).
Contracts (DPA, CCT)		Vendor due diligence for models (update SLAs, evaluation packs, logs, IP rights).
Traceability & evidence		Model cards, data/dataset sheets, inference logs.

dastra

AGENDA

01 Introduction & context

02 What data protection did teach us for AI governance

03 What data protection did NOT teach us for AI governance

04 Example: a “DPIA-like” for an LLM

dastra

Roles and Responsibilities: New Pairings (1/2)

GDPR		AI Act
GDPR Pairing: Controller / Processor (object = data processing)	≠	AI Act Pairing: Provider / Deployer (object = AI system or model), plus other actors (importer, distributor, product manufacturer…). Definitions in Art. 3.

➔ **Consequence: The GDPR ⇆ AI Act mapping is imperfect (different objects and responsibilities).** GDPR defines who processes which data.The AI Act defines who builds, integrates, and uses which system.These are not the same objects, hence the trap of one-to-one mappings.

➔ The right approach is a **contractual chain**:Technical documentation passed downstream, continuous logs and monitoring and change SLAs (fixes, incidents)

Roles and Responsibilities: New Pairings (2/2)

What This Changes in Contracts:

1. Evaluation packages: Technical documentation + transparency information for integrators (Annexes XI–XII / GPAI obligations).
2. Logs & traceability: For high-risk systems, logging capability (Art. 12) and log retention by the provider (Art. 19).
3. Updates & fixes: Post-market monitoring plan (Art. 72) + corrective actions / notification of parties (Art. 20).

From Individual Risk to Systemic GPAI Risk (1/2)

GDPR		AI Act
Privacy mainly deals with **individual harms.**	≠	Here, we are addressing **systemic** risks (network effects, cross-dependencies, concentration of power)

➔ **Consequence:** With GPAI, the regulator targets the upstream part of the ecosystem. Since August 2, 2025, model providers must publish a summary of training content, maintain documentation, implement security measures…and even more so if the model poses systemic risk.

➔ **The GPAI Code of Practice** is a useful shortcut: complying with it makes it easier to demonstrate conformity and reduces the burden for signatories.

From Individual Risk to Systemic GPAI Risk (2/2)

2025 Framework:

1. **GPAI obligations** effective since August 2, 2025: technical documentation, copyright policy, public summary of training data; plus enhanced obligations if systemic risk applies.
2. **GPAI Code of Practice** (July 10, 2025): a voluntary but recognized tool, validated by the Commission/AI Board, to demonstrate compliance; signatories are publicly listed by the AI Office.

Dynamic Control vs. “Paper” Compliance

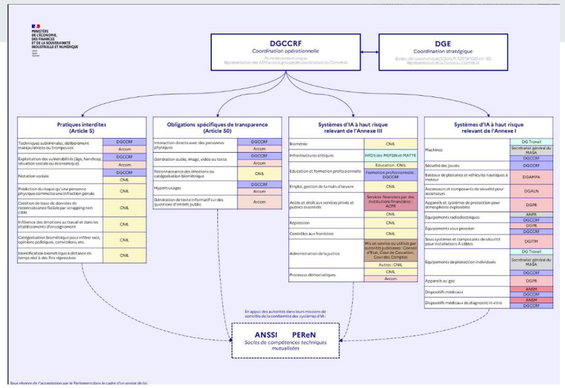
GDPR		AI Act
Review required whenever processing is modified	≠	• Mandatory **post-market monitoring** (for high-risk systems): a monitoring system to collect and analyze performance data throughout the system’s lifecycle.
Processing records in the format of Article 30		• **Logging:** ability to automatically record events (Art. 12) + log retention (Art. 19).
Incident notification to authorities within 72 hours		• **Incidents: r**eporting of serious incidents to authorities “without delay” (Art. 73).

➔ **Practical Consequence:** Record of AI systems and assessments (updated at each version/patch), alert thresholds, periodic audits

Enforcement: towards a multitude of supervisory authorities

GDPR	≠	AI Act
1 supervisory authority per country or jurisdiction(ex. APD in Belgium or CNIL in France)		Multiple authorities per country or jurisdiction based on the principle of “sectoral specialization”: Ex. 19 in France • **DGE**: coordination • **CNIL**: biometrics, data, sensitive uses (justice, employment, education) • **DGCCRF**: commercial practices, consumer protection, transparency • **Arcom**: media, deepfakes, disinformation • **ANSM**: medical devices • **ACPR**: finance and essential services • **Etc.**

➔ **Consequence** : more authorities = more enforcement?



