DPO Consulting
Your personal data protection officer

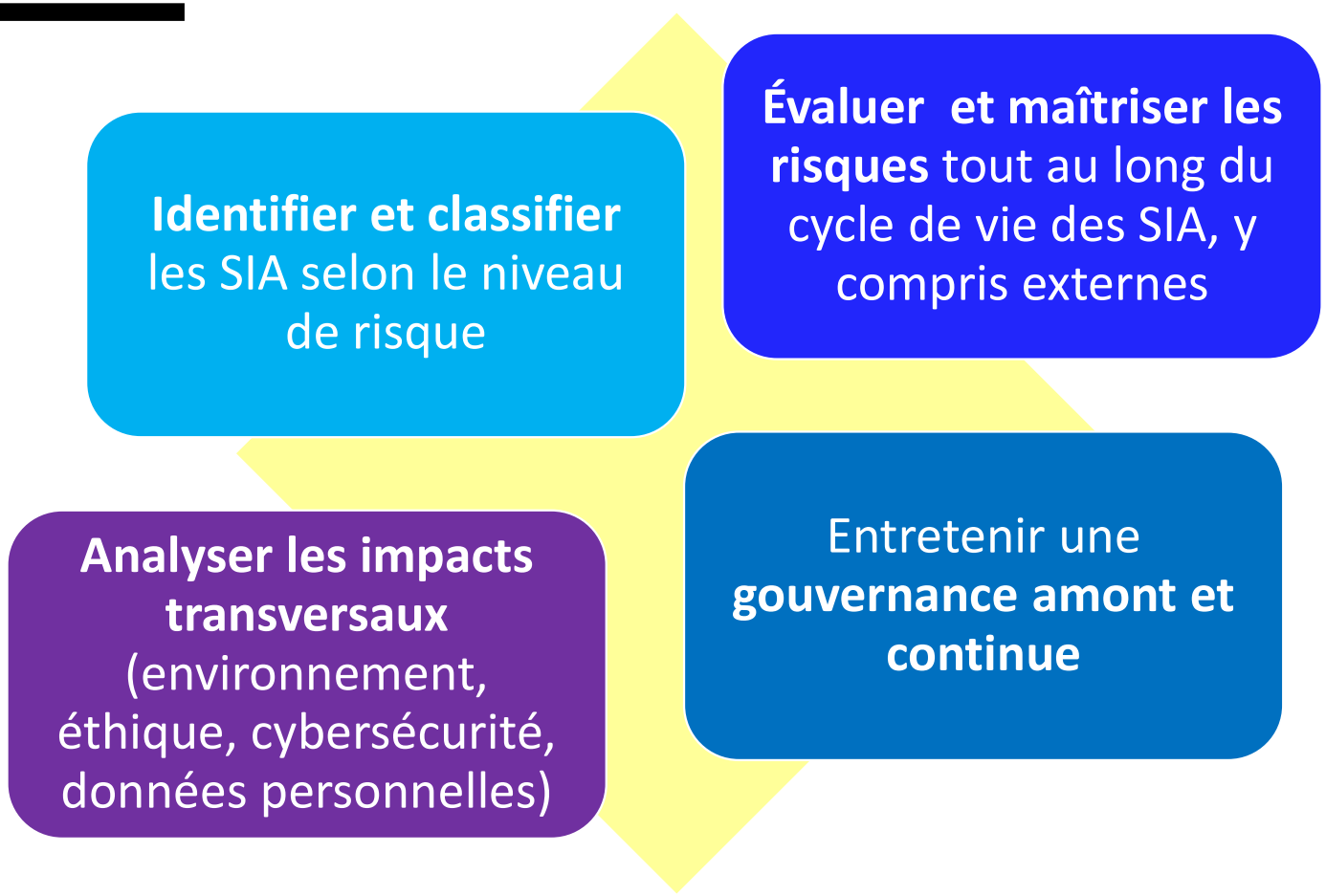
Les 4 Saisons de la data
IA • CYBERSECURITÉ • PROTECTION DES DONNÉES

COMMENT LES MÉTHODES DE CONFORMITÉ, CARTOGRAPHIE ET TRAITEMENT MISES EN PLACE PAR LES DPO PEUVENT-ELLES ÊTRE MISES AU SERVICE DE L'IA ?

