



Ce que la protection des données nous a appris sur la gouvernance de l'IA

Brunch & Learn
25 Septembre 2025
Lille



Bienvenue



Paul-Emmanuel Bidault

Co-fondateur et CEO de Dastra

Expertise en logiciels de gouvernance des données personnelles

Expérience en conseil en gouvernance des données et en gestion des risques

SOMMAIRE

01

Introduction &
contexte

02

Ce que la protection
des données nous a
appris

03

Ce que la protection
des données ne nous
a PAS appris

04

Exemple concret : un
“DPIA-like” pour un
LLM

La protection des données et la gouvernance de l'IA

La Data est aujourd'hui le carburant de l'IA: si elles sont mal protégées, elle nous expose ; si elles sont de mauvaise qualité, elles coûtent cher ; si elles sont bien gouvernées, elles deviennent le meilleur levier pour réduire les charges et sécuriser les contrôles !

UN ENJEU ...

La protection des données est un enjeu critique :

- ◆ Les volumes de données explosent : transactions, pièces contrôlées, données ESG, logs IT, remontées des tiers, etc.
- ◆ La qualité des données est souvent insuffisante : doublons, documents incomplets, données non normalisées, etc.
- ◆ Le risque de sanction si les données sont incomplètes ou biaisées existe et se renforce avec de nouvelles réglementations et obligations (telle que l'IA Act)

... ET UN LEVIER

Parmi les usages les plus fréquemment identifiés :

- ◆ Automatisation de processus (de contrôles notamment)
- ◆ Analyse des contrats (écarts de conformité)
- ◆ Veille réglementaire
- ◆ Prévion / Prévention des risques (pattern de fraude ou de comportement déviants par exemple)
- ◆ Mise en place d'un chatbot (base de connaissance dynamique qui réfléchit)
- ◆ Risk scoring pour la due diligence des tiers

Les grands défis des DPO

Les Délégués à la Protection des Données font face à quelques défis majeurs qui bousculent leurs pratiques et leur positionnement interne :

UNE MATIÈRE COMPLEXE ET VARIÉE

Les réglementations deviennent de plus en plus exigeantes et portent sur des sujets de plus en plus vastes : conformité data, protection des clients, cybersécurité, IA, blanchiment d'argent ou encore finance durable

UN RISQUE PERMANENT À SÉCURISER

L'arrivée à maturité de certaines technologies et leur utilisation accrue expose les organisations à des risques cyber et de fraude croissants

LA NÉCESSITÉ D'ÊTRE DANS L'URGENCE

Les réglementations évoluent très vite et nécessitent une capacité d'adaptation quasi instantanée

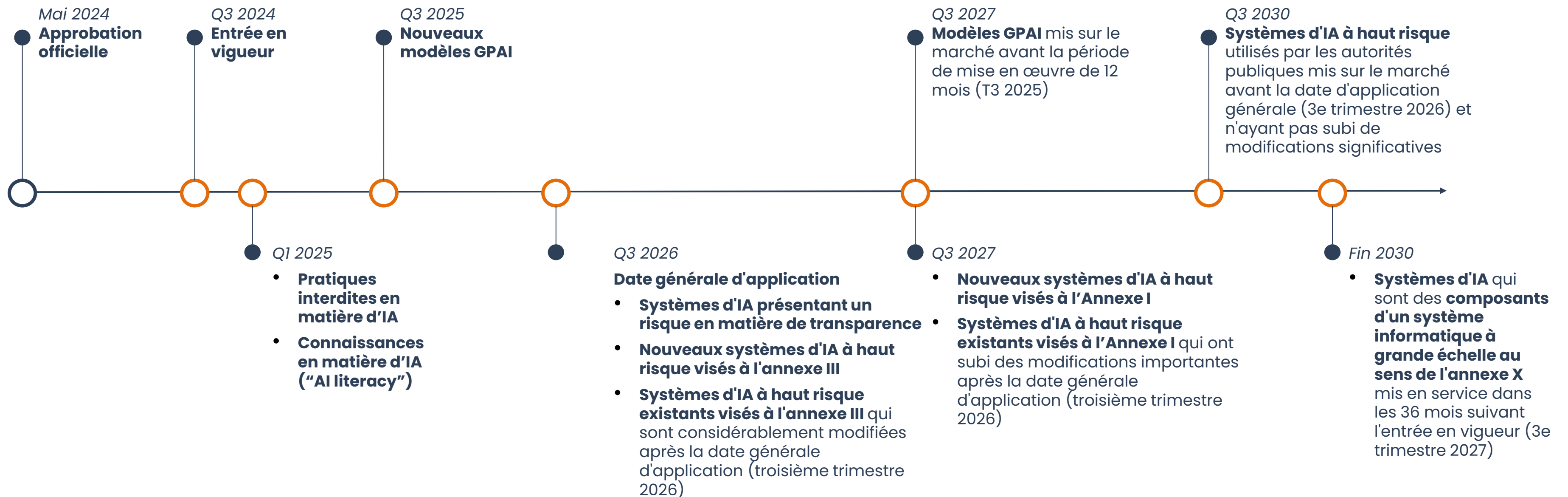
NE PAS RALENTIR LE BUSINESS

Les contrôles ne doivent pas alourdir les processus métier ni nuire à l'expérience client

Pour répondre au mieux à ces grands défis, les Délégués à la Protection des Données que nous rencontrons font face à une nécessité de transformation qui intègre des aspects organisationnels, de processus, d'outillage ou encore de compétences.

Pourquoi la gouvernance de l'IA maintenant ?

Usage massif, risques diffus, et calendrier contraignant AI Act avec obligations qui s'échelonnent jusqu'en 2026



SOMMAIRE

01

Introduction &
contexte

02

Ce que la protection
des données nous a
appris

03

Exemple concret : un
“DPIA-like” pour un
LLM

04

Ce que la protection
des données ne nous
a PAS appris

Ce que la protection des données nous a appris en 4 axes

Ce que la privacy nous a appris se décline notamment en 4 axes que l'on réutilise pour l'IA :



Principes

- Ce que c'est : valeurs & règles directrices.
- Exemples (privacy) : transparence, minimisation, accountability, by design.
- À retenir pour l'IA : AI by design, explicabilité, limites d'usage.



