Feuille de route
de conformité
au Règlement IA

Réalisée par LE CLUB DPO **avec le concours de la CNIL**

Le Règlement européen sur l'Intelligence Artificielle (RIA) représente un tournant majeur dans la régulation technologique. Adopté en mars 2024, ce texte instaure un cadre juridique contraignant pour tous les acteurs - publics et privés - qui développent, intègrent ou utilisent des systèmes d'IA. Cette révolution réglementaire s'applique progressivement de février 2025 à août 2026/2027, laissant aux organisations une fenêtre d'opportunité limitée pour se conformer.

Gouvernance et pilotage
Structurer l'organisation pour anticiper et maîtriser

Cartographie des systèmes d'IA
Identifier et documenter l'écosystème IA de l'organisation

Qualification des rôles
Déterminer les responsabilités selon les fonctions exercées

Plan d'actions RIA/RGPD
Intégrer les démarches de conformité de manière cohérente

Gestion des risques
Appliquer les obligations selon les niveaux de risque

Accountability et preuves
Démontrer et maintenir la conformité dans la durée

CONTEXTE

Le contexte réglementaire : une révolution en marche

Le Règlement IA marque une évolution fondamentale dans l'approche européenne de la régulation technologique. Contrairement aux textes précédents, il adopte un périmètre d'application particulièrement large, englobant tous les systèmes d'IA, qu'ils soient développés en interne, achetés sur étagère ou intégrés à des solutions existantes.

Cette réglementation s'articule autour d'une logique de risques, établissant des obligations différenciées mais néanmoins contraignantes selon l'usage et le niveau de risque des systèmes déployés.

Cette approche graduée permet aux organisations de concentrer leurs efforts sur les systèmes les plus critiques tout en maintenant un niveau de vigilance approprié sur l'ensemble de leur écosystème IA.

L'enjeu dépasse largement la simple conformité réglementaire.

Il s'agit désormais d'un impératif stratégique touchant l'image de marque, la capacité d'innovation responsable et la compétitivité sur les marchés européens. Les organisations qui anticipent ces changements transformeront cette contrainte réglementaire en un avantage concurrentiel durable.

CALENDRIER D'ENTRÉE EN VIGUEUR

Application progressive de février 2025 à août 2026/2027

PÉRIMÈTRE ÉTENDU

Tous les systèmes d'IA, internes comme externes

APPROCHE PAR LES RISQUES

Obligations différenciées selon l'usage

ARTICULATION

Comprendre l'articulation RIA-RGPD

Une distinction fondamentale doit être établie : le RGPD encadre les données personnelles tandis que le RIA encadre tous les systèmes d'IA.
Ces deux réglementations ne se substituent pas l'une à l'autre mais s'additionnent, créant un environnement réglementaire complexe où chaque texte porte ses propres exigences dans son domaine de compétence.
Cette coexistence réglementaire implique que les organisations doivent désormais naviguer entre deux logiques complémentaires : la protection des données personnelles d'une part, et la gouvernance des systèmes d'intelligence artificielle d'autre part.
L'intersection de ces deux domaines crée des zones de complexité particulière, notamment lorsque des systèmes d'IA traitent des données personnelles.

RGPD - Protection des données

- ✓ RGPD - Protection des données
- ✓ Focus sur les données personnelles
- ✓ Droits des personnes concernées
- ✓ Accountability et documentation
- ✓ Analyse d'impact

RIA - Gouvernance de l'IA

- ✓ RIA - Gouvernance de l'IA
- ✓ Focus sur tous les systèmes d'IA
- ✓ Approche par niveaux de risque
- ✓ Obligations techniques spécifiques
- ✓ Surveillance et conformité continue

L'approche optimale consiste à développer une stratégie intégrée qui traite ces deux réglementations de manière cohérente, en identifiant les synergies possibles et en évitant les redondances.
Cette vision globale permettra aux DPO et aux équipes de conformité de maximiser l'efficacité de leurs efforts tout en garantissant une couverture réglementaire complète.

ÉTAPE 1

Gouvernance et pilotage

La mise en place d'une gouvernance robuste constitue le socle indispensable de toute démarche de conformité réussie.