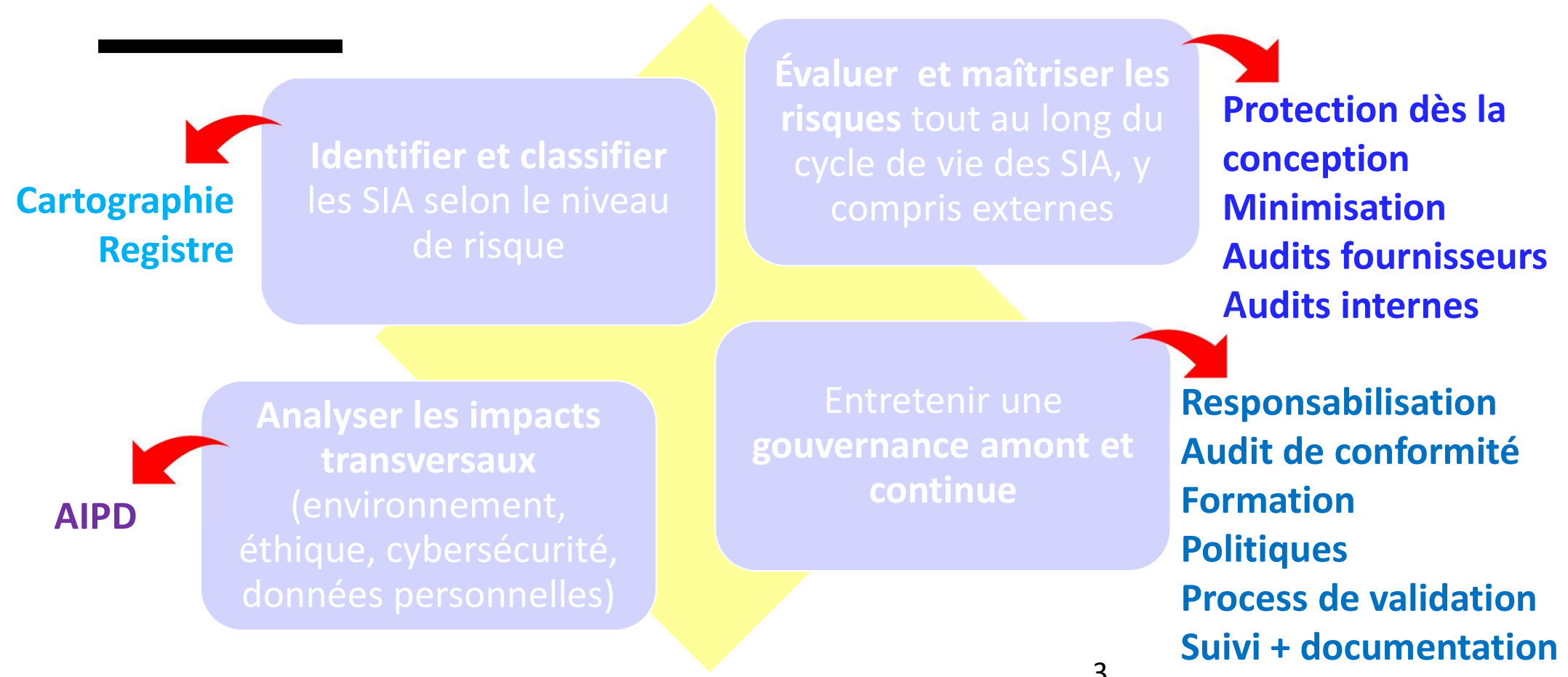
CHRISTOPHE DROT,
DIRECTEUR GENERAL DPO CONSULTING