Organisation

- Ce que c'est : rôles, responsabilités, gouvernance.
- Exemples (privacy) : Responsable/Sous-traitant, DPO, sponsors.
- À retenir pour l'IA : gouvernance transversale, owners (modèle/données), référent IA.



Processus

- Ce que c'est : flux de travail & décisions répétables.
- Exemples (privacy) : registres, DPIA, gestion incidents.
- À retenir pour l'IA : cartographie des systèmes, évaluations de risques, monitoring continu.



Outillage

- Ce que c'est : artefacts & outils pour agir et prouver.
- Exemples (privacy) : registres, gabarits DPIA, portails droits.
- À retenir pour l'IA : registre IA, model/data cards, bancs d'essai, logs & dashboards.



Principes : le RGPD, des réflexes utiles pour le RIA

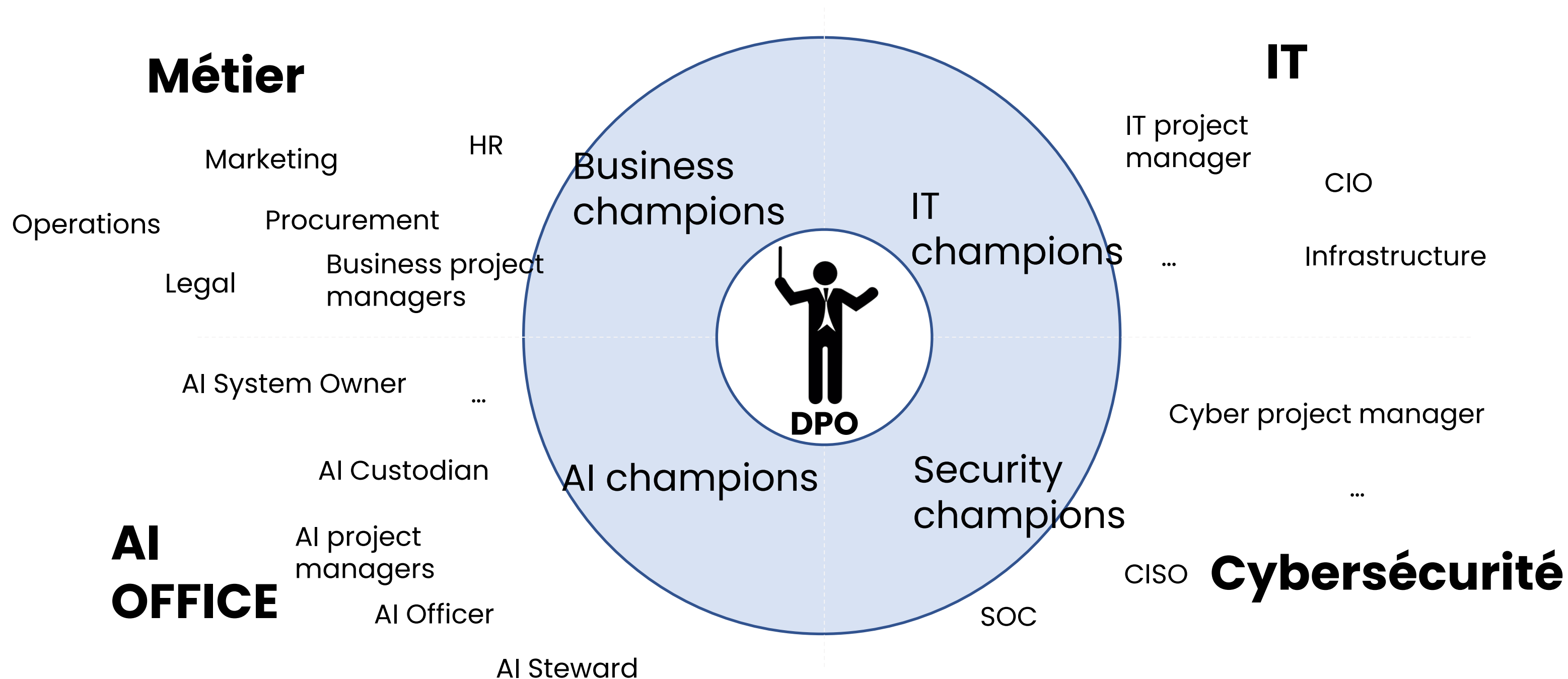
Principes RGPD
Transparence
Minimisation / limitation des finalités
Accountability
Privacy by design
Sécurité & qualité
Approche par les risques



Principes RIA
Notices claires côté IA (usage, limites, contacts).
Données & capacités du modèle limitées à l'usage visé.
<i>Evidence by default</i> (preuves de choix, tests, arbitrages).
AI by design : contrôles intégrés dès la conception (HITL, garde-fous, red teaming)
Traçabilité datasets, gouvernance des versions, revue biais/erreurs.
Classification des systèmes d'IA : interdits, à haut risques, limités, minimal



