France Digitale
Jouons collectif

WAVESTONE

Février 2024

Mise en conformité AI Act

les clés pour comprendre et appliquer la loi sur l'IA

Sommaire

AI Act is coming !

Vous développez une solution basée sur l'Intelligence Artificielle ou vous intégrez de l'IA dans vos processus, produits ou services ? **Préparez-vous: vous allez devoir vous mettre en conformité avec une nouvelle réglementation, l'AI Act.**

On vous résume les conséquences pratiques de cette réglementation ⤵

L'AI Act vise à garantir que les systèmes et modèles d'intelligence artificielle commercialisés au sein de l'Union européenne soient utilisés de manière éthique, sûre et respectueuse des droits fondamentaux de l'UE.

Concrètement, qu'est-ce que ça va changer ? L'AI Act crée une réglementation produit, allant du marquage CE à l'interdiction de mise sur le marché, applicable aux systèmes et modèles d'intelligence artificielle faisant l'objet d'une commercialisation et d'une mise sur le marché. Les activités de recherche, sans objectif commercial, ne sont pas concernées.

Qui doit opérer la mise en conformité ? Tous les fournisseurs*, distributeurs* ou déployeurs* de systèmes et de modèles d'IA, personnes morales (entreprises, fondations, associations, laboratoires de recherche, etc.), dont le siège social se situe dans l'Union européenne, ou lorsque le siège social est situé en dehors de l'Union européenne, qui commercialisent leur système ou modèle d'IA dans l'Union européenne.

Tous les systèmes et modèles d'IA sont-ils concernés par la réglementation "produit" ?
Le niveau de réglementation et les obligations associées dépendent du niveau de risque que présente le système ou le modèle d'IA. Il y a 4 niveaux de risques, et 4 niveaux de mise en conformité :

- risque inacceptable : les systèmes et modèles d'IA à risque inacceptable sont interdits et ne peuvent être commercialisés ni dans l'Union européenne ni utilisés à l'export ;
- haut risque : les systèmes et modèles d'IA à haut risque doivent faire l'objet d'un marquage CE pour être commercialisés ;
- risque faible : les systèmes et modèles d'IA à risque faible doivent faire l'objet d'obligations d'information et de transparence vis-à-vis des utilisateurs ;
- risque minime : les systèmes et modèles d'IA à risque minime peuvent se contenter de respecter des codes de conduite.

Des obligations particulières s'appliquent aux IA génératives et au développement de modèles d'IA à usage général* (e.g. *Large Language Models* ou "*LLMs*"), avec une réglementation différente selon que le modèle est open source ou ne l'est pas, et selon d'autres critères subsidiaires (puissance de calcul, nombre d'utilisateurs, etc.).

Sous quel délai faut-il se mettre en conformité ? Des délais différents, entre 6 et 36 mois, s'appliquent selon le niveau de risque des systèmes et modèles d'IA. **Quel que soit le délai, il est essentiel d'être préparé et d'anticiper la mise en conformité qui va venir perturber les roadmaps tech, produit et légales des entreprises.**

Tout comprendre des obligations de l'AI Act

Les obligations de mise en conformité des systèmes d'IA dépendent du niveau de risque.

	Risque inacceptable	Haut risque	Risque faible	Risque minime
?	**Ces systèmes contreviennent aux valeurs de l'UE et portent atteinte aux droits fondamentaux.** L'article 5.I dresse une première liste (scoring social, identification biométrique généralisée, deepfakes, manipulation de contenu, porter atteinte à certaines catégories de la population, etc.) mise à jour régulièrement	**Ces systèmes sont déployés dans des produits à haut risque définis à l'annexe II ou dans des secteurs à haut risque définis à l'Annexe III de l'AI Act**	**Il s'agit des systèmes qui interagissent avec des personnes physiques (art. 52, I) et qui ne sont ni à risque inacceptable, ni à haut risque** comme par exemple des deep fakes à vocation artistique ou des chatbots	**Il s'agit des autres systèmes d'IA (non définis comme inacceptables, à haut risque ou à risque faible)** comme par exemple les IA dans les jeux vidéos, les filtres anti-spam, etc.
	Interdiction de commercialisation y compris en dehors de l'UE	**Cas d'usage à haut risque** Déclaration de conformité + Enregistrement dans la base de données de l'UE + Marquage CE	**Cas d'usage n'est pas à haut risque*** Déclaration de conformité + Enregistrement dans la base de données de l'UE	**Obligation d'information** aux utilisateurs que le contenu a été généré par l'IA	**Application volontaire de codes de conduite**
	6 mois après la publication de l'AI Act (ie. novembre 2024, TBC*)	**24 mois ou 36 mois** après la publication de l'AI Act (si le système d'IA à haut risque est déjà régulé par d'autres textes européens)		**24 mois** après la publication de l'AI Act (ie. octobre 2026, TBC)	**24 mois** après la publication de l'AI Act (ie. octobre 2026, TBC)
	35 millions d'euros ou 7% du CA annuel mondial (montant le + ou - élevé selon la catégorie d'entreprise)	**15 millions d'euros ou 3% du CA annuel mondial** (montant le + ou - élevé selon la catégorie d'entreprise)		**7,5 millions d'euros ou 1% du CA annuel mondial** (montant le + ou - élevé selon la catégorie d'entreprise)	

*TBC : *to be confirmed*

*Les entreprises ont la possibilité de démontrer que l'usage de l'IA, bien que déployé dans un secteur à haut risque, ne présente pas, en tant que tel, un haut risque.

