Guide de mise en œuvre de l'*AI Act*

Partie 1 : Obligations

1.1 Cartographie des obligations applicables aux organisations

Cigref
RÉUSSIR LE NUMÉRIQUE

numeum
Engager le numérique

Table des matières

Introduction

Les entreprises, les administrations publiques, dès lors qu'elles intègrent des processus numérisés, doivent se préparer à assurer leur conformité à la loi européenne sur l'intelligence artificielle.

Le défi étant de taille, l'application de l'*AI Act* se fera progressivement sur une période de deux ans.

À partir du 2 février 2025, l'interdiction des systèmes d'IA « à risque inacceptable » s'appliquera. Il faut donc que les organisations concernées identifient dès à présent si elles ont des systèmes d'IA répondant à cette définition. Pour cela, elles doivent commencer sans plus attendre à cartographier les obligations auxquelles elles sont soumises.

La « cartographie des obligations applicables aux organisations » propose aux praticiens du numérique un mode opératoire pour identifier les obligations liées aux IA, applicables à leur organisation et déterminées dans l'*AI Act*, en fonction du type d'IA (système ou modèle), du risque associé (inacceptable à minime) et du rôle de l'organisation dans la chaîne de valeur (fournisseur, déployeur, mandataire, importateur et distributeur).

Le **processus à suivre pour chaque type d'IA** est le suivant :

- **Déterminer la nature de l'IA ;**
- **Analyser les risques ;**
- **Identifier le rôle de son organisation pour cette IA ;**
- **En déduire ses obligations.**

Cette démarche est illustrée dans le schéma suivant.