Cette première étape consiste à désigner un responsable du projet "Conformité RIA" , qui pourra être le DPO, le RSSI, un juriste spécialisé ou un responsable d'une cellule IA dédiée. Ce pilote doit bénéficier d'une légitimité organisationnelle claire et d'un accès direct à la direction générale.

L'efficacité de cette gouvernance repose sur la création d'une équipe projet transversale réunissant les compétences essentielles : informatique, juridique, innovation et représentants des métiers utilisateurs d'IA.

Cette diversité de profils garantit une approche holistique qui prend en compte tous les aspects de la problématique, des contraintes techniques aux enjeux business en passant par les exigences réglementaires.

Désignation d'un pilote

Nommer un responsable avec une lettre de mission claire définissant son rôle de coordination, d'arbitrage et de reporting vers la direction.

Équipe transversale

Constituer un groupe de travail réunissant IT, juridique, innovation et métiers avec une comitologie définie.

Feuille de route interne

Établir un planning prévisionnel avec RACI, livrables et présentation de kickoff à la direction.

Formation des équipes

Sensibiliser les services concernés aux enjeux juridiques, techniques et éthiques de l'IA.

La définition d'une feuille de route interne détaillée avec calendrier, livrables et allocation de moyens permet de transformer cette ambition en plan d'action concret. Cette planification doit intégrer les contraintes opérationnelles de l'organisation tout en respectant les échéances réglementaires.
L'investissement dans la formation des équipes constitue un prérequis indispensable pour garantir l'appropriation des enjeux par l'ensemble des parties prenantes.

ÉTAPE 1

Gouvernance et pilotage

MESSAGE CLÉ AU DIRIGEANT

Gouverner l'IA, c'est maîtriser les risques tout en anticipant les opportunités.

ÉTAPE 2

Cartographie des systèmes d'IA

La cartographie constitue l'épine dorsale de la démarche de conformité. Elle vise à identifier exhaustivement tous les systèmes pouvant être qualifiés de systèmes d'IA selon la définition de l'article 3 du RIA. Cette phase d'inventaire doit couvrir tant les systèmes existants que ceux en projet, qu'ils soient développés en interne, achetés sur le marché ou intégrés à des solutions tierces.

La complexité de cette étape réside dans la nécessité de documenter précisément le niveau de risque de chaque système identifié selon les catégories établies par le Règlement : risque minimal, obligation de transparence, risque élevé ou systèmes interdits. Cette qualification détermine directement l'ampleur des obligations applicables et doit donc être menée avec une rigueur particulière.

Inventaire exhaustif

Identifier tous les systèmes algorithmiques de l'organisation et déterminer lesquels relèvent de la définition de l'IA selon l'article 3 du RIA.

Évaluation des risques

Classer chaque système selon les quatre niveaux : minimal, transparence, risque élevé, ou interdit. Justifier cette affectation de manière documentée.

Attribution des rôles

Identifier pour chaque système qui est développeur, déployeur, et les autres rôles selon les définitions du Règlement.

La cartographie doit repérer les systèmes d'IA à usage général et ceux à risque systémique, soumis à des obligations particulières. Documenter les finalités, les données et leur sensibilité au regard du RGPD permet d'anticiper les interactions entre les deux réglementations.

Cette cartographie doit être tenue à jour en continu. L'évolution rapide des technologies et des usages impose une vigilance constante pour garantir la qualité et l'exhaustivité des informations. Cela implique un contrôle constant.

ÉTAPE 2

Cartographie des systèmes d’IA

MESSAGE CLÉ AU DIRIGEANT

Cartographier, c'est comme avec le RGPD : faire l'état des lieux des risques et exigences applicables.

Connaître le périmètre à traiter, c'est la base de toute action efficace.

ÉTAPE 3

Qualification des rôles et responsabilités

La qualification précise des rôles constitue un enjeu majeur car elle détermine directement l'étendue des obligations applicables à l'organisation.
Le Règlement IA définit cinq rôles principaux : fournisseur, déployeur, importateur, distributeur et mandataire.
Chaque rôle porte des responsabilités spécifiques et cumulatives, nécessitant une analyse fine de la position de l'organisation dans la chaîne de valeur de l'IA.

