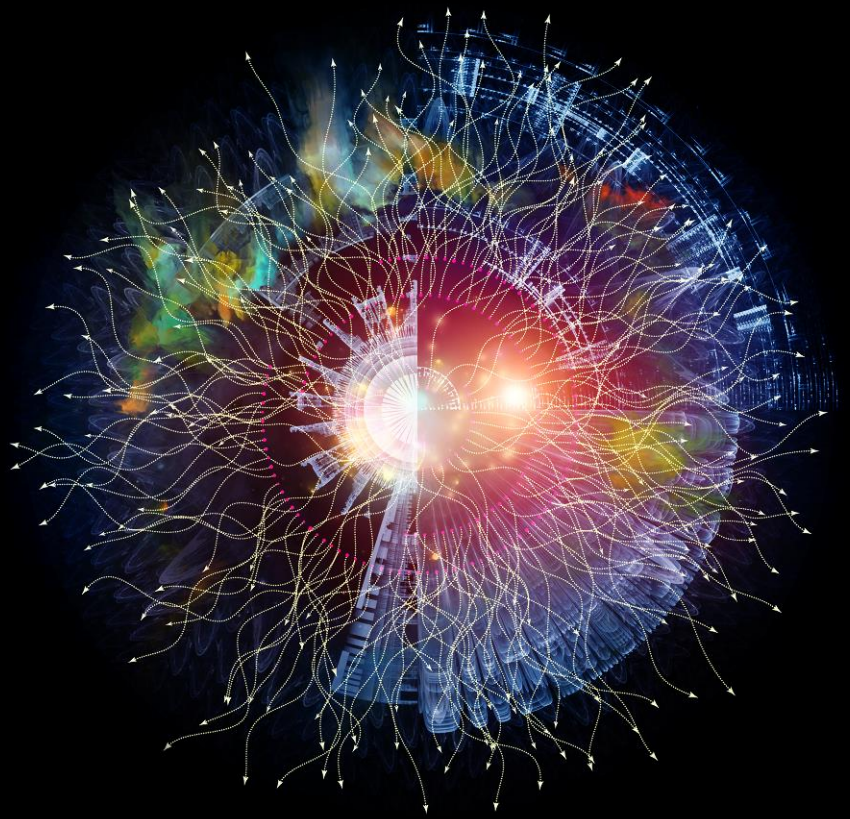
Deloitte.



Artificial Intelligence Act

Mai 2021

Risk Advisory – Deloitte France

L'Artificial Intelligence Act en un mot

La proposition de règlementation prévoit des règles harmonisées sur l'intelligence artificielle.

Comment l'**AI Act** vous impacte ?

Sur quoi se concentre-t-elle ?

- Centré sur l'humain
- Approche fondée sur le risque
- Classification des systèmes d'IA

À qui s'applique-t-elle ?

- Fournisseurs, utilisateurs, importateurs et distributeurs de systèmes d'IA au sein de l'UE

Quand s'appliquera-t-elle?

- Selon une interview, la mise en œuvre et le processus de ratification pourrait prendre entre 2 à 5 ans

Pourquoi devez-vous vous en soucier ?

- Votre organisation peut déjà avoir des systèmes d'IA en place
- La non-conformité peut entraîner des amendes allant jusqu'à 30.000.000€ ou 6% du chiffre d'affaires

Que pouvons-nous faire?

- Informer nos clients sur le sujet
- Deloitte dispose d'un cadre pour mettre en oeuvre une IA de confiance

Le 21 avril 2021, la Commission européenne a proposé le premier cadre juridique sur l'IA jamais mis en œuvre, qui traite des risques de l'IA et qui positionne l'Union Européenne comme un acteur de premier plan à l'échelle mondiale. Ce document a vocation à donner une vision synthétique des enjeux de cette règlementation.

L'aboutissement d'un travail de plus de 2 ans

Au total, 1215 institutions ou particuliers ont contribué à cette proposition de réglementation

En quoi l'**AI Act** se distingue des papiers précédents?