La précision utile

Les obligations de mise en conformité prévues dans l'AI Act s'appliquent à chaque système ou modèle d'IA et non à l'entreprise dans son ensemble. Il est donc conseillé de réaliser une cartographie de tous les systèmes d'IA utilisés au sein de votre entité.

Quelques exemples pour bien comprendre !

Nous vous proposons trois cas concrets pour comprendre comment se fait la classification du niveau de risque, et la mise en conformité le cas échéant.

#1 Les filtres anti-spam : un système d'IA à risque minime

Une entreprise crée un programme pour empêcher les e-mails non sollicités, indésirables et infectés par des virus d'arriver dans les boîtes mails de ses employés. Le programme utilise des algorithmes pour déterminer la probabilité qu'un e-mail soit un spam ou non.
Ce type de système d'IA ne requiert pas un degré de conformité élevé car cet usage de l'IA n'est ni à risque inacceptable, ni à haut risque ou ni à risque faible comme défini dans l'AI Act. Cependant, il est recommandé de mettre en place un code de conduite pour les systèmes d'IA. Ce code de conduite doit être élaboré sur la base d'objectifs clairs et d'indicateurs clés de performance pour mesurer la réalisation de ses objectifs. Les exigences pourraient inclure des éléments tels que l'équité, la transparence, la confidentialité et la durabilité. Ce code de conduite pourra d'ailleurs être appliqué à plusieurs systèmes d'IA au sein de l'entreprise s'ils visent des objectifs similaires.

#2 Les deep fakes artistiques : un système d'IA à risque faible

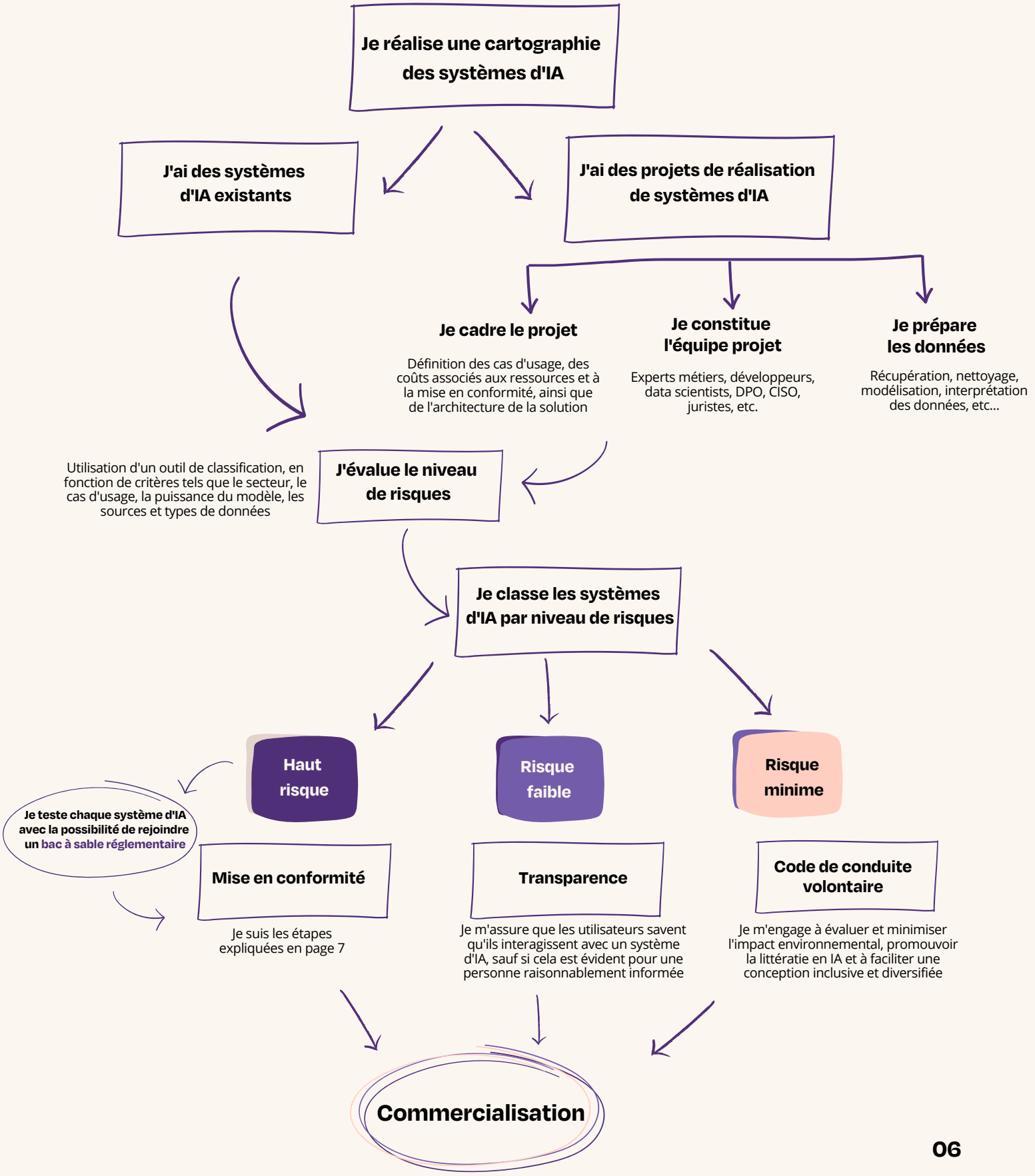
En tant que société de production, vous souhaitez élaborer une formation vidéo sur la physique quantique en utilisant l'image d'Einstein, générée par une IA, qui anime la formation. Il est impératif d'expliciter que le contenu a été créé à l'aide de cette technologie. Vous devrez donc ajouter une information ou un avertissement dans la formation pour expliquer que l'image a été générée par une IA (le choix de la mention est libre afin de ne pas entraver l'affichage ou le contenu en lui-même). Cela permettra aux apprenants de comprendre que l'image d'Einstein est générée par une machine.