3 juillet 2025

SECURISER LES SIA…

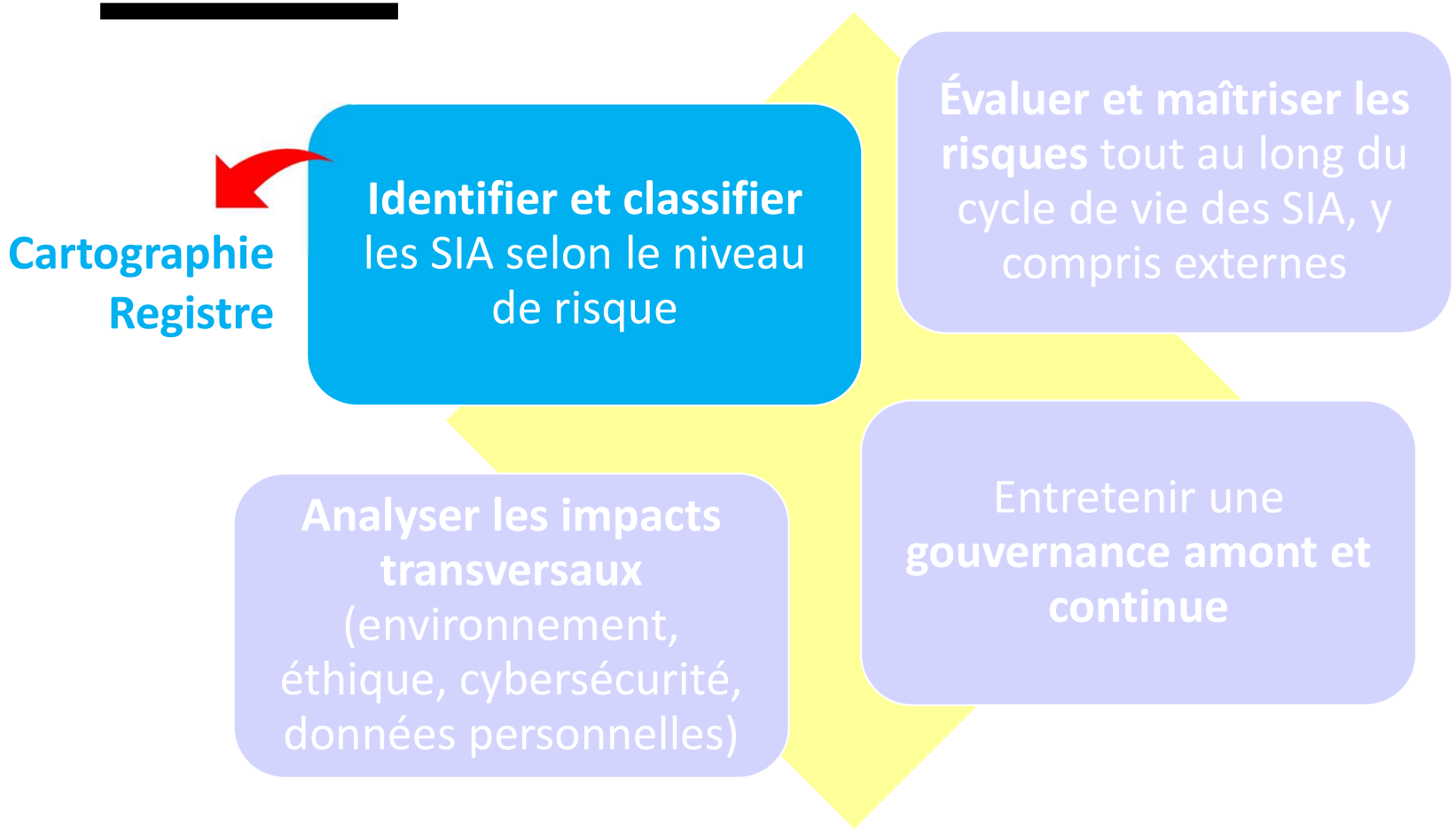


…AVEC LES MÉTHODES ET OUTILS DU DPO !