- Données
- RGPD
- Intelligence Artificielle

L'UE se positionne en tant que leader sur la mise en œuvre d'une réglementation internationale et stimule l'innovation

Lignes directrices de la CE

Lignes directrices en matière d'éthique pour une IA digne de confiance

8 avril 2019

Document de la CE

Stratégie européenne pour les données

19 février 2020

AEPD Guide

Adaptation du Règlement général sur la protection des données (RGPD) aux produits et services d'IA

13 février 2020

Rapport de la CE

Impact en matière de sécurité et de responsabilité de l'IA, de l'IoT et de la robotique

19 février 2020

Document de la CE

Livre blanc sur l'IA

19 février 2020

Étude du PE

L'impact du RGPD sur l'IA

15 juillet 2020

Liste d'évaluation de la CE

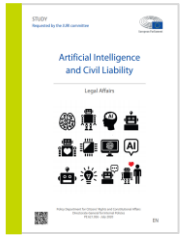
IA digne de confiance (ALTAI) pour l'auto-évaluation

17 juillet 2020

Étude du PE

IA et respect de la loi

13 juillet 2020



Étude du PE

IA et responsabilité civile (affaires juridiques)

13 juillet 2020

Document de proposition de la CE

Data Governance Act

25 novembre 2020

Étude du PE

Régime de responsabilité civile pour l'IA

18 septembre 2020

Étude du PE

Cadre de l'UE sur les aspects éthiques de l'IA, de la robotique et des technologies connexes

20 septembre 2020

AI ACT

Réglementation sur une approche européenne de l'IA

21 avril 2021

Entrée en vigueur de l'AI ACT

2019 — 2020 — T1 (en) — T2 (en) — T3 (en) — 2021 — 2023-2025

L'objectif de l'AI Act

La proposition prévoit un cadre législatif pour traiter l'IA à l'avenir, dans le but de stimuler l'innovation et d'atténuer les risques.

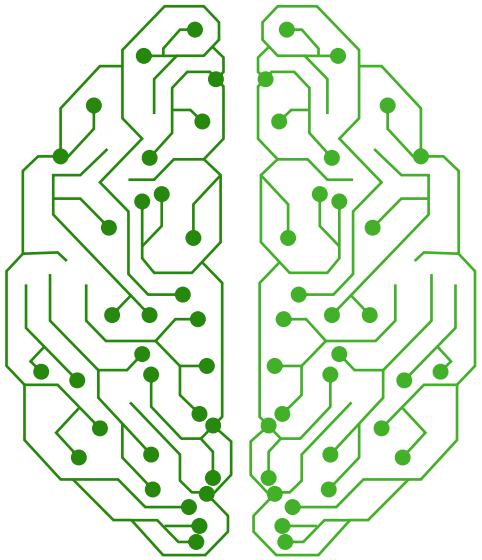
Comment tenez-vous compte des implications éthiques des cas d'usage **IA**?

L'IA Act à pour ambition de ...

Favoriser la collaboration et l'**égalité de traitement** entre les États membres de l'UE et protéger les droits fondamentaux des citoyens européens à l'ère de l'IA.

Établir un processus et des rôles pour assurer la **qualité** au lancement ainsi que tout au long du cycle de vie.

Assurer le mise en place d'une **IA éthique**, inculquer les valeurs européennes tout en améliorant la transparence.



Comment il compte y parvenir...

Mettre en place une **norme unique dans toute l'UE** pour éviter la fragmentation.

Garantir une **sécurité juridique** qui encourage l'innovation et l'investissement dans l'IA en créant des « bacs à sable réglementaires » pour l'IA.

Mettre en place une **base de données européenne publique** pour les cas d'usage IA « très risqués » et un code de conduite.

Sanctions

Les infractions peuvent entraîner jusqu'à **30 millions d'euros d'amende ou 6% du chiffre d'affaires annuel mondial** en cas de violation de l'Art. 5 ou l'Art. 10.

Tout autre manquement aux exigences ou aux obligations peut entraîner une amende de **20 millions d'euros ou de 4% du chiffre d'affaires annuel mondial**.

Informations inexactes ou trompeuses soumises aux organismes notifiés ou aux ANC : **10 millions d'euros ou 2% du chiffre d'affaires annuel mondial**.

