# Entrée en vigueur du règlement européen sur l'IA : les premières questions-réponses de la CNIL

*12 juillet 2024*

*Depuis un an, la CNIL a lancé son plan d'action pour promouvoir une IA respectueuse des droits des personnes sur leurs données et sécuriser les entreprises innovant en la matière dans leur application du RGPD.*
*À l'occasion de la publication du règlement IA au JOUE, la CNIL répond à vos questions sur ce nouveau texte.*

Le règlement européen sur l'IA (ou AI Act) vient d'être publié au Journal officiel de l'Union européenne (JOUE) et entrera progressivement en application à partir du 1er aout 2024. Qui est concerné ? Qu'est-ce qui distingue le règlement IA du RGPD et en quoi se complètent-ils ?

# Présentation du règlement IA

## Qu'est-ce que prévoit le règlement IA (ou AI Act) ?

Le règlement européen sur l'IA (RIA) est la première législation générale (ou exhaustive) au monde sur l'intelligence artificielle. Il vise à **encadrer le développement, la mise sur le marché et l'utilisation de systèmes d'intelligence artificielle (IA), qui peuvent poser des risques pour la santé, la sécurité ou les droits fondamentaux.**

### Quatre niveaux de risque

Le RIA propose **une approche fondée sur les risques en classant les systèmes d'IA en quatre niveaux :**

- **Risque inacceptable : le RIA interdit un ensemble limité de pratiques contraires aux valeurs de l'Union européenne et aux droits fondamentaux.**

  *Exemples : la notation sociale, l'exploitation de la vulnérabilité des personnes, le recours à des techniques subliminales, l'utilisation par les services répressifs de l'identification biométrique à*

*distance en temps réel dans des espaces accessibles au public, la police prédictive ciblant les individus, reconnaissance des émotions sur le lieu de travail et dans les établissements d'enseignement.*

- **Haut risque : le RIA définit les systèmes d'IA comme étant à haut risque lorsqu'ils peuvent porter atteinte à la sécurité des personnes ou à leurs droits fondamentaux ce qui justifie que leur développement soit soumis à des exigences renforcées** (évaluations de conformité, documentation technique mécanismes de gestion des risques). Ces systèmes sont listés dans l'annexe I pour les systèmes intégrés dans des produits qui font déjà l'objet d'une surveillance de marché (dispositifs médicaux, jouets, véhicules, etc.) et dans l'annexe III pour les systèmes utilisés dans huit domaines spécifiques.

  *Exemples : systèmes biométriques, des systèmes utilisés dans le recrutement, ou pour des usages répressifs.*

- **Risque spécifique en matière de transparence** : **le RIA soumet des systèmes d'IA à des obligations de transparence spécifiques,** notamment en cas de risque manifeste de manipulation.

  *Exemples : recours à des chatbots ou à la génération de contenu artificiel.*

- **Risque minimal : pour tous les autres systèmes d'IA, le RIA ne prévoit pas d'obligation spécifique.** Il s'agit de la très grande majorité des systèmes d'IA actuellement utilisés dans l'UE ou susceptibles de l'être selon la Commission européenne.

### Les modèles d'IA à usage général

Par ailleurs, le RIA encadre aussi **une nouvelle catégorie de modèles dits à usage général**, notamment **dans le domaine de l'IA générative**. Ces modèles se définissent par leur capacité à servir à un grand nombre de tâches (comme les grands modèles de langage, ou *LLM*, tels que ceux proposés par les sociétés Mistral AI ou OpenAI), ce qui les rend difficiles à classer dans les catégories précédentes.

**Pour cette catégorie, le RIA prévoit plusieurs niveaux d'obligation, allant de mesures de transparence et de documentation minimales** (article 53) **à une évaluation approfondie et la mise en place de mesures d'atténuation des risques systémiques que certains de ces modèles pourraient comporter**, notamment en raison de leur puissance : risques d'accidents majeurs, d'utilisation à mauvais escient pour lancer des cyberattaques, la propagation de biais préjudiciables (relatifs à l'appartenance ethnique ou au genre par exemple) et aux effets discriminatoires à l'encontre de certaines personnes, etc. (voir en particulier le considérant 110).