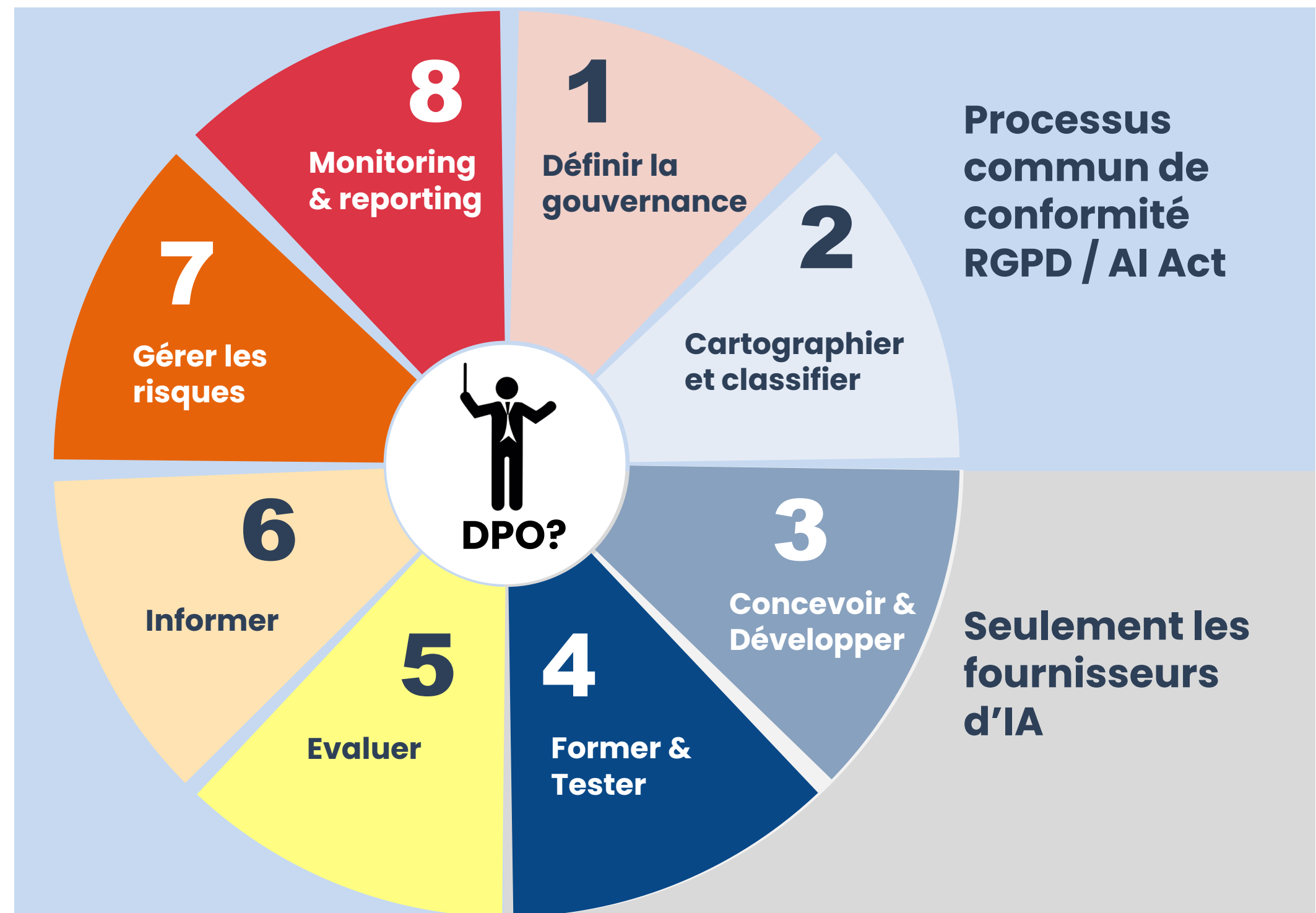
Organisation : le DPO, un acteur naturel déjà présent au sein de l'écosystème de gouvernance de l'IA





Processus : leçons opérationnelles du RGPD utiles au RIA

- **Anticiper** : conformité « by design / default » (revue IA dès le cadrage).
- **Documenter pour prouver** : décisions, métriques, résultats de tests → pipeline de preuves.
- **Intégrer aux processus** : RACI clair (produit, data, juridique), validation avant mise en prod.
- **Mesurer** : KPIs de gouvernance (couverture cartographie/évals, temps de détection, incidents traités).
- **Former & aligner** : AI literacy, exemples concrets, canal de questions.



La « roue » de la conformité



Outillage : Des outils RGPD déjà fonctionnels

Outils RGPD

Registre des traitements & documentation

DPIAs & évaluations

Bases légales

Contrats (DPA, CCT)

Traçabilité & preuves



Artefacts RIA

Base du registre des systèmes d'IA (usage, modèle, données, propriétaires, risques, contrôles, monitoring).

DPIA-like IA (FRAIA, biais, sécurité, droits d'auteur, explicabilité).

Politiques d'usage & notices IA (info utilisateur).

Due diligence fournisseurs de modèles (SLAs de mise à jour, packs d'évaluation, logs, droits IP).

Model cards, data/dataset sheets, journal d'inférences.

SOMMAIRE

01

Introduction &
contexte

02

Ce que la protection
des données nous a
appris

03

Ce que la protection
des données ne nous
a PAS appris

04

Exemple concret : un
“DPIA-like” pour un
LLM

A. Rôles et responsabilités : nouveaux couples (1/2)

RGPD
Binôme Responsable de traitement / Sous-traitant (objet = traitement de données)

≠

RIA
Binôme Fournisseur / Déployeur (objet = système ou modèle d'IA), + autres acteurs (importateur, distributeur, fabricant de produit...). Définitions à l'Art. 3.

- **Conséquence** : le mapping RGPD ⇔ AI Act est **imparfait** (objets et responsabilités différents). Le RGPD organise **qui traite quelles données**. Le RIA organise **qui fabrique, intègre et utilise quel système**. Ce ne sont pas les mêmes objets : d'où le piège des mappings 1-pour-1
- La bonne approche, c'est une **chaîne contractuelle** : docs techniques au downstream, **logs** et **monitoring** en continu, et des **SLA de changement** (correctifs, incidents).

A. Rôles et responsabilités : nouveaux couples (2/2)

Ce que ça change dans les contrats:

1. **Paquets d'évaluation** : docs techniques + infos de transparence aux intégrateurs (Annexes XI-XII / obligations GPAI).
2. **Logs & traçabilité** : en haut risque, capacité de **journalisation** (Art. 12) et **conservation des logs** par le fournisseur (Art. 19)
3. **Mises à jour & correctifs** : **plan de monitoring post-marché** (Art. 72) + **actions correctives / info des parties** (Art. 20).

B. Du risque individuel vers le risque systémique GPAI (1/2)

RGPD

la privacy traite surtout des **atteintes individuelles**

≠

RIA

On gère des risques **systémiques** (effets réseau, dépendances transversales, concentration de pouvoir).

- **Conséquence** : Avec les GPAI, le régulateur vise l'amont de l'écosystème. Depuis le 2 août 2025, les fournisseurs de modèles doivent publier un résumé du contenu d'entraînement, tenir une documentation et appliquer des mesures de sécurité — et encore plus si le modèle présente un risque systémique.
- Le **Code GPAI** est un **raccourci utile** : s'y conformer **facilite la preuve** et **allège la charge** pour les signataires

B. Du risque individuel vers le risque systémique GPAI (2/2)

Cadre 2025:

1. **Obligations GPAI** applicables **depuis le 2 août 2025** (doc technique, politique copyright, résumé public des données d'entraînement ; + obligations renforcées si **risque systémique**)
2. **Code de bonnes pratiques GPAI** (10 juil. 2025) = **outil volontaire adéquat** validé par la Commission/AI Board pour démontrer la conformité ; signataires listés publiquement par l'AI Office.