3

IDENTIFIER ET CLASSIFIER LES SIA



IDENTIFIER ET CLASSIFIER LES SIA

Cartographie

Processus

- Cartographie des processus
- S'adosser aussi sur le Registre des traitements

Identifier les SIA

- Questionnaires de détection des SIA
- Cartographie des dépendances aux SIA

Classifier les SIA

- finalités,
- modèle,
- données,
- impacts
- …

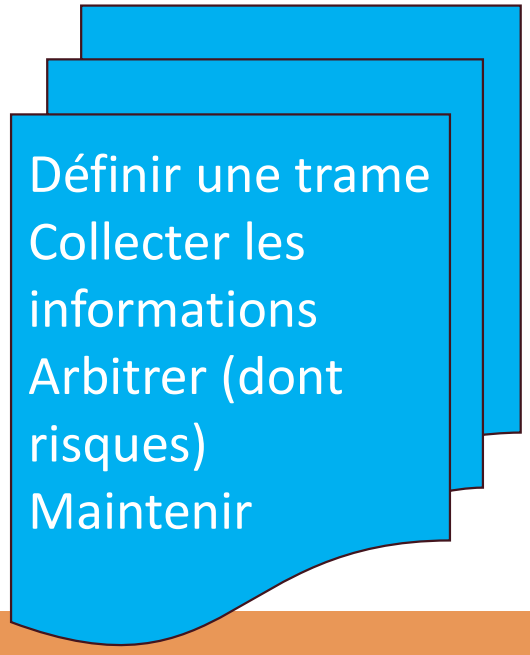
Risque

Sponsoriser
Définir des rôles
Animer
Processer la démarche
Documenter

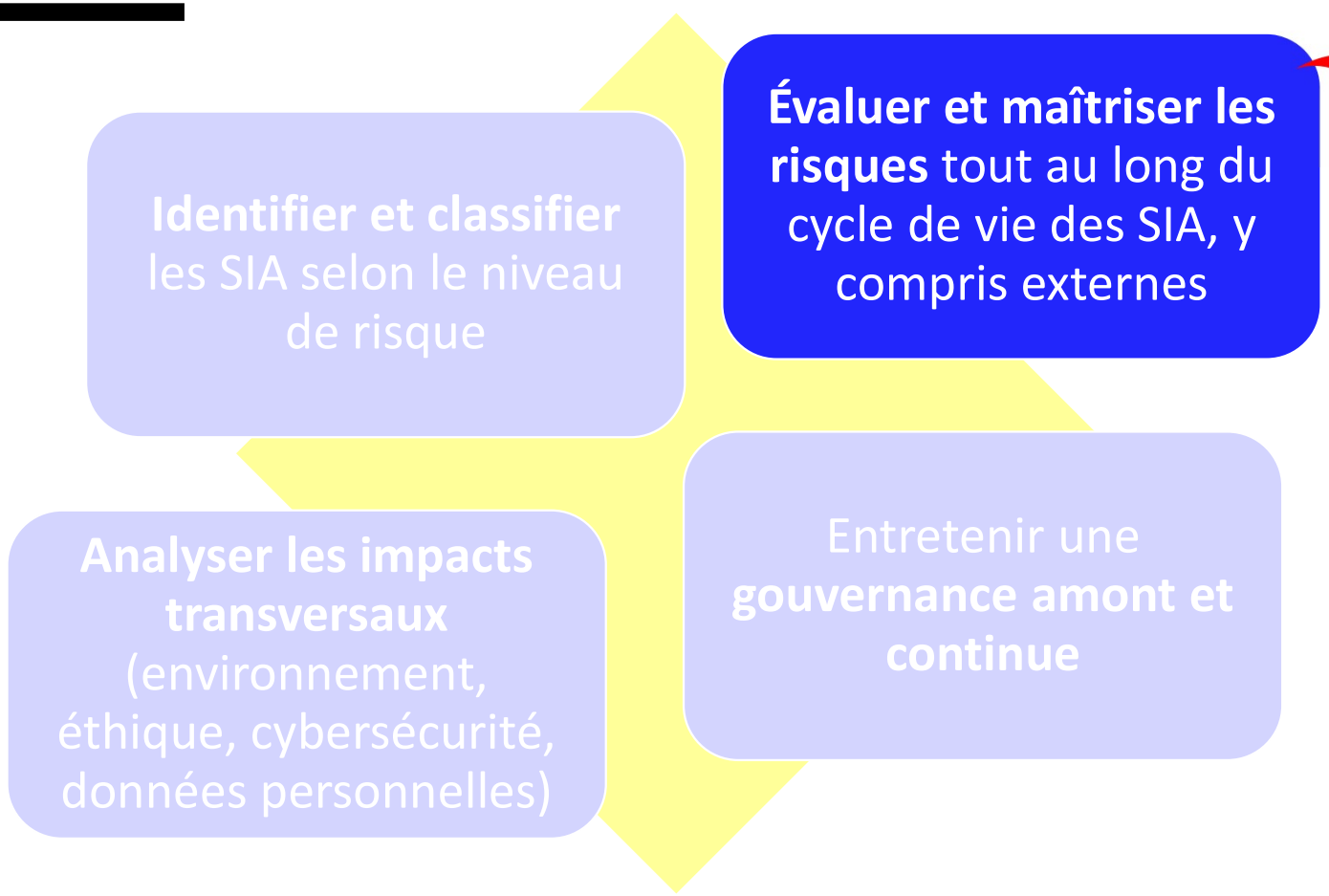
IDENTIFIER ET CLASSIFIER LES SIA

Registre

- **Documentation à triple vertu** :
  - Collecter les informations
  - Analyser les risques
  - Maintenir un référentiel vivant et commun
- **Le Registre comme base documentaire** :
  - Les finalités
  - Les traitements x les SIA
  - Les données
  - Les risques
  - Les liens avec les tiers (dont fournisseurs)
  - Les sécurités



EVALUER ET MAITRISER LES RISQUES



Protection dès la conception
Minimisation
Audits fournisseurs
Audits internes

EVALUER ET MAITRISER LES RISQUES

Protection dès la conception

Définir un process
Définir des rôles
Déployer
Animer
Implémenter
Tracer

Sur la base des risques identifiés :

- Démarche de maîtrise de chaque SIA **dès l'amont**
- Identification des **risques**
- Déploiement des **sécurités**
- **Tests** sur recettes
- **Corrections**
- Déploiement en production
- **Traçage des actions** pour les implémenter sur les itérations suivantes
- Contrôler, **auditer**

EVALUER ET MAITRISER LES RISQUES