Pour aller plus loin : consulter la FAQ de la Commission européenne

## Qui contrôlera l'application du RIA dans l'UE et en France ?

Le RIA prévoit **une structure de gouvernance qui s'opère à deux niveaux.**

## La gouvernance au niveau européen

La coopération européenne, visant à permettre **une application cohérente du RIA**, est bâtie autour du **Comité européen de l'IA** (articles 65 et 66). Cet organe rassemble des **représentants de haut niveau de chaque État membre** ainsi que, à titre d'observateurs, du Contrôleur européen de la protection des données (l'homologue de la CNIL auprès des institutions européennes). **Le Bureau de l'IA** (institution de la Commission européenne nouvellement créé) participe mais sans droit de vote.

Par ailleurs, le RIA introduit deux autres instances destinées à éclairer le Comité de l'IA dans ses choix :

- le forum consultatif (organe multi-acteurs qui pourra conseiller le Comité européen de l'IA et la Commission européenne dans l'exercice de leurs missions) ; et
- le groupe scientifique d'experts indépendants (scientifiques de haut niveau qui appuieront le Bureau de l'IA dans sa mission de supervision des modèles d'IA à usage général, ainsi que les autorités nationales pour leurs activités d'application de la loi).

En outre, **les modèles d'IA à usage général sont supervisés par le Bureau de l'IA**, de même que les systèmes d'IA reposant sur ces modèles lorsque le système et le modèle sont mis au point par le même fournisseur. La compétence sera **partagée entre le bureau de l'IA et les autorités nationales de surveillance du marché pour les systèmes d'IA à usage général à haut risque.**

## La gouvernance au niveau national

Le RIA prévoit la désignation d'une ou plusieurs autorités compétentes pour endosser le rôle **d'autorité de surveillance du marché**. Il appartient à chaque État membre d'organiser la structure de gouvernance qui lui apparaît la plus à même de permettre une bonne application du RIA dans un délai d'un an. Si plusieurs autorités compétentes sont désignées au sein d'un même État membre, l'une d'entre elles doit endosser le rôle de point de contact national, afin de faciliter les échanges avec la Commission européenne, les autorités homologues et vis-à-vis du public.

Le RIA ne se prononce pas sur la nature de cette ou ces autorités, à l'exception :

- du Contrôleur européen de la protection des données, qui est expressément désigné comme autorité de surveillance pour les institutions, organismes ou organes de l'Union européenne (à l'exception de la Cour de justice de l'Union européenne agissant dans l'exercice de ses fonctions judiciaires) ;
- des autorités de protection des données qui sont mentionnées vis-à-vis du rôle de surveillance de marchés d'un grand nombre de systèmes d'IA à haut risque (article 74) ;
- enfin, les systèmes d'IA à haut risque déjà soumis à une réglementation sectorielle (listés à l'annexe I) resteront régulés par les autorités qui les contrôlent aujourd'hui (par exemple, l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) pour les dispositifs médicaux).

| | RIA | RGPD |
|---|---|---|

| | | |
|---|---|---|
| **Autorités en charge** | **Pour les systèmes d'IA** : une ou plusieurs autorités compétentes en charge de la surveillance du marché et de la désignation des organismes notifiés (au choix des États membres)<br>**Pour les modèles d'IA à usage général** : Bureau de l'IA au sein de la Commission européenne | Autorité de protection des données de chaque Etat membre |
| **Coopération européenne** | Comité européen de l'IA<br>Groupe de coopération administrative (> ADCO ) | Comité européen à la protection des données (CEPD)<br>> Guichet unique (*one stop shop*) et mécanisme de cohérence |
| **Référent interne aux organismes** | Pas de personne expressément identifiée | Délégué à la protection des données |

## Comment la CNIL va-t-elle prendre en compte le RIA ?

La CNIL est chargée de veiller au respect du RGPD, qui est une réglementation fondée sur des principes généraux applicables à tous les systèmes informatiques. Il s'applique donc aussi aux données personnelles traitées pour ou par les systèmes d'IA, y compris lorsqu'ils sont soumis aux exigences du RIA.

**En pratique, la CNIL prévoit de s'appuyer sur ces exigences pour guider et accompagner les acteurs dans le respect du RIA, mais également du RGPD en proposant une vision intégrée des règles applicables**. La CNIL considère en effet que ce nouveau règlement doit permettre aux acteurs de mieux comprendre leurs obligations quand ils développent ou déploient des IA.