Une définition vaste de l'IA

L'AI Act prend en compte le Machine Learning, mais aussi de nombreux modèles statistiques utilisés depuis des années

Selon l'AI Act, quels sont les modèles en votre possession pouvant être considérés comme de l'**IA** ?

"L'intelligence artificielle (IA) désigne tout **logiciel** développé à l'aide d'**une ou plusieurs des techniques** et approches énumérées à l'**Annexe I**, et capable, pour un ensemble donné d'**objectifs définis par l'Homme**, de **générer des résultats** tels que du contenu, des prédictions, des recommandations ou des décisions **influençant les environnements** avec lesquels ils interagissent "

Machine Learning, comprenant l'apprentissage supervisé, non supervisé et par renforcement, ainsi qu'une grande variété d'autres méthodes comme le Deep Learning.

Approches fondées sur la logique et la connaissance, y compris la représentation des connaissances, la programmation inductive (logique), les bases de connaissances, les moteurs d'inférence et déductifs, le raisonnement (symbolique) et les systèmes experts.

Approches statistiques, estimation bayésienne, méthodes de recherche et d'optimisation

Complète

Couvre toutes les IA actuelles et futures, y compris le Machine Learning, le Deep Leraning ainsi que les systèmes hybrides.

A l'épreuve du futur

En se concentrant davantage sur les risques et les cas d'usage que sur la technologie elle-même.

Sécurité juridique

Aussi neutre que possible en ce qui concerne les détails techniques, afin de couvrir les applications qui ne sont pas encore connues ou développées.

Le champ d'application de l'AI Act

La proposition se concentre sur les systèmes d'IA « très risqués » fournis/utilisés au sein de l'Union Européenne.

Comment êtes-vous affecté ? En tant que fournisseur ? Importateur ? Distributeur ? Utilisateur ?

Quelles sont les entités concernées par l'AI Act ?

Entités concernées

- Tout organismes à l'intérieur et à l'extérieur de l'UE qui fournit un système d'IA à destination et/ou qui impacte des individus dans l'UE
- Tout Fournisseurs/Importateurs/Distributeurs mettant à disposition un système d'IA au sein de l'UE
- Tout utilisateur de systèmes d'IA au sein de l'UE
- Tout fournisseur ou utilisateur situé dans un pays tiers, mais dont le résultat produit par le système d'IA est utilisé dans l'Union Européenne

Entités hors du champ d'application

- Autorités publiques d'un pays tiers ou organismes internationaux utilisant des systèmes d'IA dans le cadre d'accords internationaux de coopération policière et judiciaire avec l'Union ou avec un ou plusieurs États membres
- Utilisation purement privée et non commerciale

Aperçu des systèmes d'IA

La proposition utilise une approche fondée sur le risque pour différencier quatre types de systèmes d'IA en fonction de leurs potentiels dangers et risques.

Avez-vous fait le point sur vos systèmes d'**IA** actuels et leur degré de risque ?

1

Systèmes d'IA à risque « inacceptable » (Art. 5)

Mise en œuvre Interdite

- Manipulation du comportement, des opinions et des décisions de l'homme
- Classification des individus en fonction de leur comportement social
- Identification biométrique à distance en temps réel, sauf exceptions sur autorisation spéciale

Exemple : Scoring social

2

Systèmes d'IA « très risqués » (HRAIS, Art. 6)

Autorisés sous réserve de conformité aux exigences d'une évaluation ex-ante *

- Principaux axes du règlement (Annexe III)
- Régimes communs avec ceux déjà soumis à une norme européenne harmonisée
- Liste supplémentaire à réexaminer chaque année par le Conseil d'administration européen de l'IA « AI board » (Art. 84)

Exemple : Recrutement

3

Systèmes d'IA avec des obligations spécifiques de transparence (Art. 52)

Autorisés mais soumis à des obligations d'information/de transparence

- Interaction avec les humains
- Utilisés pour détecter des émotions ou déterminer des catégories sur la base de données biométriques
- Génération de contenus modifiés/créés par IA

Exemple : Bot agissant comme un humain (bots)