Minimisation

- **Identification des données** utilisables
- Analyse de la **nécessité** de traiter des données brutes
- Analyse des **impacts à long terme** des traitements sur des données personnelles > dont profilage, décisions automatisées…
- Déploiement de **minimisations des données**
  - ➢ Minimisation de la collecte
  - ➢ Anonymisation
  - ➢ Pseudonymisation avec restrictions fortes sur les clés
- Déploiement de **minimisations des processus** de traitements
- **Destruction des données non nécessaires**
  - ➢ Jeux intermédiaires
  - ➢ Résultats nominatifs non nécessaires

Définir une politique
Définir un process
Tester puis déployer
Tracer
Auditer

EVALUER ET MAITRISER LES RISQUES

Audits fournisseurs

Fournisseur : tout organisme qui « *développe un système d'IA ou le fait développer*, *en vue de sa mise sur le marché ou de sa mise en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit* ».

Définir un process
Définir des rôles
Déployer
Animer
Encadrer dans des contrats
Tracer

- Déployer un **Questionnaire fournisseur**
- Intégrer le questionnaire dans les **achats**
- **Analyser** les retours, auditer, éventuellement tester et recetter
- **Décider de l'utilisation ou non** du SIA et des modalités de sécurisation
- **Encadrer** contractuellement
- **Auditer** régulièrement (risques d'évolutions non maîtrisées)

EVALUER ET MAITRISER LES RISQUES

Audits internes

Définir un process
Définir des rôles
Déployer
Animer
Encadrer dans des contrats
Tracer