#3 La notation de crédit : un système d'IA à haut risque

Vous êtes une institution financière qui souhaite créer une IA pour évaluer la solvabilité des demandeurs de crédit. Vous avez accès à des données sensibles de vos clients (historique de crédit, revenus, emplois), et sur cette base, vos algorithmes définissent si un prêt doit être accordé et sous quelles conditions. Votre cas d'usage est considéré comme à haut risque car il peut être discriminant. Pour pouvoir commercialiser votre IA, vous devez vous engager dans la démarche de mise en conformité.

Que faire pour mettre en conformité les systèmes d'IA existants, et/ou s'assurer que les futurs projets le soient ?

L'AI Act s'applique aussi bien aux systèmes déjà en place (*legacy*) qu'aux nouvelles solutions. Voici une démarche type pour vous y retrouver !



🔍 Les 10 étapes de mise en conformité des systèmes d'IA à haut risque

☐ **Système de gestion des risques**	J'adopte des mesures de gestion des risques appropriées et ciblées pour répondre aux risques identifiés.
☐ **Données et gouvernance des données**	J'utilise des données d'entrainement de qualité, je respecte les pratiques appropriées de gouvernance des données, je m'assure que les jeux de données sont pertinents et non-biaisés.
☐ **Documentation technique**	J'inclus les éléments minimums spécifiés dans l'Annexe IV.
☐ **Traçabilité**	Je m'assure que des archives sont disponibles tout au long de la durée de vie du système d'IA, avec un suivi conçu pour la traçabilité et leur transparence.
☐ **Supervision humaine**	J'incorpore des outils d'interface homme-machine pour prévenir ou minimiser les risques en amont, permettant ainsi aux utilisateurs de comprendre, d'interpréter et d'utiliser en confiance ces outils.
☐ **Exactitude, robustesse et sécurité**	J'assure une exactitude, une robustesse et des mesures de cybersécurité contantes, tout au long du cycle de vie du SIA, avec des métriques de précision déclarées, une résilience contre les erreurs et des mesures appropriées pour traiter les biais potentiels.
☐ **Système de gestion de la qualité**	J'établis et je documente un système de gestion de la qualité couvrant la conformité réglementaire, la conception, le développement, les tests, la gestion des risques, la surveillance post-commercialisation, la déclaration d'incidents, la communication, la gestion des données, la conversation des enregistrements, la gestion des ressources et la responsabilité.
☐ **Déclaration de conformité de l'UE**	Je rédige la déclaration de conformité, lisible et signée, pour chaque système d'IA à haut risque, affirmant la conformité avec les exigences du Chapitre 2, je la maintiens à jour pendant 10 ans, je soumets des copies aux autorités nationales, et je la mets à jour quand nécessaire.
☐ **Marquage CE**	Je m'assure que le marquage CE est apposé de manière visible, lisible et indélébile, ou numériquement accessible pour les systèmes numériques, indiquant ainsi la conformité aux principes généraux et aux lois de l'Union applicables.
☐ **Enregistrement**	Avant de mettre sur le marché ou de mettre en service la solution d'IA, j'inscris l'entreprise ainsi que le système dans la base de données de l'UE mentionnée à l'Article 60.