4

Systèmes d'IA à risque minime ou nul

Autorisé sans aucune restriction

Exemple : Maintenance prédictive

*A l'exception des systèmes d'IA « très risqués » développés ou utilisés à des fins militaires. Pour les HRAIS qui sont régis par l'un des articles suivants, seul l'article 84 devrait s'appliquer.
Règlement (CE) 300/2008 ; Règlement (UE) 167/2013 ; Règlement (UE) 168/2013 ; Directive 2014/90/UE ; Directive (UE) 2016/797, Règlement (UE) 2018/858;Règlement (UE) 2018/1139 ; Règlement (UE) 2019/2144.

Systèmes d’IA à risque « inacceptable » (art. 5)

Les applications d'IA qui présentent un risque « inacceptable » sont interdites.

Fournissez-vous des systèmes d'**IA** qui seraient considérés à risque « inacceptable » ?

1 **Manipulation subliminale** entraînant un préjudice physique/psychologique

Exemple : Pour pousser les chauffeurs routiers à conduire plus longtemps que ce qui est sain et sûr, un son inaudible est diffusé dans leur cabine. L'IA est utilisée pour trouver la fréquence qui maximise cet effet sur les conducteurs.

2 **Exploitation d'enfants, de personnes handicapées mentales ou de personnes vulnérables** entraînant un préjudice physique/psychologique

Exemple : Un jouet avec un assistant vocal intégré pousse les enfants à adopter un comportement dangereux sous couvert d'un jeu d'apprentissage.

3 **Scoring social à usage général**

Exemple : Un système d'IA calcule l'échelle de crédit des personnes sur la base d'un "mauvais comportement" social insignifiant ou non pertinent.

4 **Identification biométrique à distance en temps réel** afin de maintenir l'ordre dans les espaces accessibles au public**.

* * Il existe des exceptions

Exemple : Pour trouver un petit délinquant, toutes les caméras publiques disponibles scannent chaque visage qui apparaît dans le champ de vision de la caméra et le comparent à une base de données en temps réel.

Systèmes d’IA « très risqués » (HRAIS, Art. 6)

L'IA « très risquée » est définie à la fois par des caractéristiques générales et des domaines spécifiquement ciblés.

Fournissez-vous des systèmes d'**IA** qui seraient considérés comme « très risqués » ?

Systèmes d’IA « très risqués » (article 6)

- Systèmes d'IA utilisés comme un composant orienté sécurité d'un produit ou utilisé comme un produit à part entière
- Produits ou systèmes d’IA couverts par la législation d'harmonisation de l'Union énumérée à l'annexe II
- Produits ou systèmes d’IA pour lequel la mise en service ou la mise sur le marché nécessite une évaluation de la conformité par un organisme tiers

Domaines spécifiques à l'IA « très risquée » (Annexe III)

- La liste comprend les éléments suivants :
    1. Identification biométrique et catégorisation de personnes physiques
    2. Gestion et exploitation d’infrastructures critiques
    3. Éducation et formation professionnelle
    4. Emploi, gestion des collaborateurs et accès au travail indépendant
    5. Accès et jouissance aux services privés essentiels et aux services et prestations publics
    6. Application du droit
    7. Gestion de migrations, d'asile et de contrôles aux frontières
    8. Administration de la justice et processus démocratiques
- Tous les systèmes d'IA dans ces domaines ne sont pas « très risqués »
- La liste est mise à jour régulièrement (12 mois, article 84)

Systèmes d’IA « très risqués » (HRAIS, Art. 6)

Les systèmes d’IA « très risqués » doivent à la fois se conformer à des normes de qualité strictes et respecter les exigences en matière de divulgation, de contrôle et de suivi.

Quelle infrastructure de gouvernance avez-vous mise en place pour vos systèmes d'**IA** ?