AGENDA

01 Introduction & context

02 What data protection did teach us for AI governance

03 What data protection did NOT teach us for AI governance

04 Example: a “DPIA-like” for an LLM

dastra

LLMs in the Enterprise: Promises and Reality

- 📈 Explosion of use cases: customer support, drafting, HR, document analysis…

- ⚙️ Easy integration via API → rapid deployments

- ❗ Problem: these tools process massive volumes of data without native transparency

How can GDPR compliance be ensured in this context?

dastra

Challenge #1: Model Input

🔍 Problem: ingestion of personal data

- Internal documents, customer tickets, emails…
- No filtering = personal + sensitive data = risk

dastra

Challenge #2: Model Output and Hallucinations

Is the generated content compliant?

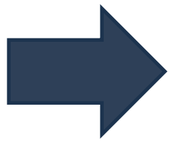
- Can it contain personal data?➔ Yes
- Can it invent false facts?➔ Yes (hallucinations)

dastra

Challenge #3: Data Subject Rights

LLMs pose a GDPR challenge:

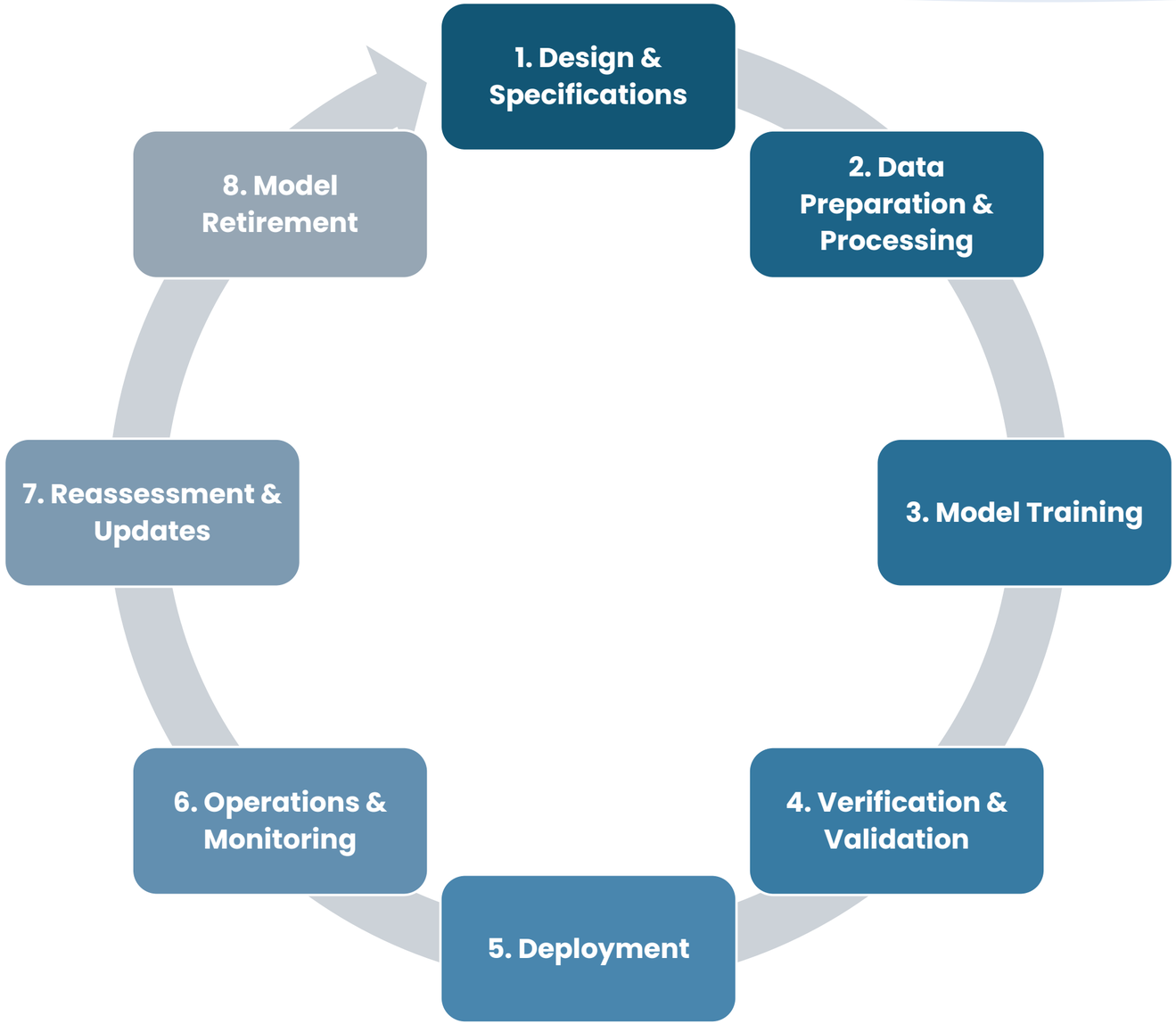
- Impossible to access the “source data”
- No traceability on inputs/outputs
- No guarantee of effective deletion