C. Contrôle dynamique vs conformité « papier »

RGPD
Revue dès modification du traitement
Fiches de traitement format article 30
Notification incident aux autorités sous 72h

≠

RIA
• Post-marché obligatoire (haut risque) : un système de monitoring pour collecter/analyser les données de performance tout au long de la vie du système. • Journalisation : capacité à enregistrer automatiquement les événements (Art. 12) + conserver les logs (Art. 19). • Incidents : signalement « sans délai » des incidents graves aux autorités (Art. 73)

→ **Conséquence** pratique : registre IA et évaluations **vivants** (mises à jour à chaque version/patch), **seuils d'alerte**, audits périodiques.

D. Enforcement: vers une multitude d'autorités de contrôle

RGPD

1 autorité de contrôle (CNIL en France)

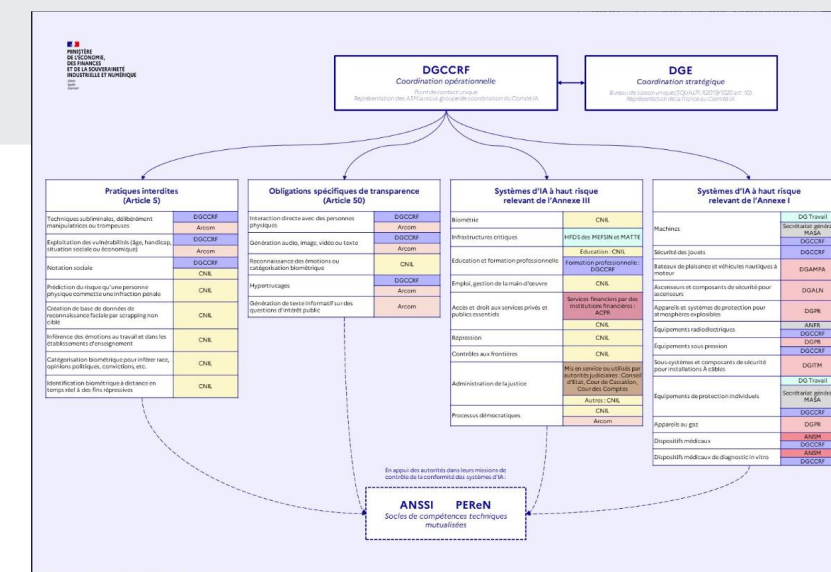
 $\neq$

RIA

Proposition de 19 autorités de contrôle selon le principe de « spécialisation sectorielle) :

- DGE: coordination
- CNIL : biométrie, données, usages sensibles (justice, emploi, éducation).
- DGCCRF : pratiques commerciales, protection des consommateurs, transparence.
- Arcom : médias, deepfakes, désinformation.
- ANSM : dispositifs médicaux.
- ACPR : finance et services essentiels.

Etc



→ **Conséquence** : plus d'autorités = plus d'enforcement?

SOMMAIRE

01

Introduction &
contexte

02

Ce que la protection
des données nous a
appris

03

Ce que la protection
des données ne nous
a PAS appris

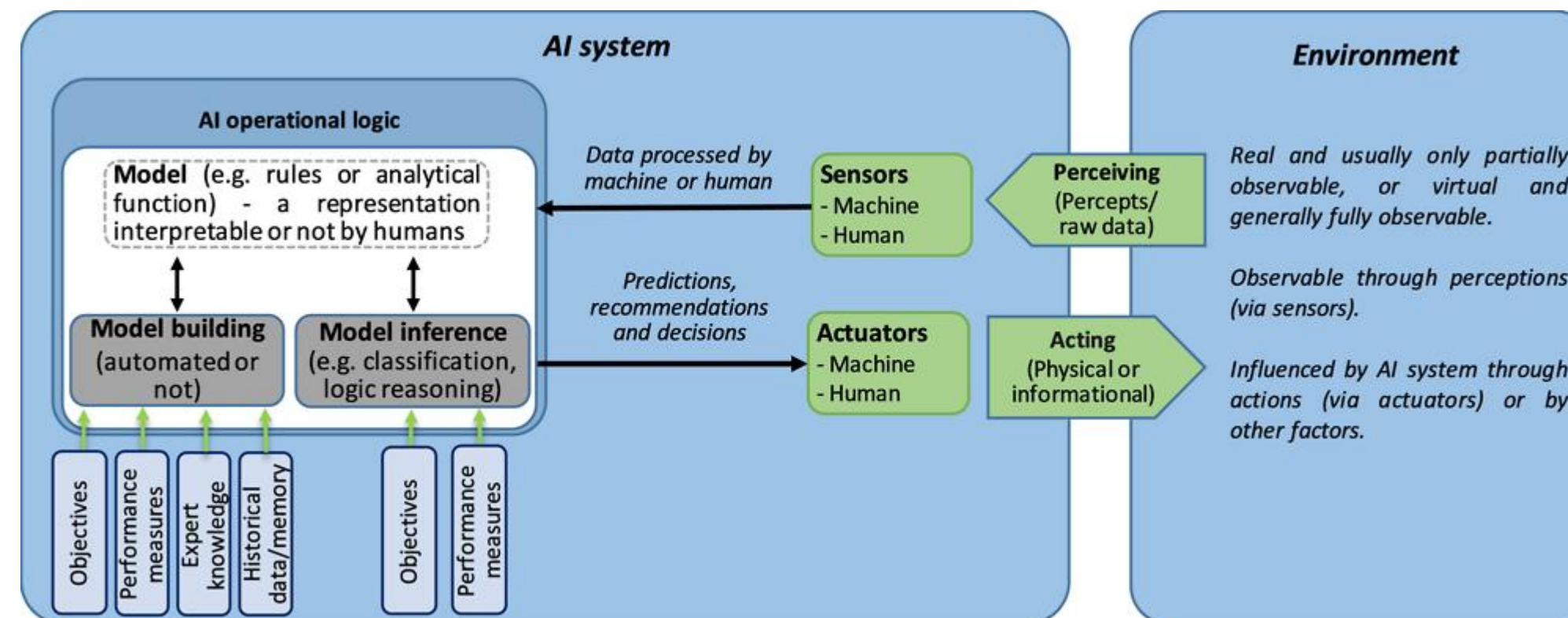
04

Exemple concret : un
"DPIA-like" pour un
LLM

Qu'est-ce qu'un système d'IA ?