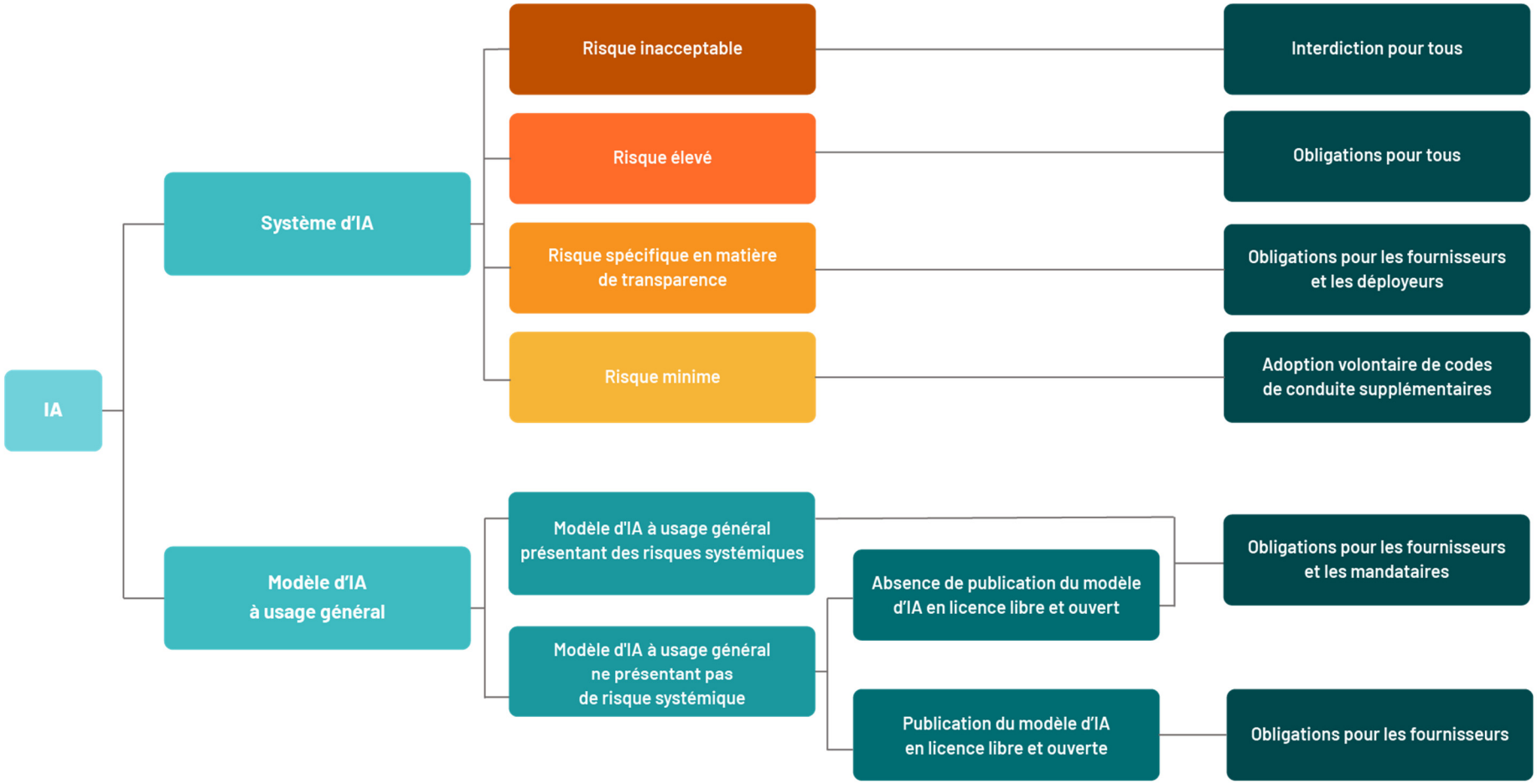

Figure 1 : Arbre de décision des obligations

1.1.1 Déterminer la nature de l'IA

L'approche de l'*AI Act* est simple : il faut dans un premier temps **distinguer** les **« systèmes d'IA »** des **« modèles d'IA à usage général »**.

Définitions : système d'IA et modèle d'IA à usage général

Système d'IA (art. 3§1) : système automatisé, conçu pour fonctionner à différents niveaux d'autonomie et pouvant faire preuve d'une capacité d'adaptation après son déploiement, qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer différentes sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels.

Autrement dit, un système d'IA peut être utilisé seul ou en tant que composant d'un produit, que le système soit physiquement incorporé dans le produit (intégré) ou qu'il serve de fonctionnalité au produit sans y être intégré (non intégré). Cette distinction facilite la compréhension des différentes catégories et des usages possibles des systèmes d'IA, en particulier dans le contexte réglementaire.

Exemple : ChatGPT est un système d'IA fournissant un *chatbot* conversationnel pour répondre aux utilisateurs.

Modèle d'IA à usage général (art. 3§63) : modèle d'IA qui, y compris lorsque il est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, présente **une grande généralité**, et est capable d'exécuter de manière compétente un **large éventail de tâches distinctes**, indépendamment de la manière dont le modèle est mis sur le marché, et à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché. Le modèle d'IA à usage général peut être intégré dans une variété de systèmes ou d'applications en aval.

Exemple : GPT (*Generative Pre-trained Transformer*) est un modèle développé pour le traitement du langage naturel (à l'instar d'OpenAI GPT).

Le processus à suivre est traité, dans **la section 1.1.2** pour les **systèmes d'IA**, et dans **la section 1.1.3** pour les **modèles d'IA**.

1.1.2 Les systèmes d'IA (SIA)

Ce premier volet propose 3 étapes pour cartographier les systèmes d'IA (SIA) afin d'identifier les obligations auxquelles se conformer. L'approche consiste à classer les systèmes d'IA en fonction de leur niveau de risque, puis d'identifier la place de l'organisation dans la chaîne de valeur pour chacun d'eux, afin d'en déduire les obligations à respecter au titre de l'*AI Act*.

Elle se construit en 3 étapes :

1/ Analyser le niveau de risque

Cette étape permet de qualifier les risques de chaque système d'IA au sein de l'organisation.

2/ Déterminer son rôle

Cette étape aide à déterminer pour chacun des systèmes d'IA, le rôle de l'organisation dans la chaîne de valeur.

3/ Identifier ses obligations

Cette étape permet d'identifier les obligations incombant à l'organisation qui découlent de ces deux critères (décrites dans les **FICHES 1 à 8**).
Un tableau récapitulatif des obligations selon les risques et les opérateurs concernés est présenté **FICHE 9**.