Right of access, rectification, or erasure is difficult to apply

dastra

The Lifecycle of an AI System



dastra

Three Main Deployment Models for LLMs

Model	Description	Examples	LLM Mastery
1. LLM as a Service	Access via cloud API, without access to model weights. Fast deployment but full dependency on the provider.	GPT-4 API (OpenAI)Claude API (Anthropic)	Low to moderate
2. LLM Off-the-Shelf	The deployer selects a model and customizes the weights (fine-tuning), often through a cloud platform or locally.	LLaMA, BLOOM, Azure OpenAI, Bedrock	Moderate to High
3. LLM développé en interne	The model is trained, hosted, and managed by the organization itself. Full autonomy but significant complexity.	Advanced R&D Case / Large Enterprises / AI Startups	Very high

dastra

Distinction Provider / Deployer (AI Act):

Provider: the entity that develops and offers the AI system

Deployer: the entity that integrates and uses the system with end users

dastra

GDPR Responsibilities depending on the LLM Model used

Model	Deployer as Data Controller	Provider as Data Controller	Provider as Processor
LLM as a Service	Defines purposes and means (user queries, business use cases)	Reuses data for training, monitoring, or analytics	Processes data according to the deployer's instructions (API, hosting)
LLM "Off-the-Shelf"	Customizes the model, controls data (preprocessing, outputs, workflows)	Retains or reuses data (debugging, continuous improvement)	Platform acting under deployer's instructions (cloud, managed API)
Self-developed LLM	Full control: objectives, training, hosting	Not applicable: provider and deployer are the same entity	Not applicable
Agentic AI	Manages inputs, memory, tasks, interactions with external tools	May retain interaction data to improve its modules or intelligent components	Tool or API providers executing actions at the deployer's request (sub-instructions)

dastra

Risques privacy d’un LLM (1/2)

Risks	Description	GDPR articles
1. Insufficient data protection	Lack of encryption, unauthorized access, insecure APIs, unsecured logs → exposure to leaks	Art. 32, Art. 5(1)(f), Art. 9
2. Poor anonymization	Poorly pseudonymized data used for training → possible inferences	Art. 5(1)(a)(b), Art. 25
3. Unlawful processing during training	No legal basis for using personal data in training datasets	Art. 5(1)(a)(c), Art. 6(1), Art. 7
4. Processing of sensitive or judicial data	Use of health, religion, or criminal record data without a clear legal framework	Art. 9(1)(2), Art. 10
5. Negative impact on individuals	Biased or incorrect outputs used to make decisions	Art. 5(1)(d)(a), Art. 22, Art. 25
6. Absence of human intervention	Automated decisions (loan approval, recruitment) without human intervention	Art. 22(1)(3), Art. 12

dastra

Risques privacy d’un LLM (2/2)

Risks	Description	GDPR articles
7. Non-compliance with data subject rights	Impossible to correct, delete, or restrict the data contained in a model	Art. 12–14, 16–18, 21
8. Unlawful reuse of data	Use of prompts or outputs for purposes other than those intended, without providing information	Art. 5(1)(b)(a), Art. 28(3)(a), Art. 29
9. Unlimited storage	Retention of prompts, logs, or outputs beyond what is necessary	Art. 5(1)(e), Art. 25
10. Unlawful transfers outside the EU	Processing carried out in non-adequate countries without safeguards (e.g., cloud LLM hosted in China)	Art. 44–46
11. Non-compliance with data minimization	Collection of very large amounts of data to train or fine-tune the model	Art. 5(1)(c), Art. 6(1)(f), Art. 25