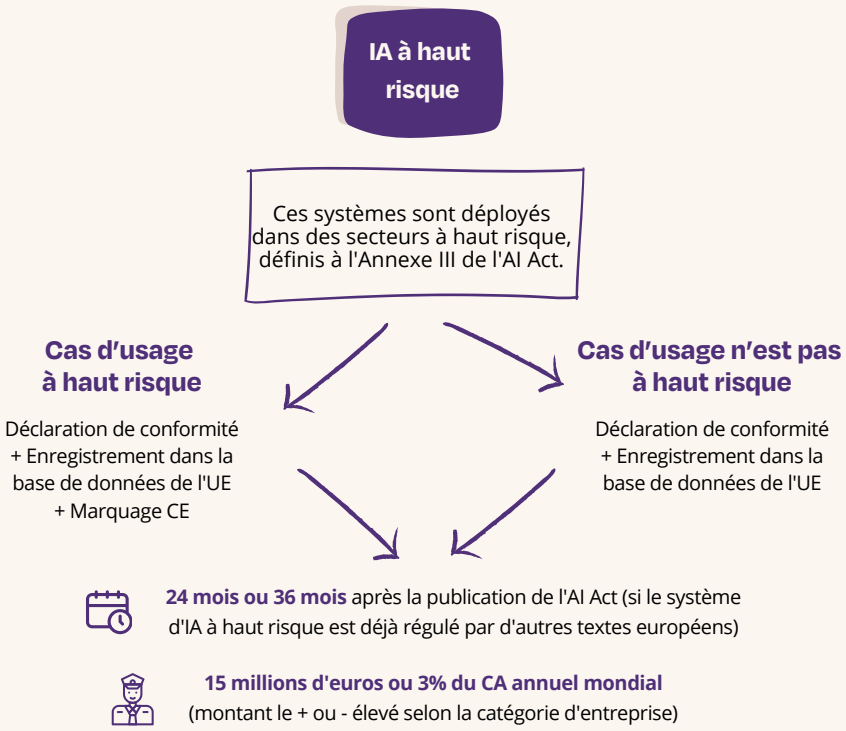
Cas pratique : application de la démarche de mise en conformité aux ressources humaines, un système d'IA à haut risque

TechInnovate est une entreprise fictive qui ambitionne de développer une solution d'IA visant à faciliter et optimiser le processus de présélection des candidats. On a appliqué ici notre démarche de mise en conformité :

- La société identifie des **cas d'utilisation pour son nouveau système d'IA**, incluant l'analyse automatique de CV, un entretien virtuel automatisé, et l'analyse des retours post-entretien.
- Le **coût estimé du projet s'élève à environ 60 000 €**, en prenant en considération la nécessité de mobiliser un expert métier en RH, un expert en cybersécurité et en protection des données, trois data scientists, un chef de projet pour une durée d'un mois, et un juriste pour deux jours pour accompagner la mise en conformité. Il faudra prévoir un budget spécifique pour le processus de test si celui-ci s'effectue dans le cadre du bac à sable réglementaire.
- TechInnovate **collecte des données** provenant de l'expérience professionnelle, des compétences techniques, des références et des entretiens, et modélise ces informations.
- Pour **évaluer les risques**, la société utilise un outil prenant en compte le secteur (ressources humaines), la sensibilité des données (compétences et performances individuelles), et la complexité du modèle IA.
- Le moteur de recommandations de TechInnovate est **classé comme présentant un risque élevé**, en raison de l'utilisation de données personnelles et sensibles pour améliorer l'efficacité du recrutement, avec le risque potentiel de biais algorithmes pouvant influencer les décisions.
- Pour pallier ces risques, TechInnovate décide de **tester son système d'IA dans un bac à sable réglementaire** afin de s'assurer notamment de l'absence de biais. Il doit respecter l'ensemble des conditions prévues à cet effet par son autorité nationale, mais cela lui permet de tester son système dans un environnement régulé et contrôlé sans enfreindre la réglementation applicable.
- TechInnovate entreprend ensuite **la mise en conformité de son système d'IA conformément à l'AI Act**. Cette démarche inclut la mise en place de politiques de confidentialité et de sécurité des données pour gérer les risques, le respect des normes de gouvernance des données, l'intégration des mesures spécifiées dans l'Annexe IV, la conservation des archives de formation du modèle, l'assurance de la précision du modèle, la robustesse du système, et la mise en œuvre des mesures de cybersécurité, tout en instaurant un système de gestion de la qualité.
- TechInnovate **documente en détail** la manière dont chaque exigence de l'AI Act est respectée dans sa **déclaration de conformité**. Après avoir complété toutes les étapes de mise en conformité, TechInnovate soumet son dossier aux autorités compétentes, obtient le marquage CE et procède ensuite à son enregistrement dans la base de données de l'UE.
- Désormais en mesure de **commercialiser son moteur de recommandations** amélioré, TechInnovate met en avant son **marquage CE,** renforçant ainsi la confiance de ses clients quant à la conformité de leur solution IA.

Focus sur les IA à haut risque

On vous rappelle comment la réglementation des IA à haut risque fonctionne :



Voici les étapes à suivre

1 - Déterminer si le système ou modèle d'IA est déployé dans un secteur à haut risque

Pour déterminer si un système d'IA est à haut risque selon l'IA Act, il faut vérifier s'il est inclus dans la liste prévue à l'Annexe II et l'Annexe III de cette réglementation.