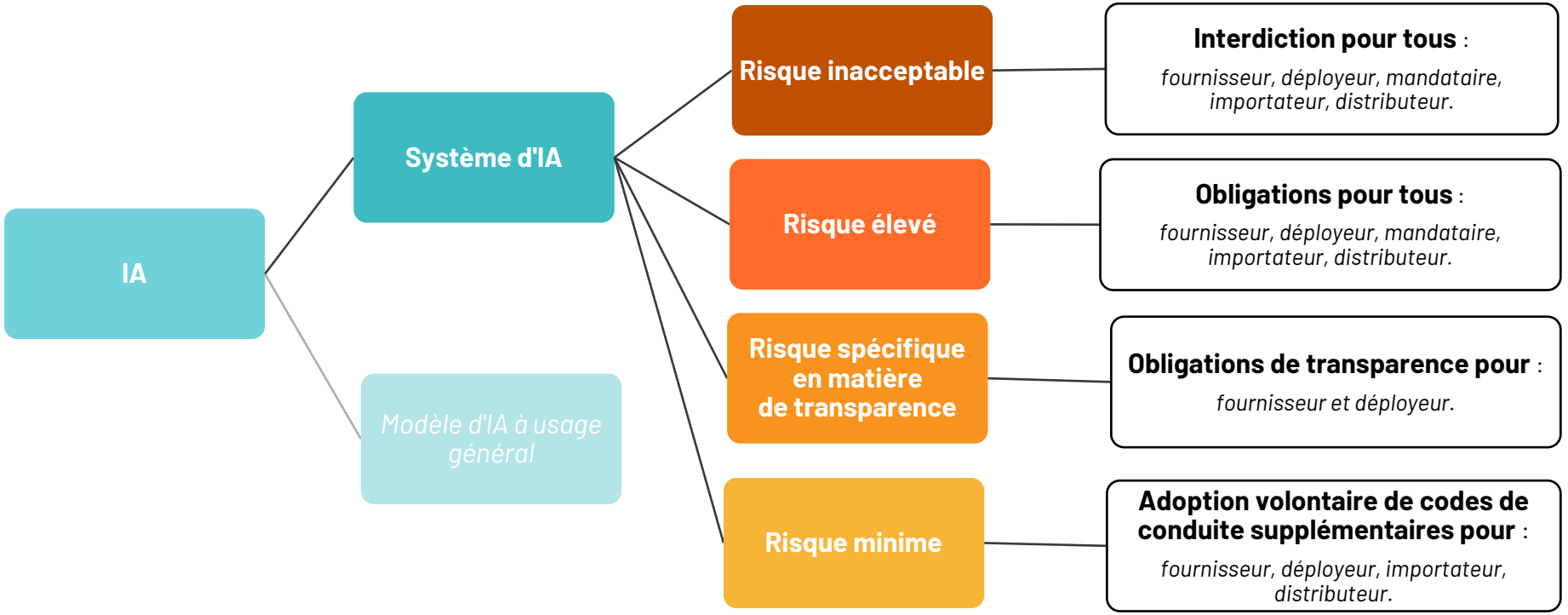

Figure 2 : Arbre de décision des obligations pour les SIA

1.1.2.1 Analyser le niveau de risque des systèmes d'IA (SIA)

Cette première étape a pour objectif d'identifier le niveau de risque de chaque système d'IA, échelonné sur 4 niveaux : risque inacceptable, risque élevé, risque spécifique en matière de transparence et risque minime.