Fournisseur

Développe ou fait développer un système d'IA et le met sur le marché sous son nom ou sa marque

Déployeur

Utilise un système d'IA sous sa propre autorité (hors usage personnel non professionnel)

Importateur, distributeur ou mandataire

Est impliqué dans la distribution dans l'UE d'un système d'IA haut risque portant le nom d'un organisme tiers hors UE

Le fournisseur porte la responsabilité la plus lourde : conformité technique, évaluation de conformité avant mise sur le marché, documentation technique exhaustive, marquage CE si requis, système de gestion de la qualité, surveillance post-commercialisation et mesures correctives. Ces obligations s'étendent également à la coopération avec les autorités compétentes et à la désignation d'un mandataire UE si l'organisation est établie hors Union.

Le déployeur assume des responsabilités opérationnelles cruciales : utilisation conforme aux instructions, surveillance humaine effective, vérification de la qualité des données d'entrée, conservation des journaux, signalement des incidents graves et réalisation d'analyses d'impact si nécessaire. Ces obligations impliquent une transformation profonde des pratiques organisationnelles et une montée en compétence des équipes utilisatrices.

Responsabilités du Fournisseur

- ✓ Conformité technique complète
- ✓ Évaluation de conformité préalable
- ✓ Documentation technique détaillée
- ✓ Système de gestion qualité
- ✓ Surveillance post-marché

Responsabilités du Déployeur

- ✓ Usage conforme aux instructions
- ✓ Surveillance humaine effective
- ✓ Contrôle qualité des données
- ✓ Conservation des journaux
- ✓ Formation du personnel

Les rôles d' importateur, distributeur et mandataire portent des responsabilités plus ciblées. L'importateur doit vérifier la conformité des systèmes importés, le distributeur s'assure de la disponibilité de la documentation appropriée, tandis que le mandataire sert d'interlocuteur UE pour les fournisseurs établis hors Union.

ÉTAPE 3

Qualification des rôles et responsabilités

MESSAGE CLÉ AU DIRIGEANT

Chacun son rôle, chacun ses responsabilités, chacun doit les connaître.

ÉTAPE 4

Élaboration du plan d'actions RIA/RGPD

L'élaboration d'un plan d'actions intégré RIA/RGPD constitue le pivot stratégique de la démarche de conformité. Cette approche holistique vise à imbriquer harmonieusement les deux réglementations pour éviter les redondances, optimiser les ressources et créer des synergies entre les obligations respectives.
Cette intégration s'avère particulièrement critique lorsque les systèmes d'IA traitent des données personnelles.

Au niveau des systèmes, le plan doit prévoir la mise en œuvre d'un système de management qualité pour les IA à haut risque, intégrant les exigences de robustesse, de sécurité et de traçabilité. Les dispositifs d'alerte, d'audit et de retrait doivent être dimensionnés selon les niveaux de risque identifiés.
La documentation technique et informationnelle requise par le RIA doit se conjuguer avec les obligations documentaires du RGPD.

Management qualité IA

Systèmes de qualité pour IA haut risque avec robustesse, sécurité et traçabilité intégrées

Dispositifs d'alerte

Mécanismes d'audit, d'alerte et de retrait dimensionnés selon les niveaux de risque

Documentation intégrée

Documentation technique RIA conjuguée avec les obligations documentaires RGPD

Le plan d’actions RIA/RGPD doit instaurer une gouvernance IA claire au sein de l’organisation, comprenant comité de pilotage, task force opérationnelle, politique générale, revues périodiques et contrôles.
Celle-ci doit s'interfacer efficacement avec l'organisation RGPD, en définissant clairement le rôle du DPO dans les projets IA traitant des données personnelles.
Mettre en place un programme de formation IA ciblé est un investissement stratégique majeur. Il doit couvrir les aspects juridiques, techniques et éthiques de l'IA tout en intégrant les dimensions RGPD pertinentes.
La formation doit être adaptée aux différentes profils et parties prenantes.

ÉTAPE 4

Élaboration du plan d'actions RIA/RGPD

MESSAGE CLÉ AU DIRIGEANT

La conformité RIA c'est maintenant.

Plus tard, ce sera plus cher et potentiellement trop tard.

ÉTAPE 5

Gestion intégrée des risques RIA/RGPD

La gestion des risques constitue le cœur opérationnel de la conformité, nécessitant une approche méthodologique rigoureuse pour chaque projet IA.
Cette démarche implique de prévoir une analyse de risques systématique intégrant simultanément les exigences du RIA et du RGPD, créant une vision unifiée des enjeux de conformité et permettant une optimisation des efforts de mise en conformité.