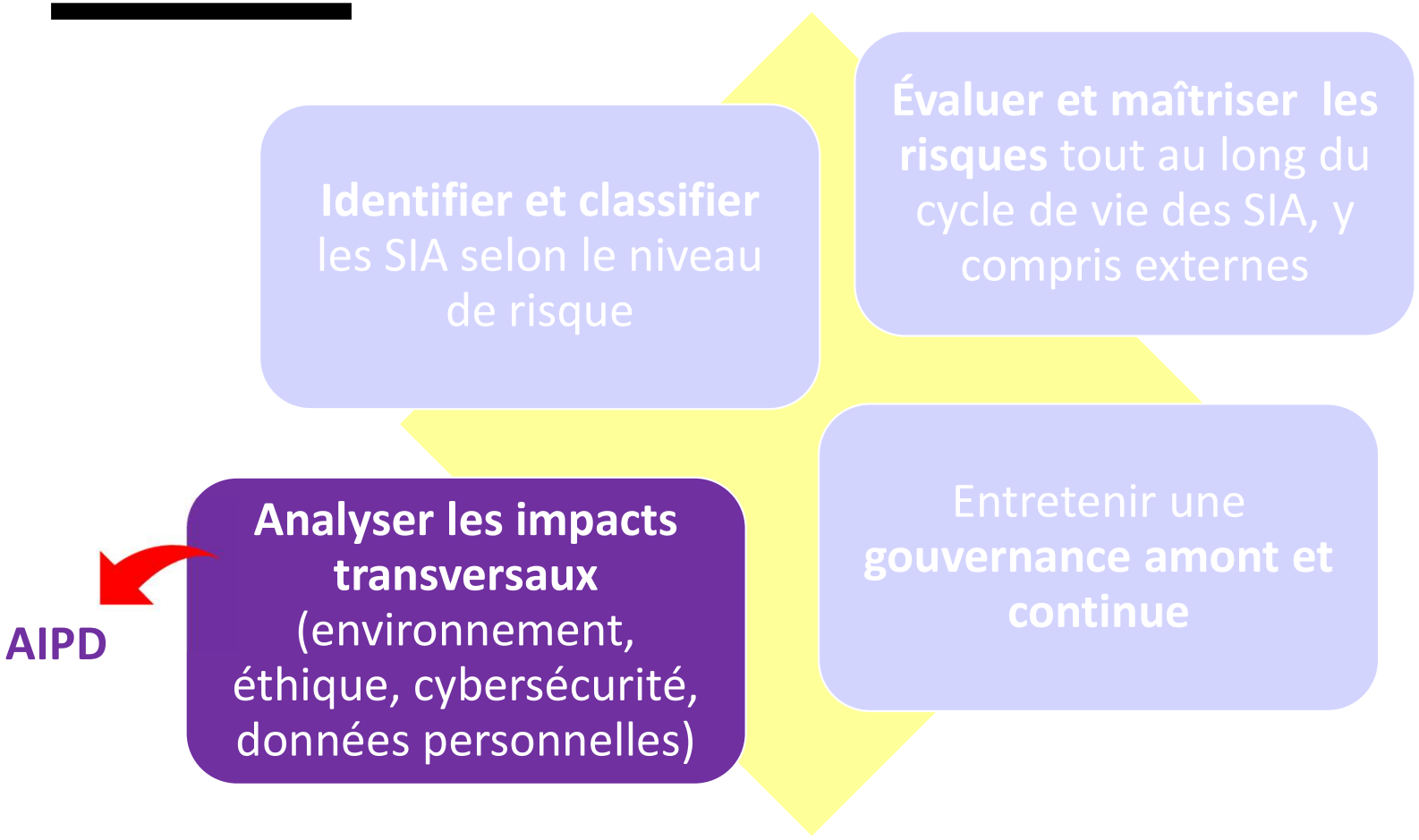
Traitements de données et SIA sont vivants :

- Évolutions techniques internes (versions)
- Evolutions des usages et données insérées, nouvelles finalités
- Environnement (attaques, influences)
- Apprentissage des SIA

Mettre en place des **processus de révision et d'audit**

- Suivre toutes évolutions, réanalyser le risques
- Modifier la documentation et les contrats
- Mettre en place des contrôles internes
- Auditer

ANALYSER LES IMPACTS



ANALYSER LES IMPACTS

AIPD Analyses d'impact sur la protection des données

Définir un process
Définir des rôles
Systématiser
Adapter modèle AIPD aux SIA
Documenter

- Tout SIA contenant des données personnelles doit faire l'objet d'une AIPD dès risques pour les personnes
- Tout analyse d'impact SIA peut s'adosser sur la méthodologie de l'AIPD :
  - Méthodologie couvrant les **finalités, la conformité et l'analyse des risques**
  - Nécessité d'**ouvrir l'analyse aux autres composantes du AI Act** : impacts, sécurité, éthique et RSE, gouvernance, apprentissage, déviances…