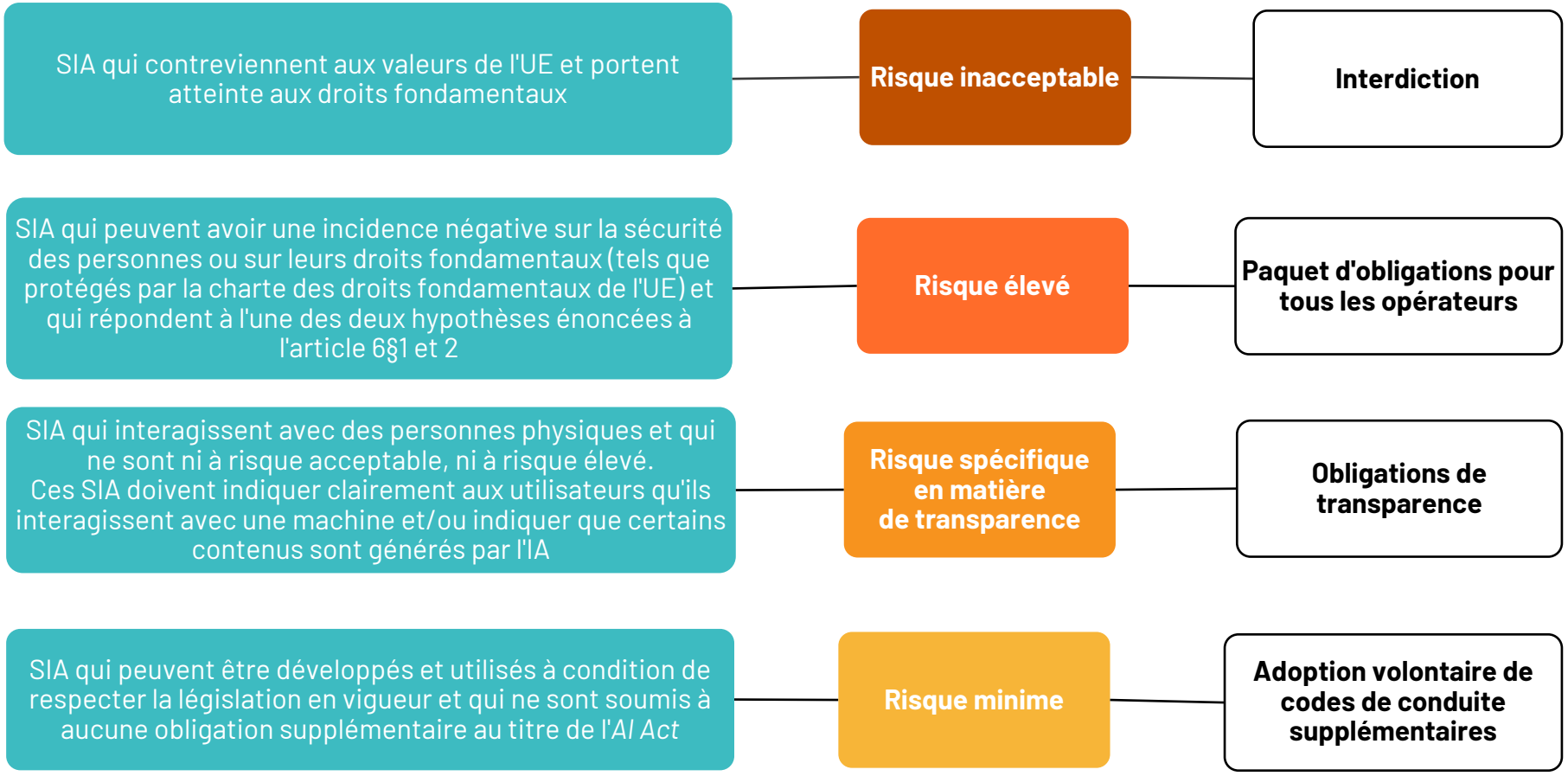

Figure 3 - Récapitulatif de la qualification des risques des systèmes d'IA

Risque inacceptable

Article 5 de l'*AI Act*

Un système d'IA à risque inacceptable est un SIA qui répond à l'un de ces 8 cas :

1. recourt à des **techniques subliminales** ou des **techniques manipulatrices** ou **trompeuses** ayant pour **objectif/effet d'altérer le comportement** d'une personne et **l'amenant ainsi à prendre une décision qu'elle n'aurait pas prise** autrement, ce qui causerait un **préjudice** ;

2. **exploite des vulnérabilités (dues à l'âge, au handicap ou à la situation sociale ou économique)** d'une personne en ayant pour objectif/effet **d'altérer substantiellement son comportement,** d'une manière qui causerait un **préjudice important à cette personne ou à un tiers ;**

3. **évalue/classifie des personnes** en **fonction de leur comportement social (similaire au « *crédit social* ») ou de caractéristiques personnelles ou de personnalités connues** conduisant à un **traitement préjudiciable ou défavorable** ;

4. **évalue les risques** d'une personne à **commettre une infraction pénale uniquement sur la base du profilage d'une personne ou de l'évaluation de ses traits de personnalité ou caractéristiques** ;

5. **crée/développe** des **bases de données** de **reconnaissance faciale** par le moissonnage non ciblé d'images faciales provenant d'internet ou de la vidéosurveillance ;

6. **infère les émotion**s d'une **personne** sur le **lieu de travail/établissement d'enseignement** (sauf raison médicale ou de sécurité) ;

7. utilise des **catégorisations biométriques** aux fins de l'authentification ou pour classer **individuellement des personnes** et en **déduire** leur **race**/ leurs **opinions politiques**/ leur affiliation à une **organisation syndicale**/ leurs **convictions religieuses** ou **philosophiques**/ leur **vie sexuelle** ou leur **orientation sexuelle,** (à moins que cela ne soit accessoire à un autre service commercial et strictement nécessaire pour des raisons techniques objectives ; voir art. 3§40). Par exemple, sont interdits les filtres utilisés sur les services de réseaux sociaux en

ligne qui classent par catégorie les caractéristiques faciales ou corporelles afin de permettre aux utilisateurs d'ajouter ou de modifier des images ou des vidéos ;

8. utilise un système **d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives.**

Exemple : Les systèmes d'IA qui permettent une « notation sociale » par les gouvernements ou les entreprises sont considérés comme une menace évidente pour les droits fondamentaux des citoyens et sont donc interdits.

Les SIA à risque inacceptable sont **interdits à partir du 2 février 2025 (article 113)**. Dès lors, sont interdits « *la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA* » (article 5) :

- La « **mise sur le marché** » s'entend comme la première mise à disposition d'un système d'IA ou d'un modèle d'IA à usage général sur le marché de l'UE (article 3§9). Ainsi, la notion de « mise sur le marché » semble correspondre au moment où le produit est accessible pour être vendu/distribué, qu'il soit ou non utilisé immédiatement ;
- La « **mise en service** » s'entend comme la fourniture d'un système d'IA en vue d'une première utilisation directement au déployeur ou pour usage propre dans l'UE, conformément à la destination du système d'IA (article 3§10). Ainsi, la notion de « mise en service » semble correspondre à l'entrée en fonction d'un SIA dans un environnement d'usage.