“ Un **système automatisé** conçu pour fonctionner à différents niveaux d'**autonomie** et capable de démontrer une capacité d'adaptation après son déploiement, **qui**, à des fins explicites ou implicites, **déduit** à partir des données qu'il reçoit **comment générer des résultats** tels que des prévisions, du contenu, des recommandations ou des décisions susceptibles d'influencer des environnements physiques ou virtuels. ”

Ex. A credit scoring system, autonomous driving system...



Conceptual view of an AI System
Source: [OECD](#)

Les LLM en entreprise : promesses et réalité

-  Explosion des cas d'usage : support client, rédaction, RH, analyse documentaire...
-  Intégration facile via API → déploiements rapides
-  Problème : ces outils manipulent des volumes massifs de données sans transparence native

Comment garantir le respect du RGPD dans ce contexte ?

Enjeu #1 : Alimentation du modèle

Problème : ingestion de données personnelles

- Documents internes, tickets clients, emails...
- Absence de tri = données personnelles + sensibles = danger

Enjeu #2 : Sortie du modèle et hallucinations

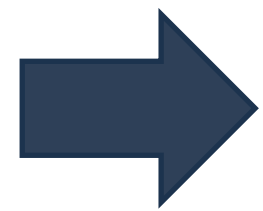
Le contenu généré est-il conforme ?

- Peut-il contenir des données personnelles ? → Oui
- Peut-il inventer des faits faux ? → Oui (hallucinations)

Enjeu #3 : Droits des personnes

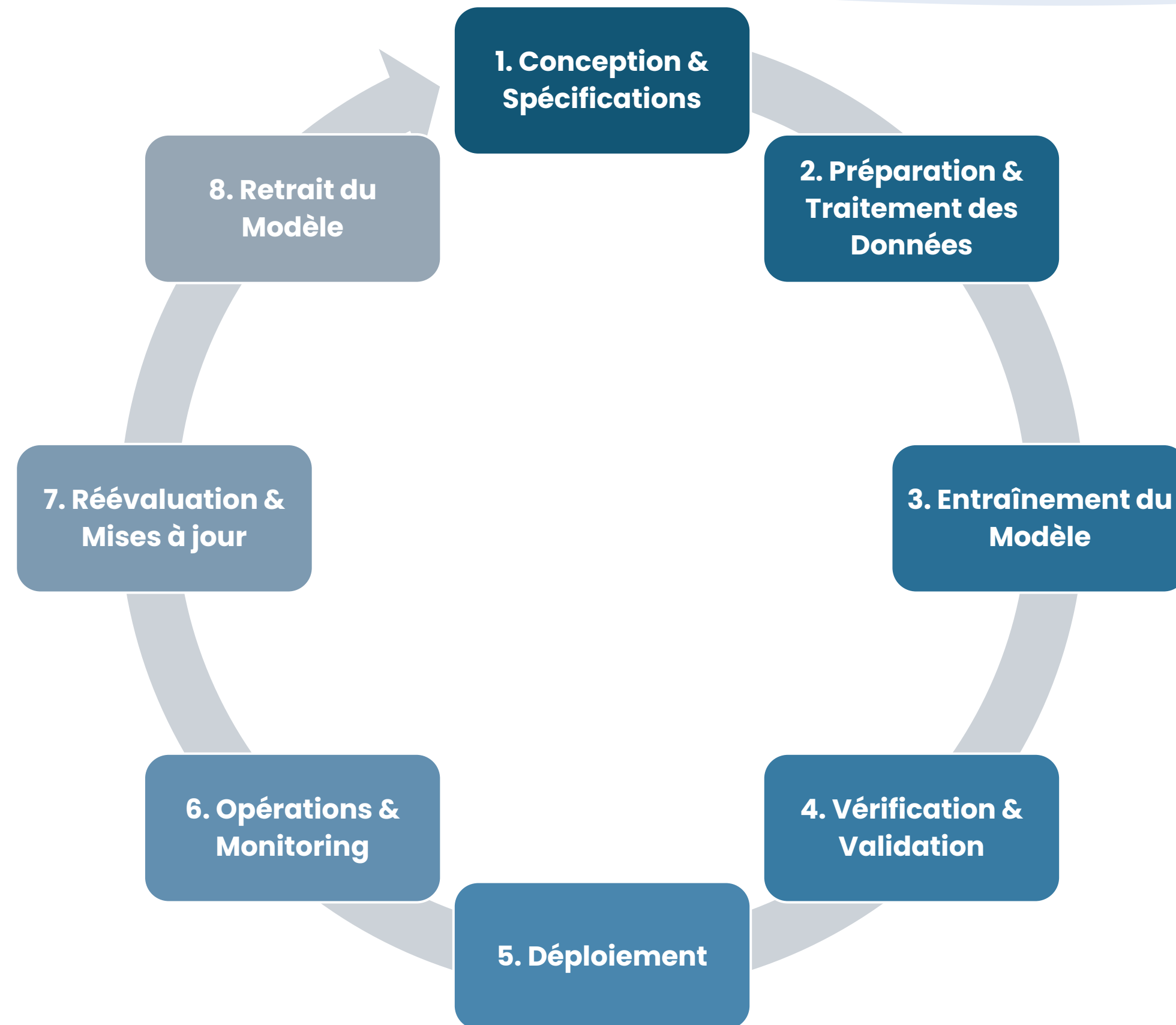
Les LLM posent un défi au RGPD :

- Impossible d'accéder aux « données sources »
- Pas de traçabilité sur les entrées / sorties
- Aucune garantie de suppression effective