Système de gestion des risques

- Processus itératif et continu comprenant des tests appropriés
- Estimation, évaluation et préparation aux risques prévisibles

Sauvegarde

- Conçu avec un enregistrement automatique des événements ("logs") :
- Période de chaque utilisation du système
- Personne physique participant à la vérification des résultats

Robustesse, précision et cybersécurité

- Conçu pour atteindre un niveau approprié de précision, de robustesse et de cybersécurité tout au long du cycle de vie
- Les niveaux appropriés sont déclarés dans la documentation du système d'IA

Données et gouvernance des données

- Des techniques appropriées de gouvernance et de gestion des données doivent être appliquées
- Ensemble de données de haute qualité et gouvernance pointue :
- Découpage des données : train, validation et test
- Données pertinentes, représentatives, exempt d’erreur et complètes
- Évaluation préalable de la disponibilité, la quantité, la pertinence et la partialité des données

Transparence et information

- Transmission de renseignements aux utilisateurs
- Le système doit être accompagné d'un mode d'emploi :
- Informations concises, complètes, correctes et claires
- Renseignement pertinents, accessibles et compréhensibles pour les utilisateurs
- Caractéristiques et limites du système d'IA

Documentation technique

- Avant la mise sur le marché
- Mise à jour continue

Supervision humaine

- Des outils d'interface humaine doivent être intégrés
- Possibilité de trouver des signes d'anomalies, de dysfonctionnements et de performances inattendues
- Possibilité de ne pas utiliser le système d'IA ; de neutraliser, d'arrêter ou d'inverser la sortie.

Systèmes d'IA à risque limité ou faible

Bien qu'il soit axé sur les IA « très risquées », l'AI Act préconise la transparence et un code de conduite pour les applications à faible risque

Vos utilisateurs sont-ils informés qu'ils interagissent avec un système d'**IA** ?

Nouvelles obligations de transparence pour certains systèmes d'IA (Art. 52)

- Informer les gens qu'ils interagissent avec un système d'IA, sauf si cela est évident.
- Prévenir les usagers en cas d'utilisation de systèmes de catégorisation par biométrie ou reconnaissance émotionnelle
- Apposer un label identifiant les "deep fake" (avec certaines exceptions) ou tout autre contenu modifié et ou créé grâce à une IA

Code de conduite éventuel sur la base du volontariat pour l'IA avec des exigences de transparence spécifiques (art. 69)

- Pas d'obligations
- La Commission et le Conseil définiront des codes de conduite destinés à favoriser l'application sur la base du volontariat des exigences aux systèmes d'IA à faible risque
- Ce code de conduite pourrait inclure la durabilité environnementale ou l'accessibilité aux personnes handicapées
- Les codes de conduite peuvent aussi être définis individuellement

Structure de gouvernance

L'AI Act suit une chaîne de responsabilité claire entre les entités nationales et supranationales.

Quels sont les organismes de régulation de l'**IA** ?

La Commission Européenne

Élaborer de nouvelles lignes directrices pour les recommandations du « AI board » et d'un groupe d'experts.

État membre

- Rôle clé dans l'application et le respect du règlement
- Désigner les autorités nationales compétentes

Groupe d'experts (en cours de planification)

Fournir une expertise et des recommandations supplémentaires, si nécessaire

AI board

- Des représentants de haut niveau des autorités nationales compétentes, le Contrôleur européen de la protection des données et la Commission.
- Fournir des conseils et une assistance à la Commission
- Contribuer aux activités de coordination et de coopération

Les **Autorités Nationales Compétentes (ANC)** garantissent l'application de la réglementation et servent d'unique source de vérité.

Notifying Authority (NA)*

Fournir et exécuter des processus d'évaluation, de désignation et de notification des organismes d'évaluation de conformité et de leur surveillance.

*Autorité d'avis

Autorité de surveillance nationale

- Coordonner les activités, faire office de point de contact pour la CE, représenter l'État membre au sein de l'« AI board ».
- Agir en tant que « NA » et « MSA », sauf si l'État membre désigne plus d'une autorité.

Market Surveillance Authority (MSA)*

- Surveiller les activités du marché
- Informer les autorités nationales en cas de violation des obligations
- Exercer des activités et prendre des mesures conformément à la réglementation (UE) 2019/1020.

*Autorité de surveillance du marché

Les **organismes d'évaluation de conformité** demandent une notification et deviennent ainsi des organismes notifiés.