Risque élevé

Article 6 de l'*AI Act*

Un système d'IA est qualifié de « SIA à risque élevé » dans deux hypothèses distinctes :

Hypothèse 1 : Le système d'IA répond aux 2 critères cumulatifs suivants :

- **L'usage comme composant de sécurité** : le système d'IA est utilisé comme un composant de sécurité dans un produit couvert par la réglementation européenne (voir Annexe I) ou est lui-même un produit (par exemple, le système d'IA est en lui-même un dispositif médical.)
- **L'évaluation de conformité** : le produit contenant le système d'IA fait l'objet d'une évaluation de conformité obligatoire effectuée par un organisme tiers avant d'être mis sur le marché ou en service.

Exemple : Les logiciels médicaux fondés sur l'IA ou les systèmes d'IA utilisés pour le recrutement doivent respecter des exigences strictes, notamment concernant les systèmes d'atténuation des risques, la qualité des ensembles de données utilisés, la fourniture d'informations claires à l'utilisateur, le contrôle humain, etc.

Hypothèse 2 : Le système d'IA relève des domaines listés à l'Annexe III :

- **Biométrie** : systèmes d'identification biométrique à distance ; systèmes d'IA destinés à être utilisés à des fins de catégorisation biométrique, en fonction d'attributs ou de caractéristiques sensibles ou protégés, sur la base de la déduction de ces attributs ou de ces caractéristiques ; systèmes d'IA destinés à être utilisés pour la reconnaissance des émotions.
- **Infrastructures critiques** : systèmes d'IA destinés à être utilisés en tant que composants de sécurité dans la gestion et l'exploitation d'infrastructures numériques critiques, du trafic routier ou de la fourniture d'eau, de gaz, de chauffage ou d'électricité.
- **Éducation et formation professionnelle** : systèmes d'IA destinés à déterminer l'accès, l'admission ou l'affectation de personnes physiques à des établissements d'enseignement ou de formation professionnelle ; systèmes d'IA destinés à évaluer les acquis d'apprentissage ; systèmes d'IA destinés à évaluer le niveau d'enseignement approprié qu'une personne recevra ou sera en mesure d'atteindre ; systèmes d'IA destinés à surveiller et détecter des comportements interdits chez les étudiants lors d'examens.
- **Emploi, gestion de la main-d'œuvre et accès à l'emploi indépendant** : systèmes d'IA destinés à être utilisés pour le recrutement ou la sélection de personnes physiques ; systèmes d'IA destinés à prendre des décisions influant sur les conditions des relations professionnelles,

la promotion ou le licenciement dans le cadre de relations professionnelles contractuelles, pour attribuer des tâches sur la base du comportement individuel, de traits de personnalité ou de caractéristiques personnelles ou pour suivre et évaluer les performances et le comportement de personnes dans le cadre de telles relations.

- **Accès et droit aux services privés essentiels et aux services publics et prestations sociales essentiels** : systèmes d'IA destinés à évaluer l'éligibilité des personnes physiques aux prestations et services d'aide sociale essentiels, y compris les services de soin santé ; systèmes d'IA destinés à évaluer la solvabilité des personnes physiques ou à établir leur note de crédit ; systèmes d'IA destinés à évaluer des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-vie et d'assurance maladie ; systèmes d'IA destinés à évaluer et à hiérarchiser les appels d'urgence émanant de personnes physiques ou à établir des priorités dans l'envoi des services de santé d'urgence.
- **Répression, dans la mesure où leur utilisation est autorisée par le droit de l'UE ou le droit national applicable** : systèmes d'IA destinés à évaluer le risque qu'une personne physique devienne la victime d'infractions pénales ; systèmes d'IA destinés à être utilisés comme polygraphes et outils similaires ; systèmes d'IA destinés à évaluer la fiabilité des preuves au cours d'enquêtes ou de poursuites pénales ; systèmes d'IA destinés à évaluer le risque qu'une personne physique commette une infraction ou récidive, ou destinés à évaluer les traits de personnalité, les caractéristiques ou les antécédents judiciaires de personnes physiques ou de groupes ; systèmes d'IA destinés à effectuer du profilage des personnes physiques dans le cadre de la détection d'infractions pénales, d'enquêtes ou de poursuites en la matière, ou de l'exécution de sanctions pénales.
- **Migration, asile et gestion des contrôles aux frontières, dans la mesure où leur utilisation est autorisée par le droit de l'UE ou le droit national applicable** : systèmes d'IA destinés à être utilisés comme polygraphes et outils similaires ; systèmes d'IA destinés à évaluer un risque posé par une personne physique qui a l'intention d'entrer ou qui est entrée sur le territoire d'un État membre ; systèmes d'IA destinés à aider les autorités compétentes à procéder à l'examen des demandes d'asile, de visas et de titres de séjour et à l'examen des plaintes connexes ; systèmes d'IA destinés à être utilisés dans le cadre de la migration, de l'asile et de la gestion des contrôles aux frontières, aux fins de la détection, de la reconnaissance ou de l'identification des personnes physiques.
- **Administration de la justice et processus démocratiques** : systèmes d'IA destinés à aider à rechercher et à interpréter les faits ou la loi, et à appliquer la loi à un ensemble concret de faits, ou destinés à être utilisés de manière similaire lors du règlement extrajudiciaire d'un litige ; systèmes d'IA destinés à influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums.