dastra

Risks & measures according to the phases of an LLM as a Service

Each phase of the system must be analyzed through the lens of privacy risk

Phase	Major risks	Key Mitigation Measures
1. User input	- Sensitive data leakage - Unauthorized access - Injection / jailbreaking attacks - Lack of transparency	✓ Filters and alerts for sensitive prompts ✓ Automatic anonymization ✓ TLS + at-rest encryption ✓ MFA + strong password ✓ Clear privacy policy
2. Interface / API	- Network interception - API exploitation - Vulnerable interfaces / phishing	✓ End-to-end encryption ✓ Strong authentication (OAuth, API keys) ✓ OWASP security practices ✓ Anti-phishing, brand protection ✓ Auditing & logging
3. LLM Processing	- Sensitive inferences / hallucinations - Excessive logging - Poisoning attacks - Unauthorized access to logs	✓ Content filtering + human review ✓ Minimized and encrypted logs ✓ Restricted and monitored access ✓ Advanced anonymization ✓ Cloud provider governance
4. Generated Output	- Possible re-identification - Inaccurate or sensitive content - Misuse of responses	✓ Post-processing filtering ✓ Redaction / context limitation ✓ Output usage policy ✓ Human review for critical use cases ✓ User training

dastra

How to Govern an LLM Project?

Recommended Approach

- Map out the use cases
- Limit the personal data used
- Establish a clear contract with providers (no reuse of data)
- Define responsibilities
- Carry out a DPIA (Data Protection Impact Assessment)

dastra

AI governance in action

- **Our Recommendation:** Start by implementing a simple AI governance program in 4 steps

1	2	3	4
Mapping AI systems in a record of AI systems	**Assessing the risks of AI systems**	**Implement continuous processes**	**Implementing controls**
• Training • Awareness a literacy • Repository of AI models • Register of AI systems • Generation of AI sytems information notice	• Predefined use case models • Evidence gathering • Relationship inventory	• Risk aggregation and logic • Remediation plan • AI-governed by design' procedure • Verification of compliance	• Management of policies and notices • Audit control plan • Continuous improvement

Towards ISO42001 AI management systems certification & standard?

DPO FORUM dastra

Conclusion

“ AI Governance in Action means breaking down silos between technology and oversight ”

GDPR

Since May 25, 2018

- Protection of individuals
- Principles (transparency, minimization, accountability)
- Evidence (DPIA, records)

AI Act

2024-2026

- A Risk-Based Framework
- New roles (Provider / Deployer)
- Post-market obligations (continuous monitoring)

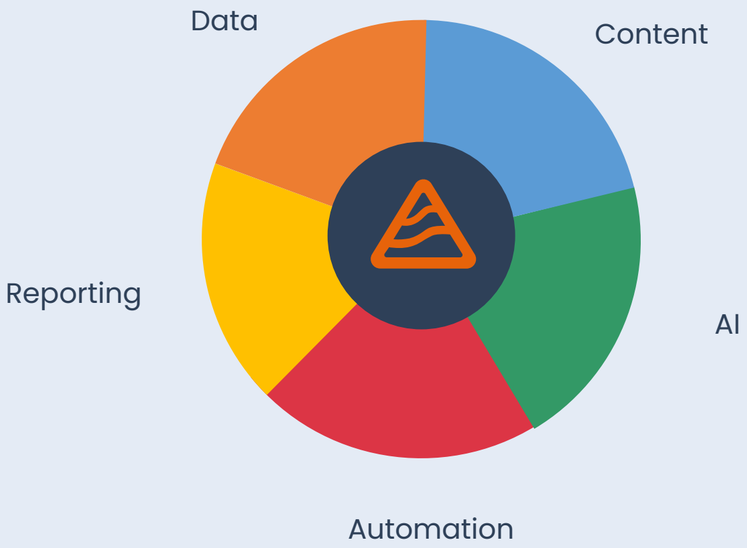
GDPR taught us to document; the AI Act requires us to orchestrate and continuously monitor.

dastra

A unified platform to ensure compliance

The Dastra data compliance platform

A unified platform to structure your data compliance operations, centralise your data and automate your processes, whatever your level of maturity.



Unify compliance, IT, legal, purchasing and risk databases

Data processing activities	Assets	Stakeholders	Data catalog	Retention schedule
Data subject	Contracts	Questionnaires	AI Systems	Risks
Security measures	Data subject requests	Data breaches & incident	Vendors	Controls

Sharing information between teams

Activity monitoring	Project information	Documents and templates

Organising and monitoring communications

Customised reports	Conversation inbox	Support and live chat
AI Assistant	Task management	Integration

dastra

dastra

Le privacy & AI hub des DPO

Contactez-nous !

❤️ **Dastra est hébergé, conçu et développé en France**