Droit d'accès, de rectification ou d'effacement
difficilement applicables

Le cycle de vie d'un système d'IA



Trois modèles principaux de déploiement des LLM

Modèle	Description	Exemples	Maitrise du LLM
1. LLM as a Service	Accès au modèle via API cloud, sans accès aux poids. Déploiement rapide mais dépendance complète au provider	GPT-4 API (OpenAI) Claude API (Anthropic)	Faible à modéré
2. LLM Off-the-Shelf	Le deployer choisit un modèle, personnalise les poids (fine-tuning), souvent via une plateforme cloud ou local	LLaMA, BLOOM, Azure OpenAI, Bedrock	Modéré à élevé
3. LLM développé en interne	Le modèle est entraîné, hébergé et contrôlé par l'organisation elle-même. Autonomie totale mais complexité importante	Cas R&D avancé / grands groupes / start-up IA	Très élevé

Distinction Provider / Deployer (AI Act) :

Provider : l'entité qui développe et offre le système d'IA

Deployer : l'entité qui intègre et utilise le système auprès des utilisateurs finaux

Responsabilités RGPD selon le modèle LLM utilisé

Modèle	Déployeur comme responsable du traitement	Fournisseur comme responsable du traitement	Fournisseur comme sous-traitant
LLM as a Service	Définit les finalités et moyens (requêtes utilisateurs, usages métiers)	Réutilise les données pour entraînement, monitoring ou analytics	Traite les données selon les instructions du déployeur (API, hébergement)
LLM "Off-the-Shelf"	Personnalise le modèle, contrôle les données (prétraitement, outputs, workflows)	Rétention ou réutilisation des données (debugging, amélioration continue)	Plateforme agissant selon les instructions du déployeur (cloud, API managée)
Self-developed LLM	Contrôle complet : objectifs, entraînement, hébergement	Non applicable : le fournisseur et le déployeur sont confondus	Non applicable
Agentic AI	Gère entrées, mémoire, tâches, interactions avec outils externes	Peut conserver les données d'interaction pour améliorer ses modules ou composants intelligents	Fournisseurs d'outils ou d'APIs exécutant des actions à la demande du déployeur (sous-instructions)

Risques privacy d'un LLM

Risque	Description	Articles RGPD
1. Protection insuffisante des données	Manque de chiffrement, accès non autorisé, failles API, logs non sécurisés → exposition aux fuites	Art. 32, Art. 5(1)(f), Art. 9
2. Mauvaise anonymisation	Des données mal pseudonymisées sont utilisées pour l'entraînement → inférences possibles	Art. 5(1)(a)(b), Art. 25
3. Traitement illicite dans l'entraînement	Aucune base légale pour utiliser des données personnelles dans les jeux d'entraînement	Art. 5(1)(a)(c), Art. 6(1), Art. 7
4. Traitement de données sensibles ou judiciaires	Utilisation de données santé, religion, casier judiciaire sans cadre légal clair	Art. 9(1)(2), Art. 10
5. Impact négatif sur les personnes	Sorties biaisées ou erronées utilisées pour prendre des décisions	Art. 5(1)(d)(a), Art. 22, Art. 25
6. Absence d'intervention humaine	Décisions automatisées (prêt, recrutement) sans possibilité d'intervention humaine	Art. 22(1)(3), Art. 12

Risques privacy d'un LLM

Risque	Description	Articles RGPD
7. Non-respect des droits des personnes	Impossible de corriger, supprimer ou restreindre les données contenues dans un modèle	Art. 12–14, 16–18, 21
8. Réutilisation illicite des données	Utilisation des prompts ou outputs à des fins autres que prévues sans information	Art. 5(1)(b)(a), Art. 28(3)(a), Art. 29
9. Stockage illimité	Conservation de prompts, logs ou outputs au-delà de ce qui est nécessaire	Art. 5(1)(e), Art. 25
10. Transferts illicites hors UE	Traitements effectués dans des pays non adéquats sans garanties (ex : cloud LLM Chine)	Art. 44–46
11. Non-respect de la minimisation	Collecte de très grandes quantités de données pour entraîner ou ajuster le modèle	Art. 5(1)(c), Art. 6(1)(f), Art. 25

Risques & mesures selon les phases d'un LLM as a Service

Chaque phase du système doit être étudiée sous l'angle du risque privacy

Phase	Risques majeurs	Mesures d'atténuation clés
1. Entrée utilisateur	- Fuite de données sensibles - Accès non autorisé - Attaques par injection / jailbreaking - Manque de transparence	✓ Filtres et alertes pour prompts sensibles ✓ Anonymisation automatique ✓ Chiffrement TLS + repos ✓ MFA + mot de passe robuste ✓ Politique de confidentialité claire
2. Interface / API	- Interception réseau - Exploitation API - Interfaces vulnérables / phishing	✓ Chiffrement de bout-en-bout ✓ Authentification forte (OAuth, API keys) ✓ Sécurité OWASP ✓ Anti-phishing, branding protection ✓ Audit & journalisation
3. Traitement LLM	- Inférences sensibles / hallucinations - Logging excessif - Attaques par empoisonnement (poisoning) - Accès non autorisé aux logs	✓ Filtrage de contenu + revues humaines ✓ Journaux minimisés et chiffrés ✓ Accès restreint et surveillé ✓ Anonymisation avancée ✓ Gouvernance fournisseurs cloud
4. Sortie générée	- Réidentification possible - Contenu inexact ou sensible - Mauvais usage des réponses	✓ Filtrage post-processing ✓ Redaction / limitation contexte ✓ Politique d'usage des outputs ✓ Revue humaine pour usages critiques ✓ Formation des utilisateurs

Comment encadrer un projet LLM ?