Toutefois, le RIA explicite aussi certaines pratiques interdites dont certaines ont déjà pu être sanctionnées par les autorités de protection des données. Par exemple, la CNIL a ainsi eu l'occasion de sanctionner la pratique relative à la création ou le développement de bases de données de reconnaissance faciale par le moissonnage d'images faciales (issues d'internet ou de dispositifs de vidéosurveillance).

Comme cela est détaillé ci-dessous, la CNIL reste pleinement compétente pour appliquer le RGPD, par exemple aux fournisseurs de modèles ou systèmes d'IA à usage général dont l'établissement principal est en France, en particulier lorsqu'ils ne font pas l'objet d'exigences de fond au titre du RIA (la France pour Mistral AI ou LightOn, l'Irlande pour ChatGPT/OpenAI ou Google/Gemini).

Depuis un an, la CNIL a lancé un plan d'action pour sécuriser les entreprises innovant en matière d'IA dans leur application du RGPD et promouvoir une IA respectueuse des droits des personnes sur leurs données. Ce plan passe notamment par la publication et la mise en consultation de fiches pratiques clarifiant l'application du RGPD en matière d'IA et formulant un certain nombre de conseils. La CNIL dialogue avec les entreprises du secteur et en accompagne certaines dans leurs projets innovants.

---

## Quand le RIA entre-t-il en application ?

Publié au Journal officiel le 12 juillet 2024, le RIA entrera en vigueur vingt jours après, soit le 1er août 2024. L'entrée en application se fera ensuite de façon échelonnée :

- **2 février 2025** (6 mois après l'entrée en vigueur) :
  - Interdictions relatives aux systèmes d'IA présentant des risques inacceptables.

- **2 août 2025** (12 mois après l'entrée en vigueur) :
  - Application des règles pour les modèles d'IA à usage général.
  - Nomination des autorités compétentes au niveau des États membres.

- **2 août 2026** (24 mois après l'entrée en vigueur) :
  - **Toutes les dispositions du règlement sur l'IA deviennent applicables,** en particulier l'application des règles relatives aux systèmes d'IA à haut risque de l'annexe III (systèmes d'IA dans les domaines de la biométrie, des infrastructures critiques, de l'éducation, de l'emploi, de l'accès aux services publics essentiels, de l'application de la loi, de l'immigration et de l'administration de la justice).
  - Mise en œuvre par les autorités des États membres d'au moins un bac à sable réglementaire.

- **2 août 2027** (36 mois après l'entrée en vigueur)
  - Application des règles relatives aux systèmes d'IA à haut risque de l'annexe I (jouets, équipements radio, dispositifs médicaux de diagnostic in vitro, sécurité de l'aviation civile, véhicules agricoles, etc.).

Par ailleurs, l'entrée en application s'appuiera sur des « **normes harmonisées** » au niveau européen qui doivent définir précisément les exigences applicables aux systèmes d'IA concernés. La Commission européenne a ainsi commandé au CEN/CENELEC (Comité européen de normalisation en électronique et en électrotechnique) dix normes actuellement en cours de rédaction. La CNIL participe activement à leur élaboration depuis janvier 2024.

---

# Comment s'articulent le RGPD et le RIA ?

## Le RIA remplace-t-il les exigences du RGPD ?

**Non.**

Le RIA est très clair sur ce point : **il ne remplace pas les exigences du RGPD.** Au contraire, il a pour but de les compléter en posant les conditions requises pour développer et déployer des systèmes d'IA de confiance.

Concrètement, le RGPD s'applique à tous les traitements de données personnelles, c'est-à-dire à la fois :

- **Lors de la phase de développement d'un système d'IA** : un fournisseur de système ou de modèle d'IA au sens du RIA sera le plus souvent considéré comme responsable du traitement au titre du RGPD ;

- **Et lors de la phase d'utilisation (ou déploiement) d'un système d'IA** : un déployeur ou utilisateur de système d'IA au sens du RIA qui traite des données personnelles en sera le plus souvent responsable au titre du RGPD.

**En revanche, le RIA fixe des exigences spécifiques dont le respect peut contribuer largement au respect des exigences du RGPD** (voir ci-dessous).

