

# **Veille Informatique**

**Sujet:** Évolution des lois RGPD : Nouvelles obligations pour les entreprises

## **Sommaire :**

1. Tendances Générales (2023-2025)
2. Innovations et ruptures majeures
3. Évolutions Législatives 2023-2025
4. Risques émergents et opportunités
5. Sources et événements marquants
6. Conclusion pour les entreprises
7. Synthèse
8. Plan Opérationnel 2024-2025

## 1. Tendances Générales (2023-2025)

### **Renforcement de la protection des données**

- Durcissement du RGPD : Face aux enjeux IA et cybersécurité, plusieurs projets européens visent à mieux encadrer les usages des données personnelles.
- RGPD et IA : Croisement de la réglementation sur les données personnelles et les traitements automatisés via des intelligences artificielles.
- Nouvelle responsabilité algorithmique : Obligation d'explicabilité renforcée pour les algorithmes traitant des données personnelles.

### **Accélération de l'encadrement de l'IA**

- Adoption de l'[AI Act](<https://artificialintelligenceact.eu/>) (mars 2024) : Première législation mondiale encadrant l'usage de l'intelligence artificielle, avec impacts directs sur la collecte de données.
- Interaction RGPD / AI Act : Les entreprises doivent désormais prouver que l'utilisation de l'IA respecte aussi les principes de protection des données.

### **Sécurité et résilience numérique**

- Adoption de la directive NIS2 (janvier 2023): Nouvelles obligations pour les infrastructures critiques et les entreprises en matière de cybersécurité.
- Loi sur la cyber-résilience (Cyber Resilience Act, 2024) : Certification obligatoire de la sécurité pour tous les produits numériques connectés.

## 2. Innovations et ruptures majeures

### **Nouveaux outils et services**

- Privacy Enhancing Technologies (PETs) : Technologies d'anonymisation et de cryptage avancé de plus en plus utilisées pour assurer la conformité RGPD.
- Outils de "Privacy by Design": Développement d'outils intégrant la protection des données dès la conception (Data Protection Impact Assessment automatisé).
- Plateformes de gestion du consentement (CMP) nouvelle génération : Automatisation des obligations RGPD/AI Act combinées.
- Exemples : OneTrust, Didomi évoluent vers des versions IA-native.

### **Pratiques émergentes**

- Data Governance AI-Driven : Gouvernance des données alimentée par IA pour monitorer automatiquement la conformité en temps réel.
- Certification de la conformité : Multiplication des labels RGPD/IA pour garantir la confiance (ex. : Europrivacy Certification, conforme à l'article 42 RGPD).

### 3. Évolutions Législatives 2023-2025

#### **2023**

- Directive NIS2 (entrée en vigueur janvier 2023) :
  - Champ étendu (PME critiques incluses).
  - Sanctions renforcées (jusqu'à 10 millions € ou 2 % du CA annuel).
  - Obligation de notification de cyberattaque sous 24h.
- Proposition de règlement ePrivacy toujours en discussion :
  - Vise à compléter le RGPD en encadrant spécifiquement les communications électroniques.

#### **2024**

- Adoption de l'AI Act (mars 2024) :
  - Catégorisation des IA par risque.
  - Nouvelles obligations pour les systèmes à "haut risque" (explicabilité, transparence, auditabilité).
  - Interdiction de certains usages IA jugés trop intrusifs (ex : reconnaissance émotionnelle en entreprise).
- Renforcement du RGPD via recommandations EDPB :
  - Mise à jour des lignes directrices sur le transfert international de données.
  - Surveillance renforcée sur l'usage des bases légales "intérêt légitime" et "consentement".
- Déploiement du Data Governance Act (DGA) :
  - Création de tiers de confiance pour l'échange sécurisé des données sensibles.

#### **2025**

- Application complète du Cyber Resilience Act (janvier 2025) :
  - Exigences de cybersécurité dès la phase de conception.
  - Déclarations de conformité obligatoires pour produits numériques (similaire au marquage CE).
- Règlement Data Act (en application 2025) :
  - Partage obligatoire des données industrielles dans certaines conditions.
  - Obligation de portabilité des données renforcée, complétant les articles 20 et 25 du RGPD.

#### 4. Risques émergents et opportunités

##### **Risques**

- Non-conformité croisée RGPD/AI Act : Oblige les entreprises à restructurer leur documentation juridique (registre de traitement + audit IA).
- Explosion des coûts de conformité: Gouvernance data, cybersécurité, évaluation d'impact exigent de lourds investissements.
- Multiplication des sanctions : Les autorités (CNIL, EDPS, etc.) sont plus sévères et collaborent plus étroitement.
  - Ex : Meta (Facebook) a écopé d'une amende record de 1,2 milliard € en mai 2023 pour transferts illicites de données vers les USA.