L'Annexe III de l'AI Act définit 8 grands domaines d'activités identifiés comme à "haut risque" :

1. Identification biométrique et catégorisation des personnes physiques
2. Infrastructures critiques
3. Education et formation professionnelle
4. Emploi, gestion des travailleurs et accès au travail indépendant
5. Accès et jouissance des services privés essentiels et des services et avantages publics
6. Forces de l'ordre
7. Gestion de la migration, de l'asile et du contrôle des frontières
8. Administration de la justice et processus démocratiques

2 - Engager le processus de mise en conformité (i.e. le marquage CE)

Tous les systèmes d'IA à haut risque seront évalués avant leur mise sur le marché et tout au long de leur cycle de vie. Les entreprises concernées devront ainsi disposer du marquage CE pour commercialiser leur solution, sauf si elles parviennent à démontrer que l'usage fait du système ou modèle d'IA n'est pas, en tant que tel, à haut risque.

Il faut alors suivre la checklist de la mise en conformité détaillée en page 7.

3 - Sauf s'il est possible de démontrer que le système d'IA n'est pas à haut risque

Pour les systèmes d'IA visés à l'Annexe III, les systèmes d'IA ne sont pas considérés comme étant à haut risque si les conditions cumulatives suivantes sont réunies :

- le système d'IA ne présente pas un risque significatif de préjudice à la santé, à la sécurité ou aux droits fondamentaux des personnes physiques ;
- le système d'IA n'influence pas de manière substantielle le résultat de la prise de décision.

Ce sera notamment le cas si le système d'IA est destiné à accomplir une tâche procédurale limitée, ou à améliorer le résultat d'une activité humaine préalablement achevée, ou à détecter des modèles de prise de décision ou des écarts par rapport aux modèles de prise de décision antérieurs et n'est pas destiné à remplacer ou influencer l'évaluation humaine préalablement réalisée, sans examen humain approprié ; ou à accomplir une tâche préparatoire.

A noter que le système d'IA sera toujours considéré comme à haut risque si le système effectue un profilage des personnes physiques.

Si le système d'IA n'est pas considéré comme étant à haut risque par l'entreprise, cette dernière doit réaliser les tâches suivantes:

- Documenter son analyse de risques
- Enregistrer son système dans la base de donnée de l'UE
- Rester à la disposition de l'autorité nationale en cas de contrôle

Cette procédure fait courir un risque d'insécurité juridique important.

Le regard de Gide : le cas particulier des systèmes d'IA intégrés comme composants de sécurité d'un produit déjà couvert par une autre réglementation européenne (Annexe II)

GIDE
GIDE LOYRETTE NOUEL

Parmi les IA considérées comme étant à haut risque, l'AI Act liste différents systèmes d'IA intégrés comme une composante de sécurité dans des produits qui font déjà l'objet d'une réglementation sectorielle. Il s'agit de produits déjà soumis à des exigences spécifiques et à des tests de conformité avant de pouvoir être mis sur le marché. Les cas d'usage visés sont très variés : systèmes d'IA utilisés comme composantes de sécurité dans les jouets pour enfants, dans les dispositifs médicaux, dans les ascenseurs, etc. La nature même du produit dans lequel le système d'IA est intégré implique, selon les institutions européennes, que ce système présente un risque élevé.

Ces systèmes doivent respecter l'ensemble des obligations prévues dans l'AI Act pour les systèmes d'IA à haut risque ainsi que les exigences issues de la réglementation sectorielle applicable au produit dans lequel le système d'IA s'insère.

Pour assurer la cohérence entre les exigences des différentes réglementations et tenter de limiter la charge liée à l'application cumulative de l'AI Act et de la réglementation sectorielle applicable au produit visé :

- l'AI Act prévoit que le fournisseur peut intégrer le dispositif nécessaire pour respecter l'AI Act aux procédures et documents qui sont déjà prévus par la réglementation sectorielle ;
- le délai de mise en conformité à l'AI Act est allongé ; les entreprises devront être conformes à l'AI Act dans les 36 mois suivant la publication du texte.

Le cas particulier de l'IA générative et des modèles d'IA à usage général

Pour les modèles d'IA à usage général (et notamment les *Large Language Models*, ou *LLM*), les obligations de mise en conformité dépendent de la nature open source ou non du modèle, et de critères subsidiaires (notamment, la puissance de calcul > ou < à 10^25 FLOPS).

Modèle de base

ie. puissance de calcul <10^25 FLOPS

Open source

Conformité avec la Directive Copyright

+ Résumé détaillé des jeux de données d'entrainement

Pas Open source

Conformité avec la Directive Copyright

+ Résumé détaillé des jeux de données d'entrainement

+ Documentation technique

Modèle à risque systémique

ie. puissance de calcul >10^25 FLOPS

Open source

Conformité avec la Directive Copyright

+ Résumé détaillé des jeux de données d'entrainement

+ Documentation technique

Pas Open source

Conformité avec la Directive Copyright

+ Résumé détaillé des jeux de données d'entrainement

+ Série d'autres obligations : documentation technique, évaluation, atténuation des risques, déclaration d'incidents sérieux, tests d'adversité (*red teaming*), cybersécurité, consommation d'énergie

Les précisions utiles

La qualification de modèle de base ou de modèle systémique. A ce jour, seul le critère de la puissance de calcul (> ou < 10^25 FLOPS) a été retenu. L'AI Office pourra compléter cette définition dans un second temps pour tenir compte de critères additionnels, comme le nombre de *business users*.