ANALYSER LES IMPACTS

	AI Act	RGPD
Objectif	Identifier les risques liés à l'IA sur la sécurité et les droits fondamentaux	Identifier les risques liés au traitement des données personnelles
Analyse obligatoire ?	Oui, pour les systèmes à haut risque (et dans certains cas, pour les usages publics)	Oui, pour les traitements susceptibles d'engendrer un risque élevé
Contenu	Description du système, des usages, des risques et des mesures de protection	Description du traitement, des finalités, des risques, des mesures techniques et organisationnelles
Documentation	Doit être incluse dans la documentation technique + conservée	Doit être formalisée (DPIA) et disponible pour l'autorité de contrôle
Mise à jour	Revue continue **requise**	Revue périodique **recommandée** (notamment si les risques changent)

GOUVERNER LES SIA

Identifier et classifier les SIA selon le niveau de risque

Évaluer et maîtriser les risques tout au long du cycle de vie des SIA, y compris externes

Analyser les impacts transversaux (environnement, éthique, cybersécurité, données personnelles)

Entretenir une **gouvernance amont et continue**

Responsabilisation
Audit de conformité
Formation
Politiques
Process de validation
Suivi + documentation
Droits des personnes

GOUVERNER LES SIA

Responsabilisation

Analyser la responsabilité SIA par SIA
Définir des rôles
Encadrer
Gouverner

Les responsabilités de la conformité IA sont :

- **Sensiblement les mêmes que pour le RGPD** : notions de responsables à différents degrés, qui doivent s'assurer de leurs obligations + régime de sanctions
- **Mais quand même différentes** : pas de RT, RTco et ST, mais :
  - **Fournisseur (provider)** : Celui qui développe un système d'IA.
  - **Déployeur (user)** : Celui qui utilise le système d'IA à des fins professionnelles.
  - **Importateur** : Fait entrer un système d'IA sur le marché européen.
  - **Distributeur** : Met sur le marché un système d'IA sans l'avoir modifié.

GOUVERNER LES SIA

Mobiliser, Former et Piloter les acteurs

Identifier les acteurs
Définir des rôles
Former
Mobiliser
Gouvernance

Les acteurs de la conformité IA sont :

- **Sensiblement les mêmes que pour le RGPD** : Direction générale, métiers, DPO, DSI, il faut donc qu'ils se mobilisent
- **Mais ouverts à d'autres acteurs** : il faut aussi associer :
  - **Data owners** : ce sont souvent leurs données qui sont traitées
  - **Data analysts** : au cœur de l'exploitation des SIA
  - **Data governors** : ceux qui gouvernent la donnée globalement ou par secteur / BU…
  - **Filière RSE / éthique** : impacts humains et environnementaux
  - **Ingénieries informatique et cybersécurité** : nécessité de comprendre et maîtriser les impacts du LLM et des processus des SIA, nécessité de comprendre et maîtriser les impacts cybers

GOUVERNER LES SIA

Documenter

Comme pour le RGPD, la documentation est un pilier central de l'AI Act

Obligations vis-à-vis des personnes assez équivalentes au RGPD :

- **Documentation technique** : inscrire explicitement les SIA dans les formulaires, dans les politiques de confidentialités… finalités, moyens… + mentions de génération par une IA, risques de contenus trompeurs…
- **Instructions d'utilisation** : cf RGPD art 22
- **Conservation et accessibilité**: spécificité forte AI Act
- **Transparence pour les IA génératives**
- **Support pour la gestion de la conformité,** audits, conformités connexes (dont RGPD)

GOUVERNER LES SIA

Information & Droits des personnes

AI Act : protéger les droits fondamentaux des personnes face aux systèmes d'intelligence artificielle

- **obligations** pour garantir la transparence, la sécurité et le respect des libertés individuelles.

Obligations vis-à-vis des personnes assez équivalentes au RGPD :

- **Information** : inscrire explicitement les SIA dans les formulaires, dans les politiques de confidentialités… finalités, moyens… + mentions de génération par une IA, risques de contenus trompeurs…
- **Droits à l'intervention humaine** : cf RGPD art 22
- **Protection contre les discriminations** : spécificité forte AI Act
- **Consentement**
- **Droits de recours et de réparation**

Rédiger des politiques
Définir des procédures
Répondre aux demandes
Tracer