Organisme notifié

- Réaliser une évaluation de conformité : les essais, la certification et l'inspection
- Coopérer avec les autorités nationales compétentes

Parties prenantes : rôles et obligations

Les parties prenantes sont interconnectées et chacune doit remplir des obligations spécifiques

Quels sont les rôles qui vous concernent ?

Source

Fournisseur

Développe un système d'IA avec l'intention de le mettre sur le marché et/ou en service dans l'UE

- Vérification de conformité
- Système de gestion de la qualité
- Documentation technique et mises à jour
- Enregistrement des activités du système d'IA
- Evaluation de conformité
- Coopération et collaboration permanente avec les « NCA »*
- Enregistrer le système d'IA dans une base de données européenne
- Apposer l'agrément CE et signer la déclaration de conformité
- Surveillance après la mise sur le marché

* National Competent Authorities

Intermédiaire

Importateur & Distributeur

L'importateur met l'IA (provenant de l'extérieur de l'UE) sur la marché ou en service. Le distributeur rend l'IA accessible aux autres

- S'assurer de l'évaluation de la conformité, et de l'existence d'une documentation technique, des instructions et du marquage CE
- Retirer, rappeler ou ne pas mettre le système d'IA sur le marché en cas de non-conformité réglementaire ou de non-respect des exigences
- S'assurer que le processus d'approvisionnement de l'IA n'entraîne pas de problèmes de conformité

Représentant mandaté

- Exécuter les tâches spécifiées dans le mandat émis par le fournisseur
- Tenir des registres : déclaration de conformité, documentation technique

Utilisateur final

Utilisateur

Entité utilisant un système d'IA pour ses activités professionnelles

- Utiliser le système d'IA conformément aux instructions
- Garantir la surveillance humaine
- Vérifier que les données saisies soient adaptées au but recherché
- Suivi continu des activités du système d'IA
- En cas de dysfonctionnement ou d'identification d'incidents graves ou d'autres risques, informer le fournisseur ou le distributeur du système d'IA
- Tenir des registres pendant une période donnée
- Satisfaire aux obligations légales et réglementaires en vigueur

Conformité tout au long du cycle de vie d'IA

Le lancement du produit n'est que le début des obligations de conformité pour les systèmes d'IA « très risqués »

Quels sont les rôles qui vous concernent ?

1 Conception conforme aux exigences

S'assurer que les systèmes d'IA fonctionnent de manière cohérente pour l'usage auquel ils sont destinés et soient conformes aux exigences de la réglementation

2 Evaluation de conformité

- Evaluation ex-ante de la conformité
- Exécutée par le fournisseur (Art. 43) :
  - sur la base des contrôles internes (Annexe VI)
  - sur la base d'une évaluation du système de gestion de la qualité et de la documentation technique avec l'engagement d'un organisme notifié (Annexe VII)

3 Surveillance post-commercialisation

Les fournisseurs doivent collecter, analyser et enregistrer de manière régulière et uniforme des données pertinentes pour garantir la fiabilité, la performance et la sécurité des systèmes d'IA durant tout leur cycle de vie et évaluer leur conformité continue au regard la réglementation

4 Système de notification des incidents

Communiquer et enregistrer les événements graves ainsi que les dysfonctionnements entraînant une violation des droits fondamentaux