La qualification du modèle comme étant open source ou ne l'étant pas.
L'article 52c définit les modèles open source comme des modèles rendus accessibles au public grâce à une licence gratuite et open source qui permette l'accès, l'usage, la modification et la distribution du modèle, et dont les paramètres (notamment les poids, l'information sur l'architecture du modèle et l'information sur l'usage du modèle) sont disponibles publiquement.

Des précisions à venir sur la réglementation des IA à usage général (tels que les *LLM*) : l'AI Office travaillera à élaborer des codes de pratique et une méthodologie pour définir si un modèle d'IA à usage général doit être considéré comme étant à risque systémique et pour aider leurs développeurs, distributeurs et déployeurs à se conformer aux exigences et obligations du texte.

Droit d'auteur, sets de données et IA générative : tous les modèles d'IA à usage général, qu'ils soient open source ou pas, doivent publier un résumé sur les données d'entraînement et sont soumis aux réglementations relatives au droit d'auteur.

Le regard de Gide : IA, protection des données et droit d'auteur

GIDE
GIDE LOYRETTE NOUEL

Le recours aux sets de données à l'épreuve de réglementations qui se cumulent
L'entraînement des modèles et systèmes d'IA peut reposer sur des données et contenus protégés ou dont le traitement peut faire l'objet d'une réglementation spécifique. A ce titre, l'AI Act se cumule avec d'autres réglementations en vigueur, notamment le RGPD pour les données personnelles et les législations relatives au droit d'auteur et aux droits voisins. L'utilisation de données par les systèmes et les modèles d'IA devront donc respecter l'ensemble de ces textes. En matière de données personnelles, deux points nécessitent une attention particulière pour déterminer les obligations applicables au responsable du traitement : la finalité du traitement (l'objectif poursuivi par l'utilisation des données), et les conditions de collecte et d'obtention des données.

Le respect du droit d'auteur par les fournisseurs de modèles d'IA à usage général (notamment les LLMs). Pour les modèles d'IA à usage général (notamment les LLMs), le nouveau cadre européen entend définir un équilibre entre le besoin de contenu pour entraîner les modèles et la protection des contenus par le droit d'auteur. Ainsi, l'AI Act impose aux fournisseurs de modèles d'IA à usage général l'obligation de prévoir des procédures pour assurer le respect du droit d'auteur quant aux contenus que le modèle utilise. Le droit d'opposition des ayants-droit contre la fouille et l'analyse automatisée de données (système dit de « opt-out ») laisse entrevoir de futures négociations pour un partage équilibré de la valeur générée au titre de l'utilisation des contenus par les systèmes d'IA. Les fournisseurs de modèles d'IA à usage général seront notamment soumis à des obligations de transparence concernant les ensembles de contenus utilisés pour entraîner leurs modèles. Les principes posés par la réglementation appellent d'une part à la désignation de standards techniques harmonisés pour l'identification des contenus, et d'autre part à la définition des modèles d'affaires pertinents pour un juste partage de la valeur.

Anticiper la mise en conformité avant la mise sur le marché : bacs à sable et tests en vie réelle

Anticiper la mise sur le marché avec les bacs à sable réglementaires

L'AI Act prévoit une obligation pour chaque autorité nationale de mettre en place, au niveau d'un ou plusieurs Etats membres, un bac à sable réglementaire pour l'AI Act.

Ces bacs à sables doivent être opérationnels au moment de l'entrée en application de l'AI Act, en 2026. Ils ont vocation à permettre aux fournisseurs, pour une durée déterminée, de développer, d'entraîner, de tester et de valider des systèmes d'IA avant leur mise sur le marché, en lien avec les autorités nationales compétentes, en ayant la certitude d'être conformes à l'AI Act.

Pensés pour soutenir l'innovation et la compétitivité des acteurs européens, ces bacs à sable ont vocation à faciliter l'accès au marché pour les systèmes d'IA proposés par des startups et des PMEs européennes.

Sur la base de standards techniques qui seront publiés par la Commission européenne, les autorités nationales devront préciser les critères d'éligibilité et les conditions de fonctionnement de ces bacs à sable réglementaires.

Au-delà des bacs à sable réglementaires : les tests dans la vie réelle

Indépendamment des bacs à sable réglementaires, l'IA Act prévoit également que les fournisseurs de systèmes d'IA devraient pouvoir tester leurs systèmes d'IA dans la vie réelle sans enfreindre l'AI Act, à condition de respecter des conditions précises.