Pour aller plus loin : consulter les recommandations de la CNIL relatives au développement de systèmes d'IA

---

## RIA / RGPD : comment savoir quel(s) règlement(s) s'applique(nt) à moi ?

Puisque le RIA s'applique exclusivement aux systèmes et modèles d'IA et que le RGPD s'applique à tout traitement de données personnelles, quatre situations sont possibles :

- **le RIA s'applique seul** : tel sera le cas du fournisseur d'un système d'IA à haut risque qui ne nécessite pas de données personnelles, ni pour son développement ni dans son déploiement,

*Exemple : un système d' IA appliqué à un système de gestion d'une centrale électrique*

- **le RGPD s'applique seul** : tel sera le cas du traitement de données personnelles servant à développer ou utiliser un système d'IA n'étant pas soumis au RIA,

  *Exemple : un système d'IA utilisée pour attribuer des centres d'intérêt à des fins publicitaires, ou un système exclusivement développé à des fins de recherche scientifique*

- **les deux s'appliquent** : tel sera le cas lorsqu'un système d'IA à haut risque nécessite des données personnelles pour son développement ou dans son déploiement,

  *Exemple : un système d'IA utilisé pour le tri automatique de CV*

- **ou aucun des deux ne s'applique** : tel sera le cas d'un système d'IA à risque minimal ne mettant pas en œuvre de traitement de données personnelles

  *Exemple : un système d'IA utilisé pour de la simulation dans un jeu vidéo*

| RÈGLES APPLICABLES DU RIA | APPLICATION DU RGPD |
|---|---|
| **Pratiques d'IA interdites** | **Systématiquement**, toutes les pratiques interdites supposant le traitement de données personnelles. |
| **Modèle d'IA à usage général (y compris à risque systémique)** | **Quasi-systématiquement**, les modèles d'IA à usage général se fondant le plus souvent sur l'utilisation de données personnelles pour leur entrainement |
| **Systèmes d'IA à haut risque** | **Dans de très nombreux cas** (avec des exceptions notables comme pour les systèmes d'IA des infrastructures critiques, des véhicules agricoles, des ascenseurs, etc.) |
| **Systèmes d'IA à risque spécifique en matière de transparence** | **Dans certains cas**, en particulier les systèmes destinés à interagir directement avec des personnes physiques |

## Comment le RIA impacte-t-il le RGPD ?

**Le RIA et le RGPD ne réglementent pas les mêmes objets et ne demandent pas la même approche.**

Cependant, la conformité au premier facilite, voire prépare, celle au second : par exemple, la conformité du système d'IA au RGPD est incluse dans la déclaration UE de conformité exigée par le RIA (annexe V).

Par ailleurs, le RIA résout également quelques tensions entre certaines exigences du RGPD et les siennes. Pour cela, il prolonge et prend le relais du RGPD sur certains points bien définis :

- le RIA remplace certaines règles du RGPD **pour le recours par les services répressifs à l'identification biométrique à distance en temps réel dans des espaces accessibles au public** qu'il rend très exceptionnellement possible à certaines conditions (articles 5) ;

- **il permet exceptionnellement de traiter des données sensibles (au sens de l'article 9 du RGPD) pour détecter et corriger les biais potentiels susceptibles de porter préjudice**, si cela est strictement nécessaire et sous réserve de garanties appropriées (article 10) ;

- **il permet la réutilisation de données personnelles, notamment de données sensibles, dans le cadre des « bacs à sable réglementaire » qu'il instaure.** Ces bacs à sable visent à faciliter le **développement de systèmes présentant un intérêt public important** (tels que l'amélioration du système de santé) et sont placés sous la supervision d'une autorité dédiée qui doit préalablement consulter la CNIL et vérifier le respect d'un certain nombre d'exigences (article 59).

## Transparence et documentation : comment articuler ces exigences du RIA avec celles du RGPD ?

Le RIA et le RGPD abordent parfois des notions similaires sous un angle différent.

C'est par exemple le cas du **principe de transparence** et des **obligations de documentation**, qui témoignent de la complémentarité de ces règlements.

### Les mesures de transparence

Le RGPD prévoit des obligations de transparence, qui consistent essentiellement à informer les personnes dont les données sont traitées de la manière dont elles sont traitées (pourquoi, par qui, comment, combien de temps, etc.). Cela concerne aussi bien les traitements de données consistant à développer un système d'IA que l'utilisation d'un système d'IA sur ou par un individu (qui donnerait ainsi lieu à un traitement de données personnelles).