Approche recommandée

- Cartographier les cas d'usage
- Restreindre les données personnelles utilisées
- Contrat clair avec les fournisseurs (pas de réutilisation)
- Définir ses responsabilités
- Réaliser une AIPD

Conclusion

“ La gouvernance de l'IA en action, c'est casser les silos entre la technologie et la supervision ”

RGPD

depuis 25 mai 2018

- Protection des personnes
- Principes (transparence, minimisation, accountability)
- Preuves (DPIA, registres)



AI Act

2024-2026

- Cadre **par risques**
- Nouveaux rôles (**Fournisseur / Déployeur**)
- Obligations **post-marché** (monitoring continu)



*Le RGPD nous a appris à **documenter** ; l'AI Act nous demande **d'orchestrer et surveiller** en continu.*

Construire une gouvernance IA efficace

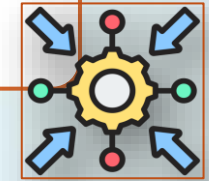
- **Notre recommandation:** Commencer par la mise en place d'un programme de gouvernance de l'IA simple en 4 étapes

1	2	3	4
Répertorier les systèmes d'IA	Evaluer les systèmes d'IA	Approuver / rejeter les projets	Mettre en œuvre les contrôles
• Formation • Sensibilisation • Référentiel de modèles d'IA • Registre des systèmes d'IA	• Modèles prédéfinis de cas d'usage • Collecte de preuves • Inventaire des relations	• Agrégation et logique des risques • Procédure « AI-governed by design » • Vérification de la conformité	• Gestion des politiques et des avis • Audit • plan de contrôle

Pilotez la conformité de vos systèmes d'IA avec Dastra

Centralisez vos systèmes d'IA

- Créez un registre complet et structuré de vos modèles et cas d'usage IA



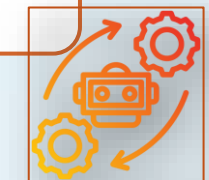
Évaluez les risques

- Classification simplifiée selon les niveaux de risque du règlement européen (minimal, limité, élevé, inacceptable)



Automatisez la conformité

- Notifications, tâches, politiques IA, rapports d'impact et tableaux de bord



Renforcez la gouvernance

- Alignez vos équipes IT, juridiques, métiers et DPO autour d'une gestion collaborative et transparente



Gagnez en efficacité

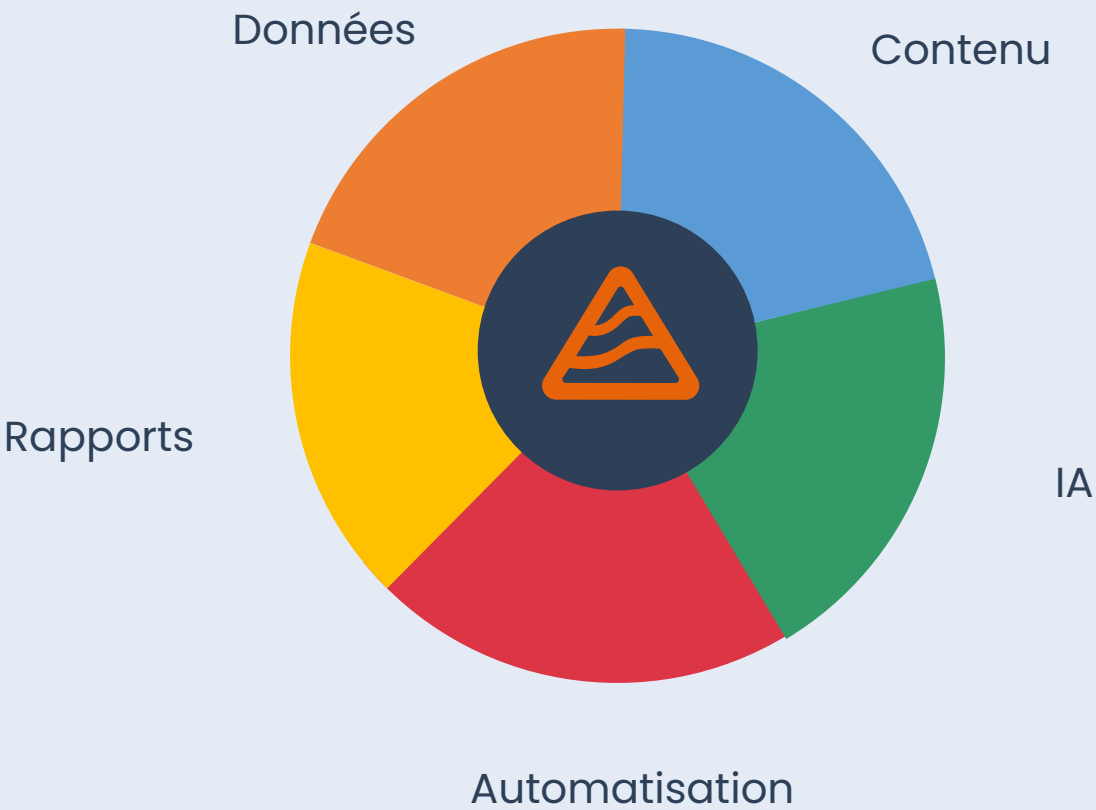
- Anticipez les audits, réduisez les coûts cachés et accélérez l'adoption responsable de l'IA



Une plateforme unifiée, pour une conformité maîtrisée

La plateforme data compliance de Dastra

Une plateforme unifiée pour structurer vos opérations de conformité, centraliser vos données et automatiser vos processus, quel que soit votre niveau de maturité.



Unifier les bases de données de conformité, IT, du juridique, des achats et des risques

Traitements de données	Actifs	Acteurs	Catalogue de données	Durées de conservation
Personnes concernées	Contrats	Questionnaires	Systèmes d'IA	Risques
Mesures de sécurité	Demandes de droits	Violations de données	Sous-traitants	Contrôles