Parmi ces conditions, figurent notamment l'obligation d'avoir obtenu l'accord de l'autorité nationale compétente, sur la base d'un plan de test qui lui a été préalablement fourni par le fournisseur. Ce plan devra notamment prévoir une durée définie pour les tests et exiger que les personnes sur lesquelles les tests sont effectués soient dûment informées et donnent leur accord.

Là encore, des standards techniques à venir de la Commission européenne doivent harmoniser les conditions dans lesquelles ces facilités de test dans la vie réelle seront mises en œuvre dans chaque Etat membre.

Les dates à retenir pour être prêt le jour J

L'AI Act va entrer en vigueur progressivement selon le niveau de risque des systèmes ou modèles d'IA, comme on l'a résumé ici :

Important : Les délais fixés par le législateur commencent à courir à compter de la date d'entrée en vigueur de l'AI Act (soit 20 jours après la publication du texte sur le Journal officiel de l'Union européenne) et devront être précisés dès que la date officielle de publication sera connue.

Si ce calendrier progressif a été pensé par le régulateur pour permettre de laisser le temps aux entreprises de se mettre en conformité, il est important d'anticiper les différentes étapes à venir.

Les risques et sanctions en cas de manquement aux règles de mise en conformité

- Pour une entreprise qui commercialise un système ou modèle d'IA à risque inacceptable, la sanction pourra aller jusqu'au montant le plus élevé entre 7% du CA mondial ou 35 millions d'euros ;
- Pour les entreprises qui ne respectent pas les obligations de mise en conformité relatives aux IA à haut risque, la sanction pourra aller jusqu'au montant le plus élevé entre 3% du CA mondial ou 15 millions d'euros ;
- En cas de transmission d'informations inexactes, incomplètes ou trompeuses, la sanction pourra aller jusqu'au montant le plus élevé entre 1% du CA mondial ou 7,5 millions d'euros.

Important : Pour les PME (notamment les startups), les sanctions seront appliquées selon une logique inverse, à savoir seront égales au montant le moins élevé entre le % de CA mondial et le plafond de 35, 15 ou 7,5M d'euros.

Vos points de contact

Vous devez compter sur 2 interlocuteurs prioritaires :

- **Deux autorités nationales**, non encore désignées pour la France, en charge de (i) la bonne application de l'AI Act et son harmonisation avec les autres autorités nationales et européennes (ii) la supervision du bac à sable national, et (iii) le contrôle et les sanctions. **Ces autorités seront vos points de contact privilégiés si vous avez des questions sur l'application de l'AI Act ou si vous voulez rejoindre le bac à sable national.**

- **L'AI Office**, intégré à la Commission européenne, composé d'experts indépendants et qui devra être créé prochainement, en charge de (i) élaborer des méthodologies pour évaluer les modèles d'IA, et (ii) surveiller les risques de sécurité associés aux modèles d'IA à usage général, en coordination avec les autorités nationales. **L'AI Office sera votre interlocuteur privilégié pour envoyer la déclaration de conformité si vous avez un système ou modèle d'IA à haut risque.**

Les autres organes sur lesquels vous pouvez compter :

- **L'AI Board**, composé de représentants d'Etats membres, assurera la coordination de l'application du texte au niveau européen, en coordination avec les futures autorités nationales ;

- **L'Advisory forum européen** est une instance représentant la société civile (notamment les entreprises) qui sera consultée régulièrement par l'AI Office pour faire des retours sur l'application de l'AI Act et anticiper l'évolution de la régulation dans le temps ;

- **L'AI Pact** est une initiative de la Commission européenne qui encourage les entreprises à prendre des engagements volontaires avant l'entrée en vigueur de l'AI Act. Concrètement, les entreprises peuvent signer une déclaration d'engagement visant à œuvrer au respect de la future loi sur l'IA, accompagnée de détails sur les actions concrètes menées à ce fin. Elles peuvent également partager leurs bonnes pratiques. La participation à l'AI Pact devrait offrir un accès facilité aux supercalculateurs européens. La participation à l'AI Pact est ouverte à tous, sous réserve d'acceptation de la candidature. Une première liste des participants sera publiée au premier semestre 2024. Vous pouvez participer ici.

Lexique

Conformité : processus qui consiste pour les entreprises à déployer des procédures préventives leur permettant d'éviter de s'exposer à des risques liés au non-respect d'une ou plusieurs réglementations. La mise en place d'une politique de conformité permet à l'entreprise une meilleure gestion des risques et lui évite de s'exposer à des risques financiers et réputationnels.

Deep fake : un contenu d'image, d'audio ou de vidéo généré ou manipulé par intelligence artificielle, qui ressemble à des personnes, objets, lieux, entités ou événements existants et qui donnerait faussement l'apparence d'être authentique ou véridique à une personne.

Déployeur : toute personne utilisant un système d'IA sous son autorité, sauf si le système d'IA est utilisé dans le cadre d'une activité personnelle non professionnelle.