5 Nouvelle évaluation de conformité

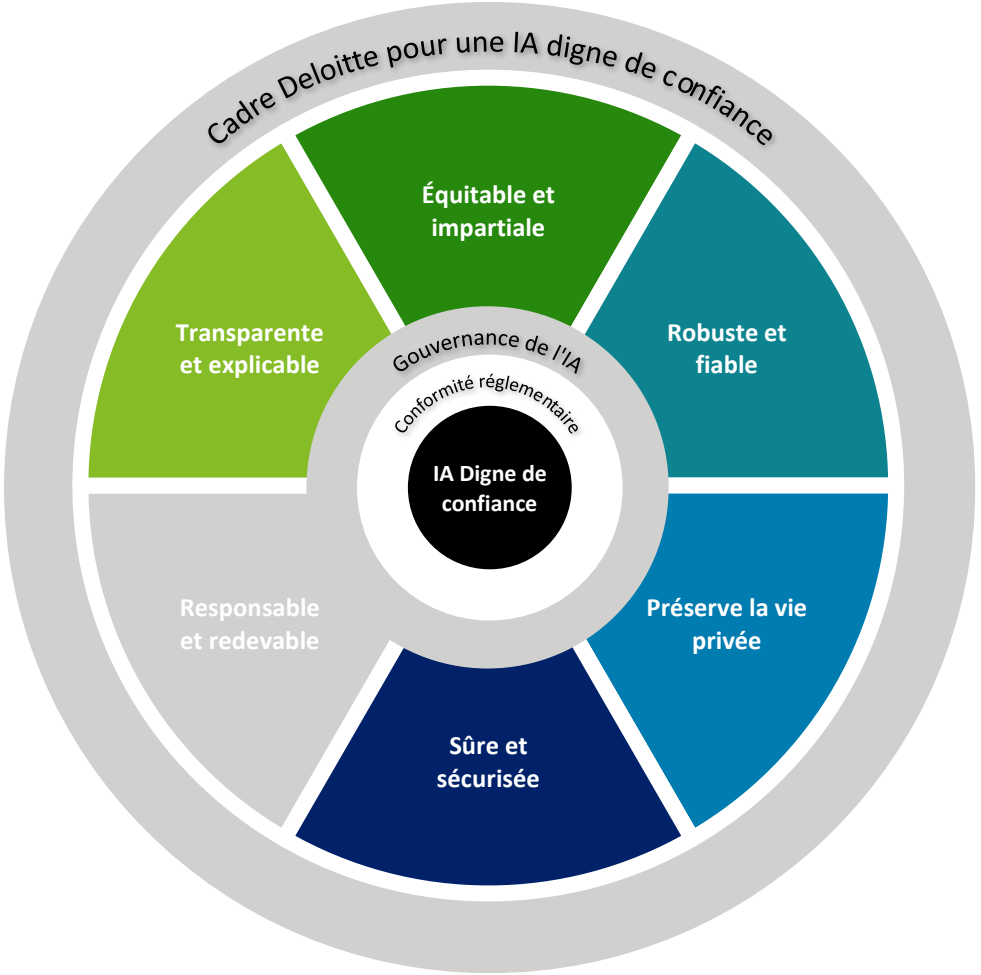
- Toute modification substantielle, telle que le changement d'objectif du système, nécessite un renouvellement de l'évaluation de la conformité
- Une évaluation par le fournisseur ou un tiers quelconque
- Prise en considération également des ajustements autres que ceux indiqués par le fournisseur pour les systèmes d'IA à apprentissage continu

Nous sommes prêts, et vous ?

La réglementation définit les exigences relatives à l'IA au sein de l'UE. Elle entraînera des changements. Nous proposons une voie à suivre.

Y a-t-il un écart entre la loi sur l'**IA** et vos normes ? Quelle est son ampleur ?

- Le projet de règlementation met l'accent sur une **application éthique** de l'IA, sur le fait que les cas d'usage soient **responsables**, et que les praticiens soient **tenus de respecter** des normes de qualité strictes.
- Cela inclut des principes généraux de traitement **équitable et impartial** des sujets (indépendamment de l'application de l'IA), mais interdit aussi explicitement certaines applications.
- L'AI Act met l'accent sur les applications "très risquées" et exige une grande transparence accompagnée de contrôles rigoureux pour garantir la **robustesse et la fiabilité** des systèmes d'IA.
- Pour garantir un fonctionnement **sûr et sécurisé** de l'IA, le règlement exige une surveillance humaine, la capacité d'assumer le contrôle ou de passer outre l'IA.
- Même pour les applications jugées à moindre risque, l'AI Act exige que les systèmes d'IA soient suffisamment **transparents**, en alertant les individus de l'usage d'une IA, et qu'ils soient **explicables**, permettant à leurs concepteurs de les contrôler efficacement.
- Le projet de règlementation est fondé sur les droits fondamentaux des citoyens, en se prémunissant contre l'exploitation des vulnérabilités, imposant une procédure standardisée, en défendant les droits des enfants, entre autres. Il **préserve la vie privée** en interdisant purement et simplement les applications de l'IA pour la surveillance en direct et à distance des citoyens.