Une exception (article 6§3) :

Un système d'IA de l'Annexe III peut être exempté de la classification à « risque élevé » s'il ne présente pas de risques significatifs pour la santé, la sécurité ou les droits fondamentaux des personnes physiques. Cette exception ne s'applique que lorsque l'une des conditions suivantes est remplie :

- Le système d'IA exécute une tâche procédurale limitée ;
- Le système d'IA est conçu pour améliorer le résultat d'une activité humaine préalablement réalisée ;
- Le système d'IA est destiné à détecter les constantes en matière de prise de décision ou les écarts par rapport aux constantes habituelles antérieures et n'est pas destiné à se substituer à l'évaluation humaine préalablement réalisée, ni à influencer celle-ci, sans examen humain approprié ;
- Le système d'IA est destiné à exécuter une tâche préparatoire en vue d'une évaluation pertinente aux fins des cas d'utilisation visés à l'annexe III.

À noter qu'un système d'IA effectuant un profilage de personnes physiques est **toujours** considéré comme étant « à risque élevé ».

Les SIA à risque élevé sont soumis à différentes obligations selon le rôle de l'entreprise dans la chaîne de valeur, c'est-à-dire selon que l'entreprise sera un fournisseur, déployeur, mandataire, importateur ou distributeur. Vous trouverez ces obligations dans le tableau « **Comment identifier les obligations qui incombent à son organisation ?** ».

Risque spécifique en matière de transparence

Article 50 de l'*AI Act*
Un système d'IA sera soumis à des obligations de transparence lorsqu'il **interagit directement avec des personnes physiques**.

Exemple : Les *chatbots*.

Ces SIA sont soumis à des obligations de transparence, selon le rôle de l'organisation dans la chaîne de valeur. Vous trouverez ces obligations dans le tableau **« Comment identifier les obligations qui incombent à son organisation ? »**.

Risque minime

Les systèmes d'IA qui ne répondent à aucune des conditions évoquées précédemment sont des SIA à risque minime pour lesquels il n'existe aucune obligation. **Les entreprises et organisations concernées pourront adopter volontairement des codes de bonnes pratiques. Ces derniers seront publiés par le Bureau de l'IA (Commission européenne) en mai 2025** et proposeront des recommandations pour guider tous les acteurs concernés. Ces recommandations viseront à encourager des pratiques responsables, même en l'absence d'obligations légales, afin de promouvoir la transparence, la sécurité, et le respect des droits fondamentaux.

Exemple : Les filtres anti-spam et les jeux vidéo fondés sur l'IA.

1.1.2.2 Déterminer le rôle de l'organisation

Cette deuxième étape a pour objectif d'identifier, pour chaque SIA, le rôle de son organisation dans la chaîne de valeur. Les types d'acteurs mentionnés ci-dessous sont regroupés sous le terme générique d'« **opérateurs** », qu'ils soient : fournisseurs, déployeurs, mandataires, importateurs ou distributeurs (voir article 3§8).

Identification des rôles dans la chaîne de valeur

Fournisseur

- Vous développez ou vous faîtes développer un SIA et le mettez sur le marché ou le mettez en service sous votre propre nom ou votre propre marque, à titre onéreux ou gratuit.
- Vous commercialisez sous votre propre nom ou votre propre marque un SIA à risque élevé déjà mis sur le marché ou mis en service.
- Vous apportez une modification substantielle à un SIA à risque élevé qui a déjà été mis sur le marché ou a déjà été mis en service de telle manière qu'il reste un SIA à risque élevé.
- Vous modifiez la destination d'un SIA, y compris d'un SIA à usage général, qui n'a pas été classé à risque élevé et a déjà été mis sur le marché ou mis en service de telle manière que le SIA concerné devient un SIA à risque élevé.