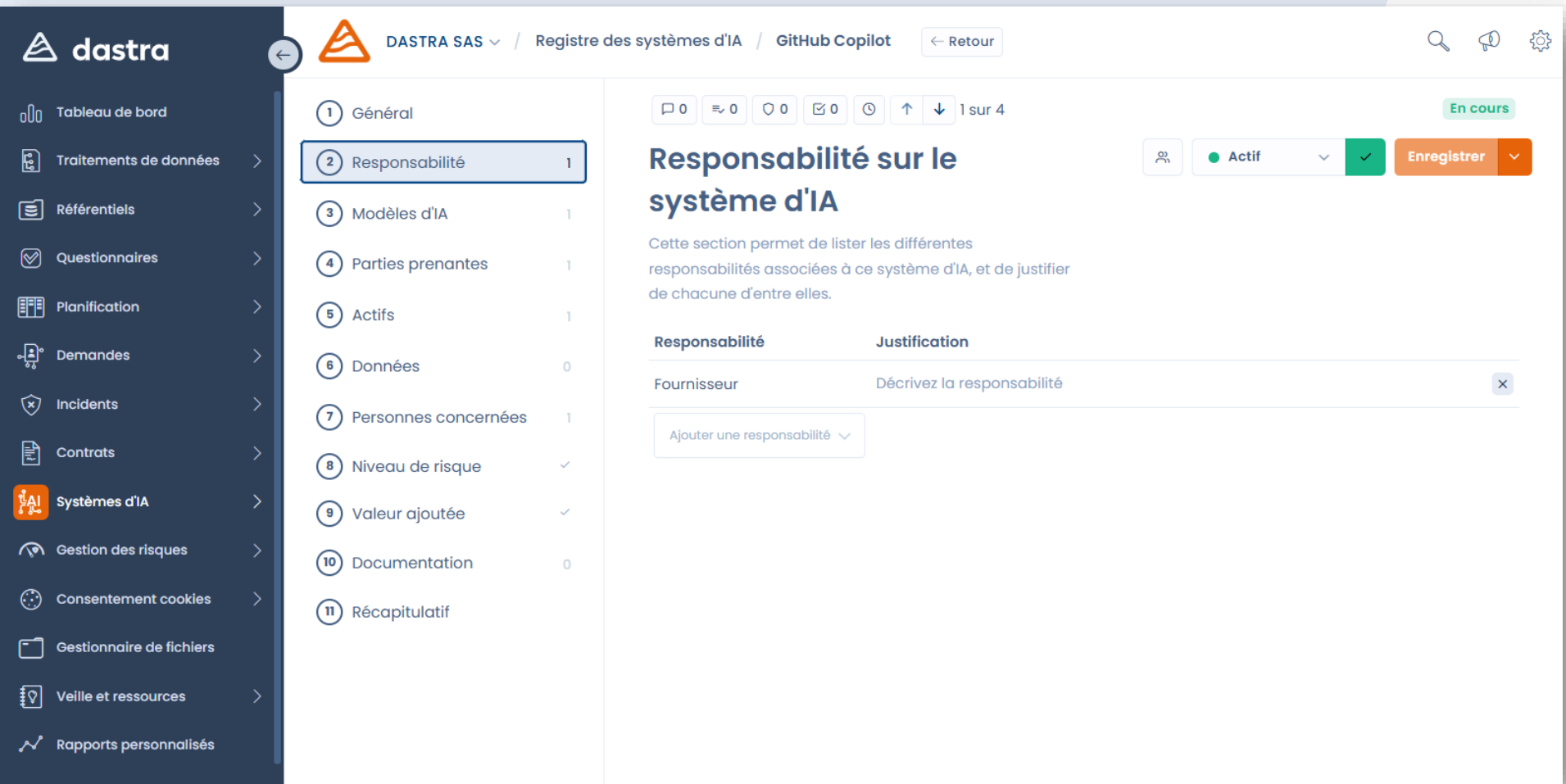
Partager les informations et automatiser les processus

Suivi de l'activité	Informations sur les projets	Documents et modèles
---------------------	------------------------------	----------------------

Organiser et suivre les communications

Rapports personnalisés	Boîte de réception des conversations	Support et chat en direct
Assistant IA	Gestion des tâches	Intégrations

Un module dédié, pour une conformité maîtrisée



Créez des rapports clairs et percutants

Générez des tableaux de bord, des analyses d'impact et des évaluations de conformité pour vos parties prenantes. Offrez à votre écosystème une visibilité complète sur vos modèles d'IA et leur performance en matière de conformité.

Enregistrement centralisé de vos systèmes d'IA

Profitez d'une vision globale et détaillée de vos systèmes d'intelligence artificielle : anticipez les risques, identifiez les opportunités et améliorez votre stratégie de gestion des modèles et ensembles de données en quelques clics.

Classification simplifiée des risques IA

Classifiez et évaluez facilement vos systèmes d'IA selon les standards de la réglementation européenne. Accélérez l'évaluation des systèmes tiers et optimisez la gestion de la conformité. Combinez ce niveau de risque à l'évaluation de la valeur business apportée par ce système.

Gestion et application des systems d'IA

Déployez vos politiques de manière efficace en traduisant les directives en actions techniques. Automatisez les notifications, l'assignation des tâches et les mises à jour pour garantir une exécution en toute simplicité.

Dastra: 80% de temps gagnés pour les équipes data compliance

Une source d'informations unique

Centralise l'ensemble
des informations

Facilite l'alignement des
équipes juridique, IT, DPO
et métiers

Évite les doublons, les
silos et les pertes
d'information

(Meilleure qualité)

Une expérience utilisateur intuitive

Facilite l'adoption

Renforce l'engagement
des équipes

Navigation pensée pour les
usages réels

(Plus d'efficacité)

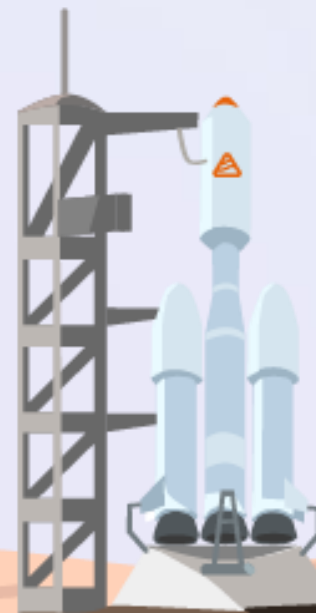
Une base de code unifiée

Facilite l'évolutivité de la
solution

Accélère l'intégration avec vos
outils internes

Réduit les coûts de
maintenance à long terme

(Réduction des coûts cachés)



Pour approfondir 🖐️



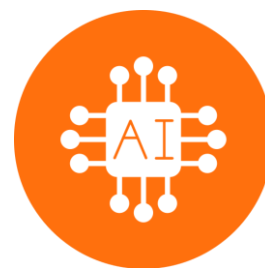
Webinaire sur l'IA Act

Comment aborder l'IA Act en tant que DPO
[Téléchargez le support de présentation ici](#)



IA Act & RGPD

Trouvez les réponses à vos questions sur l'IA Act



Les fonctionnalités : Systèmes d'IA

Vous apprendrez ici à utiliser la fonctionnalité des systèmes d'IA

Plus sur www.dastra.eu





Le privacy & AI hub des DPO



Contactez-nous !



Dastra est hébergé, conçu et développé en France