Vos 7 étapes vers la conformité

La règlementation exige une déclaration de conformité et un **agrément** CE avant le lancement d'un système d'IA « très risqué », ainsi qu'un monitoring tout au long de son cycle de vie…

Que faut-il changer dans vos processus d'IA pour intégrer **l'AI Act**?

1 Identification

Réaliser un examen approfondi des actifs existants pour repérer ceux qui utilisent de l'IA ou ceux qui peuvent être qualifiés d'IA en vertu de la nouvelle législation.

2 Classification

Evaluer le niveau de risque potentiel pour chaque actif (inacceptable, très risqué ou faible).

3 Conformité

S'assurer que la conception, le développement et la qualité des systèmes de gestion soient conformes à la réglementation

4 Evaluation de conformité

Les systèmes d'IA « très risqués » doivent être soumis à une évaluation spécifique de la conformité (Art. 19 et 43) et cette étape doit être réitérée en cas de modification substantielle future.

3 Déclaration CE

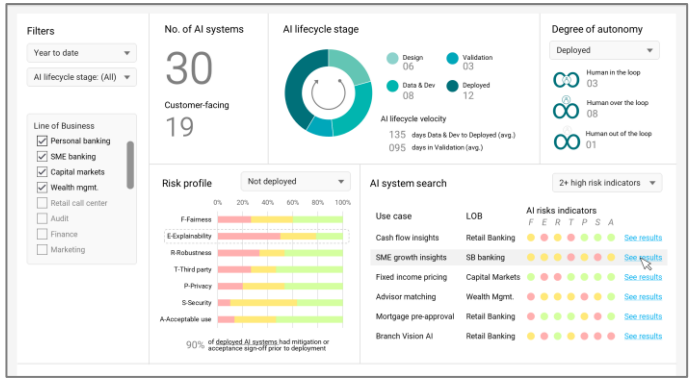
Rédiger une déclaration de conformité (Annexe 5) pour tout système d'IA « très risqué » et apposer le l'agrément CE*

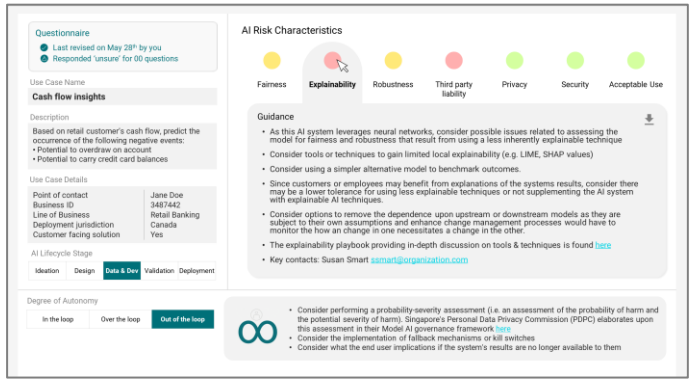
6 Commercialisation

Mise sur le marché ou en service du système d'IA « très risqué ».

7 Pilotage

Répondre aux besoins d'un suivi régulier après le lancement du système d'IA « très risqué ».





Deloitte a développé un outil pour aider les organisations à **gouverner et à gérer** efficacement les **risques associés à l'utilisation de systèmes d'IA** tout au long du cycle de vie.

Un questionnaire détaillé permet d'évaluer correctement les risques. Des résultats concrets et visibles sont présentés sur des tableaux de bord / dashboards.

* Le marquage «CE» indique qu'un actif est conforme aux exigences réglementaires

Contacts

Équipe Trustworthy AI – France

Gregory Abisror

Partner
– Deloitte France

gabisror@deloitte.fr

+336 32 83 52 36

Richard Eudes

Directeur
– Deloitte France

reudes@deloitte.fr

+336 49 12 10 62

Yves Yota Tchoffo

Senior Manager
– Deloitte France

yyotatchoffo@deloitte.fr

+336 31 34 35 70