Distributeur : toute personne physique ou morale de la chaîne d'approvisionnement, à l'exception du fournisseur ou de l'importateur, qui met un système d'intelligence artificielle à disposition sur le marché de l'Union

Fournisseur : toute personne qui développe un système d'IA ou un modèle d'IA à usage général ou qui fait développer un système d'IA ou un modèle d'IA à usage général et les met sur le marché ou met le système en service sous son propre nom ou sa propre marque, que ce soit à titre onéreux ou gratuit

Modèle d'IA à usage général ("*General Purpose AI systems*" ou "GPAI") : un système d'IA qui fait preuve d'une grande généralité et qui est capable d'exécuter un large éventail de tâches distinctes et qui peut être intégré dans une large variété de systèmes ou d'applications.

Norme : lancée à l'initiative des acteurs du marché, une norme est un cadre de référence qui vise à fournir des lignes directrices, des prescriptions techniques ou qualitatives pour des produits, services ou pratiques au service de l'intérêt général. Elle est le fruit d'une coproduction consensuelle entre les professionnels et les utilisateurs qui se sont engagés dans son élaboration" (Afnor). Il existe tout un ensemble de normes que l'on regroupe en 2 grands ensembles : les normes verticales (dites sectorielles, comme l'automobile, aéronautique, secteur bancaire, etc.) et les normes horizontales (plutôt technologiques, comme la cyber, l'IA, etc.)

Sandbox (bac à sable réglementaire) : un cadre concret et contrôlé mis en place par une autorité compétente qui offre aux fournisseurs ou futurs fournisseurs de systèmes d'IA la possibilité de développer, former, valider et tester, le cas échéant dans des conditions réelles, un système d'IA innovant, conformément à un plan de bac à sable pour une durée limitée sous supervision réglementaire.

Système d'Intelligence Artificielle : un système basé sur une machine conçue pour fonctionner avec différents niveaux d'autonomie et qui peut présenter de l'adaptabilité après son déploiement. Ce système, dans le cadre d'objectifs explicites ou implicites, déduit à partir des entrées qu'il reçoit comment générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions pouvant influencer des environnements physiques ou virtuels.

Un grand MERCI à nos contributeurs

Marianne TORDEUX-BITKER
Directrice des affaires publiques

France Digitale

marianne@francedigitale.org

Chadi HANTOUCHE
Partner

Wavestone

chadi.hantouche@wavestone.com

Julien GUINOT-DELÉRY
Associé - Propriété intellectuelle, Médias & Technologies

Gide

guinot@gide.com

Agata HIDALGO
Responsable des affaires publiques européennes

France Digitale

agata@francedigitale.org

Florence ESPITALIER
Senior Consultante

Wavestone

florence.espitalier@wavestone.com

Matthieu LUCCHESI
Counsel
Innovation & FinTech

Gide

matthieu.lucchesi@gide.com

Thomas BARREAU
IA & standardisation

France Digitale

ap@francedigitale.org

Raya CHAKIR
Consultante

Wavestone

raya.chakir@wavestone.com

Disclaimer - Important

Ce guide a été établi sur la base du compromis à l'AI Act trouvé le 29 janvier 2024 et ayant fait l'objet d'un vote en Coreper le 2 février 2024. Le compromis devrait être voté en l'état en assemblée plénière du Parlement Européen d'ici à avril 2024. L'AI Act n'entrera en vigueur que 20 jours après sa publication officielle au Journal Officiel de l'Union européenne. Les informations fournies dans ce guide peuvent donc varier à la marge par rapport à la version du texte qui sera finalement adoptée.
Ce guide n'a pas valeur de conseil juridique et nous vous invitons à vous entourer d'experts pour la mise en conformité opérationnelle.

Un document réalisé en collaboration avec

France Digitale — Jouons collectif

WAVESTONE

GIDE — GIDE LOYRETTE NOUEL

À propos de France Digitale

Fondée en 2012, France Digitale est la plus grande association de startups en Europe, avec plus de 2000 startups et investisseurs français.
L'association se donne pour mission de faire émerger des champions européens du numérique en fédérant et en portant la voix de celles et ceux qui innovent pour changer la face du monde. France Digitale est co-présidée par Frédéric Mazzella, fondateur de BlablaCar, et Benoist Grossmann, CEO d'Eurazeo Investment Manager.

À propos de Wavestone

Wavestone, l'un des tout premiers cabinets de conseil en France, et Q_PERIOR, l'un des leaders du conseil sur le marché germanophone (Allemagne – Suisse – Autriche) se sont rapprochés en 2023 pour devenir le partenaire privilégié des transformations majeures.
En s'appuyant sur plus de 5 500 collaborateurs à travers l'Europe, l'Amérique du Nord et l'Asie, le cabinet dispose d'expertises sectorielles de premier plan complétées par un portefeuille de savoir-faire cross-sectoriels permettant d'adresser à 360° les grands programmes de transformation.

À propos de Gide

Gide est un cabinet d'avocats d'affaires français à dimension internationale. Fondé à Paris en 1920, le cabinet compte aujourd'hui 11 bureaux dans le monde. Il rassemble 500 avocats de 35 nationalités différentes, reconnus parmi les meilleurs spécialistes de chacune des branches du droit national et international des affaires.