Déployeur

- Vous utilisez un SIA dans le cadre d'une activité non personnelle à caractère professionnel.

Mandataire

- Vous êtes situé ou établis dans l'UE et avez reçu et accepté un mandat écrit d'un fournisseur de SIA ou de modèle d'IA à usage général pour vous acquitter en son nom des obligations et des procédure établies.

Importateur

- Vous êtes situé ou établis dans l'UE et mettez sur le marché un SIA qui porte le nom ou la marque d'une personne physique ou morale établie dans un pays tiers.

Distributeur

- Vous n'êtes ni fournisseur ni importateur mais vous mettez à disposition un SIA sur le marché de l'UE.

1.1.2.3 Identifier les obligations incombant à l'organisation

Une fois le niveau de risque du SIA identifié et le rôle de l'organisation dans la chaîne de valeur déterminé, l'organisation peut connaître les obligations à observer. Elles sont récapitulées dans le tableau ci-dessous qui renvoie aux fiches 1 à 8, en fonction des obligations.
Un tableau récapitulatif des obligations selon les risques et les opérateurs concernés est présenté **FICHE 9**.

Comment identifier les obligations qui incombent à son organisation ?

	Fournisseur	Déployeur	Mandataire	Importateur	Distributeur
Risque inacceptable	Interdiction	Interdiction	Interdiction	Interdiction	Interdiction
Risque élevé	Obligations pour les fournisseurs d'IA à risque élevé **Voir FICHE 1**	Obligations pour les déployeurs d'IA à risque élevé **Voir FICHE 2**	Obligations pour les mandataires des fournisseurs d'IA à risque élevé **Voir FICHE 3**	Obligations pour les importateurs d'IA à risque élevé **Voir FICHE 4**	Obligations pour les distributeurs d'IA à risque élevé **Voir FICHE 5**
Risque spécifique en matière de transparence	Obligations pour les fournisseurs d'IA à risque spécifique en matière de transparence **Voir FICHE 6**	Obligations pour les déployeurs d'IA à risque spécifique en matière de transparence **Voir FICHE 7**	Aucune obligation	Aucune obligation	Aucune obligation
Risque minime	Adoption volontaire de codes de conduite supplémentaires **Voir FICHE 8**	Adoption volontaire de codes de conduite supplémentaires **Voir FICHE 8**	Adoption volontaire de codes de conduite supplémentaires **Voir FICHE 8**	Adoption volontaire de codes de conduite supplémentaires **Voir FICHE 8**	Adoption volontaire de codes de conduite supplémentaires **Voir FICHE 8**

FICHE 1

Obligations pour les fournisseurs de SIA à risque élevé

Selon l'article 16

Conformité	S'assurer de la conformité aux exigences énoncées à la section 2 intitulée « *Exigences applicables aux SIA à risque élevé* », incluant les articles 8 à 15.
Identification	L'identité du fournisseur doit être indiquée sur le SIA à risque élevé, si cela est possible, ou sur son emballage ou dans la documentation qui l'accompagne, selon le cas. Doivent apparaître le nom, la raison sociale ou la marque déposée, ainsi que l'adresse à laquelle le fournisseur peut être contacté.
Mise en place d'un système de gestion de la qualité	*Voir art. 17* Le fournisseur doit mettre en place un système de gestion de la qualité, documenté de manière méthodique et ordonnée sous forme de politiques, de procédures et d'instructions écrites, incluant : • Une stratégie de respect de la réglementation ; • Des techniques, procédures et actions systématiques destinées à la conception des SIA à risque élevé ainsi qu'au contrôle et à l'assurance de leur qualité ; • Des techniques, procédures et actions systématiques destinées au développement des SIA à risque élevé ainsi qu'au contrôle et à l'assurance de leur qualité ; • Des procédures d'examen, de test et de validation à exécuter avant, pendant et après le déploiement du SIA à risque élevé, ainsi que la fréquence à laquelle elles doivent être réalisées ; • Des spécifications techniques ; • Les systèmes et procédures de gestion des données ; • Le système de gestion des risques ; • L'élaboration, la mise en œuvre et le fonctionnement d'un système de surveillance après commercialisation ; • Les procédures relatives au signalement d'un incident grave ;