##### **Opportunités**

- Développement de nouveaux services de conformité (consulting RGPD/IA, outils de conformité SaaS).
- Valorisation des labels de confiance pour renforcer l'image de marque (ex : label "Privacy First").
- Innovation éthique : La conformité RGPD/IA devient un argument marketing, favorisant les solutions éthiques et transparentes.
- Accès facilité aux financements européens pour les entreprises mettant en œuvre la gouvernance des données (Horizon Europe, Digital Europe Programme).

#### 5. Sources et événements marquants

Date	Événement	Lien
Janvier 2023	Entrée en vigueur de la directive NIS2	[ENISA - NIS2 Overview] ( <a href="https://www.enisa.europa.eu/topics/nis-directive/nis2">https://www.enisa.europa.eu/topics/nis-directive/nis2</a> )
Mars 2024	Adoption du AI Act par le Parlement européen	[AI Act text]( <a href="https://artificialintelligenceact.eu/the-act/">https://artificialintelligenceact.eu/the-act/</a> )
Mai 2023	Amende de 1,2 Mds € contre Meta	[CNIL - Actualités sur Meta] ( <a href="https://www.cnil.fr/fr/meta-privee-dune-1-2-milliard-deuros">https://www.cnil.fr/fr/meta-privee-dune-1-2-milliard-deuros</a> )
2024	Déploiement du Data Governance Act	[EU Data Strategy]( <a href="https://digital-strategy.ec.europa.eu/en/policies/data-governance-act">https://digital-strategy.ec.europa.eu/en/policies/data-governance-act</a> )
Janvier 2025	Application du Cyber Resilience Act	[EU Cyber Resilience Act] ( <a href="https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act">https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act</a> )

6. Conclusion pour les entreprises :

Ce qu'il faut faire dès 2024-2025	Détail
Auditer les usages d'IA et mettre en conformité avec l'AI Act	Protéger les données dès la conception des projets numériques
Renforcer la cybersécurité pour répondre aux normes NIS2 et Cyber Resilience Act	Audits réguliers + procédures d'alerte interne
Mettre à jour la gouvernance RGPD/Data Act	Gestion centralisée des consentements, des risques, et du transfert de données
Investir dans la "Privacy by Design"	Protéger les données dès la conception des projets numériques

7. Synthese

Date	Événement	Impact sur entreprises	Actions nécessaires
Jan 2023	Entrée en vigueur NIS2 (cybersécurité)	Extension du champ des entreprises concernées	Mettre à jour plan cybersécurité, nommer un responsable sécurité
Mai 2023	Sanction Meta (1,2 Md€)	Sévérité des sanctions RGPD confirmée	Renforcer documentation des transferts de données hors UE
Mars 2024	Adoption AI Act	Réglementation de l'usage d'IA en entreprise	Identifier et classer ses IA, faire évaluer les risques
2024	Déploiement Data Governance Act (DGA)	Nouvelles obligations sur l'échange de données	Nommer un « Data Steward » interne, formaliser les politiques de partage
Jan 2025	Application Cyber Resilience Act	Conception sécurisée obligatoire pour produits numériques	Vérifier conformité sécurité pour tous produits/services connectés
2025	Application du Data Act	Droit à la portabilité élargi, accès obligatoire aux données industrielles	Développer des APIs sécurisées, revoir contrats de données

**Action Rapide – Plan Opérationnel 2024-2025**

**Objectif :** Être 100% conforme RGPD, AI Act et Cyber Résilience

Priorités immédiates (2024)

- [ ] Audit IA en entreprise :
  - Identifier IA à "haut risque" selon AI Act.
  - Préparer documentation explicative et évaluation des risques IA.
- [ ] Mise à jour du Registre des traitements RGPD :
  - Ajout des traitements automatisés IA.
  - Vérification des bases légales et du consentement.
- [ ] Gouvernance de la Data :
  - Définir des règles d'échange et d'utilisation des données (Data Governance Act).
  - Désigner un Responsable Data interne.
- [ ] Sécuriser la cybersécurité :
  - Revue complète de la stratégie cybersécurité NIS2.
  - Formaliser un plan de réponse aux incidents.

Roadmap 2025

Mois	Action	Responsable
Janvier	Audit de conformité produits numériques (Cyber Resilience Act)	CISO (Chief Information Security Officer)
Mars-Avril	Révision contrats et portabilité des données (Data Act)	DPO + Service Juridique
Juin	Certification ou labellisation « Privacy First » ou Europrivacy	DPO
Décembre	Simulation d'incident cyber + rapport de conformité IA	CISO + DPO

Checklist conformité 2025

- [ ] IA cartographiées, classifiées, documentées
- [ ] Registre RGPD mis à jour avec IA et bases légales adaptées
- [ ] Gouvernance data sécurisée, procédures DGA en place
- [ ] Politique cybersécurité conforme Cyber Resilience Act
- [ ] Portabilité et accès aux données prêts pour le Data Act