L'intégration des analyses de risques IA dans les analyses d'impact RGPD existantes représente une évolution naturelle des pratiques organisationnelles. Cette convergence permet d'éviter la duplication des efforts tout en garantissant une couverture exhaustive des risques.
Les systèmes d'IA à haut risque, définis conformément à l'Annexe 3 du RIA, nécessitent une attention particulière avec des mesures de protection renforcées.

Analyse de risques

Évaluation systématique pour chaque projet IA intégrant RIA et RGPD

IA haut risque

Identification selon l'Annexe 3 avec mesures de protection renforcées

Privacy by Design

Intégration des projets IA dans la démarche privacy existante

Avis DPO

Consultation systématique pour les SIA traitant des données personnelles

Droits des personnes

Anticipation de l'application des droits RGPD dans les projets IA

Violations de données

Anticipation des conséquences sur les données traitées en IA

L'intégration dans la démarche Privacy by Design existante constitue une approche pragmatique permettant de capitaliser sur les processus déjà établis. Cette intégration implique de systématiser la consultation du DPO pour tous les projets IA traitant des données personnelles, garantissant ainsi une évaluation experte des enjeux de protection des données dès la conception.

L'anticipation de l'application des droits RGPD des personnes concernées dans le contexte de l'IA représente un défi technique et organisationnel majeur.
Les droits d'accès, de rectification, d'effacement et de portabilité doivent être techniquement réalisables même dans des systèmes d'apprentissage automatique complexes. Cette exigence impose des choix architecturaux spécifiques dès la phase de conception.

ÉTAPE 5

Gestion intégrée des risques RIA/RGPD

MESSAGE CLÉ AU DIRIGEANT

Gérer ses risques RGPD/IA dès le départ, c'est s'assurer un avenir plus serein.

ÉTAPE 6

Accountability et preuves de conformité

L'intégration de la preuve de conformité dans les processus commerciaux transforme cette contrainte réglementaire en avantage concurrentiel.
La capacité à démontrer une gouvernance IA exemplaire devient un atout différenciant dans les appels d'offres, les négociations contractuelles et les relations avec les partenaires. Cette valorisation de la conformité justifie largement les investissements consentis.

La mise en place d'une comitologie RIA structurée avec revues périodiques, tableaux de bord de suivi et reporting vers la direction générale institutionnalise la démarche de conformité. Cette gouvernance pérennise les efforts de mise en conformité et garantit leur maintien dans la durée, même en cas d'évolution des équipes ou des priorités organisationnelles.

Documentation vivante

Maintien d'une documentation complète et actualisée de la conformité RIA, intégrée aux processus opérationnels

Outillage d'audit

Mise en place d'outils de contrôle automatisés et de tableaux de bord de suivi de la conformité

IA Compliance by Design

Intégration de la conformité dès la conception des nouveaux systèmes et processus

Comitologie RIA

Structure de gouvernance dédiée avec revues périodiques et reporting vers la direction

Intégrer la preuve de conformité dans les processus commerciaux crée un avantage concurrentiel. Démontrer une gouvernance IA exemplaire devient un atout différenciant dans les appels d'offres et les relations commerciales.
Cela justifie largement les investissements consentis.
La mise en place d'une comitologie RIA avec revues périodiques, tableaux de bord de suivi et reporting vers la direction générale institutionnalise la démarche de conformité. Cela permet maintenir le niveau de conformité dans le temps.

ÉTAPE 6

Accountability et preuves de conformité

MESSAGE CLÉ AU DIRIGEANT

La conformité est un actif stratégique qui demain distinguera les organisations de confiance des autres.

C'est un investissement dans votre durabilité.

FEUILLE DE ROUTE

CONCLUSION

Au terme de cette feuille de route, l'organisation dispose d'un écosystème de conformité mature et pérenne, capable de s'adapter aux évolutions réglementaires et technologiques. Cette maturité constitue un socle solide pour l'innovation responsable et la croissance durable dans l'économie numérique de demain.

LE CLUB DPO

Ce document a été réalisé par les membres du Club DPO.
Plus de ressources sur https://clubdpo.fr