**Le RIA prévoit des mesures de transparence très similaires,** par exemple sur les données ayant servi à entraîner des modèles d'IA à usage général (dont la liste doit être rendue publiquement accessible en vertu de son article 53) ou sur les systèmes ayant vocation à interagir avec des individus (article 50).

### Les exigences de documentation

Le RIA prévoit également la fourniture de documentations et informations techniques par les fournisseurs de systèmes d'IA à haut risque (article 11 et 13) ou de modèles d'IA à usage général (article 53) à leurs déployeurs et utilisateurs. Ces documentations détaillent notamment les procédures de test et d'évaluation de conformité menées.

Le RIA prévoit également que certains déployeurs de systèmes d'IA à haut risque conduisent une analyse d'impact sur les droits fondamentaux (l'article 27 concerne surtout les acteurs publics et les organismes chargés de mission de service public).

L'obligation de mener une analyse d'impact sur la protection des données (AIPD) prévue par le RGPD, complète parfaitement ces exigences du RIA. En effet, l'AIPD sera présumée requise de la part du fournisseur et du déployeur de systèmes d'IA à haut-risque, mais elle pourra surtout utilement se nourrir des documentations exigées par le RIA (article 26).

Le RIA prévoit d'ailleurs que le déployeur puisse s'appuyer sur l'AIPD déjà réalisée par le fournisseur pour mener son analyse d'impact sur les droits fondamentaux (article 27). L'objectif commun étant de permettre de prendre toutes les mesures nécessaires pour limiter les risques pour la santé, la sécurité et les droits fondamentaux des personnes susceptibles d'être affectées par le système d'IA, ces analyses peuvent même être rassemblées sous la forme d'un document unique pour éviter un formalisme trop contraignant.

Il ne s'agit ici que d'exemples de mesures complémentaires entre les deux textes, mais la CNIL participe activement aux travaux du Comité européen de protection des données (CEPD) sur l'articulation entre les règles applicables à la protection des données personnelles et le RIA, actuellement en cours. Ces travaux ont vocation à apporter davantage de clarification sur les points d'articulation, tout en permettant une interprétation harmonisée entre la CNIL et ses homologues européens.

## Pour résumer : quelles différences entre les exigences du RIA et le RGPD ?

Le RIA et le RGPD présentent de fortes similarités et une complémentarité, mais **leur objet et approches diffèrent.**

**Tableau récapitulatif des spécificités du RIA et du RGPD**

| | RIA | RGPD |
|---|---|---|
| **Champ d'application** | Le développement, la mise sur le marché ou le déploiement de systèmes et modèles d'IA | Tout traitement de données personnelles indépendamment des dispositifs techniques utilisés (dont les traitements visant à développer un modèle ou système d'IA (données d'entrainement), et les traitements réalisés au moyen d'un système d'IA) |

| | | |
|---|---|---|
| **Acteurs visés** | Principalement les fournisseurs et déployeurs de systèmes d'IA (dans une moindre mesure les importateurs, distributeurs et mandataires) | Responsables de traitements et sous-traitants<br>(dont les fournisseurs et déployeurs soumis au RIA) |
| **Approche** | Approche par les risques pour la santé, la sécurité ou les droits fondamentaux, notamment à travers la sécurité des produits et la surveillance du marché en ce qui concerne les systèmes et modèles d'IA | Approche fondée sur l'application de grands principes, l'évaluation des risques et la responsabilisation (*accountability*) |
| **Modalité principale de l'évaluation de la conformité (non exhaustif)** | Evaluation de conformité interne ou par un tiers, notamment au moyen d'un système de gestion des risques et au regard de normes harmonisées | Principe de responsabilité (documentation interne) et outils de la conformité (certification, code de conduite) |

| | | |
|---|---|---|
| **Principales sanctions applicables** | Retrait du marché ou rappel de produits<br><br>Amendes administratives pouvant aller jusqu'à 35 millions d'euros ou 7% du chiffre d'affaire annuel mondial | Mise en demeure (pouvant enjoindre de mettre le traitement en conformité, de le limiter temporairement ou définitivement, y compris sous astreinte)<br><br>Amendes administratives pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire annuel mondial |

## Pour approfondir

- Le règlement IA
- Tous les contenus de la CNIL sur l'intelligence artificielle