	• La gestion des communications avec les diverses autorités ; • Les systèmes et procédures de conservation de tous les documents et informations pertinents ; • La gestion des ressources ; • Un cadre de responsabilisation définissant les responsabilités de l'encadrement et des autres membres du personnel.
Garantie de la conservation de la documentation	*Voir art. 18* Doivent être conservées pendant 10 ans après la mise sur le marché (MsM) ou la mise en service (MeS) : • La documentation technique visée à l'article 11 ; • La documentation sur le système de gestion de la qualité visée à l'article 17 ; • La documentation sur les modifications approuvées par les organismes notifiés ; • Les décisions et autres documents émis par les organismes notifiés ; • La déclaration UE de conformité visée à l'article 47.
Tenue des journaux générés automatiquement par les SIA à risque élevé, lorsqu'ils sont sous le contrôle du fournisseur	*Voir art. 19* Les journaux doivent être conservés au moins 6 mois.
Procédure d'évaluation de la conformité avant sa MsM et sa MeS	*Voir art. 43* À noter qu'il existe diverses évaluations de la conformité qui tiennent compte des caractéristiques des SIA à risque élevé : • Pour les SIA énumérés à l'annexe III point 1 ; • Pour les SIA visés à l'annexe III points 2 à 8 ; • Pour les SIA dont la liste figure à l'annexe I, section A.

	À noter que les SIA à risque élevé qui ont déjà été soumis à une procédure d'évaluation de la conformité sont soumis à une nouvelle procédure d'évaluation de la conformité lorsqu'ils font l'objet de modifications substantielles.
Déclaration UE de conformité	*Voir art. 47* Cette déclaration doit : • Être écrite, lisible par machine, signée à la main ou électroniquement et être tenue à la disposition des autorités nationales compétentes pendant une durée de dix ans à partir du moment où le SIA à risque élevé a été mis sur le marché ou mis en service ; • Attester que l'IA à risque élevé satisfait aux exigences ; • Contenir les informations visées à l'annexe V : o Nom et type du SIA et toute référence supplémentaire non ambiguë permettant l'identification et la traçabilité du système d'IA ; o Le nom et l'adresse du fournisseur ou, le cas échéant, de son mandataire ; o Une déclaration certifiant que la déclaration UE de conformité visée à l'article 47 est établie sous la seule responsabilité du prestataire ; o Une déclaration attestant que le SIA est conforme au règlement et, le cas échéant, à toute autre législation pertinente de l'Union qui prévoit l'établissement de la déclaration UE de conformité visée à l'article 47 ; o Lorsqu'un SIA implique le traitement de données à caractère personnel, une déclaration selon laquelle ce système d'IA est conforme aux règlements (UE) 2016/679 et (UE) 2018/1725 et à la directive (UE) 2016/680 ; o Références à toute norme harmonisée pertinente utilisée ou à toute autre spécification commune par rapport à laquelle la conformité est déclarée ; o Le cas échéant, le nom et le numéro d'identification de l'organisme notifié, une description de la procédure d'évaluation de la conformité suivie et la référence du certificat délivré ; o Le lieu et la date de délivrance de la déclaration, le nom et la fonction de la personne qui l'a signée, ainsi que l'indication de la personne pour laquelle ou au nom de laquelle elle a signé et une signature.

Marquage CE	*Voir art. 48* Le marquage CE implique le respect de plusieurs exigences : • Il est apposé de façon visible, lisible et indélébile sur le SIA à risque élevé, ou sur son emballage et sur les documents d'accompagnement ; • Le cas échéant, il est suivi du numéro d'identification de l'organisme notifié responsable des procédures d'évaluation de la conformité prévues à l'article 43, étant précisé que ce numéro est également indiqué dans tous les documents publicitaires mentionnant que le SIA à risque élevé est conforme aux exigences applicables au marquage CE. À noter que pour les SIA à risque élevé fournis numériquement, un marquage CE numérique n'est utilisé que s'il est facile d'y accéder soit par l'interface à partir de laquelle l'accès à ce système s'effectue soit au moyen d'un code facilement accessible lisible par machine soit par d'autres moyens électroniques.
Obligations en matière d'enregistrement	*Voir art. 49 §1* Avant de mettre sur le marché ou de mettre en service un SIA à risque élevé tel qu'énuméré à l'Annexe III (sauf concernant les SIA visés à l'Annexe III, point 2), le fournisseur ou le mandataire s'enregistre dans la base de données de l'UE et y enregistre son système.
Mesures correctives et devoir d'information	*Voir art. 20* Les fournisseurs de SIA à risque élevé qui considèrent ou ont des raisons de considérer qu'un SIA à risque élevé qu'ils ont mis sur le marché ou mis en service n'est pas conforme, prennent des mesures correctives nécessaires pour le mettre en conformité, le retirer, le désactiver ou le rappeler. Ils informent les distributeurs du SIA à risque élevé concerné et, le cas échéant, les déployeurs, les mandataires et les importateurs en conséquence. Lorsque le SIA présente un risque (cf. art. 79§1, c'est-à-dire – au sens de l'article 3, point 19) du règlement (UE) 2019/1020 – un SIA présentant des risques pour la santé ou la sécurité, ou pour les droits fondamentaux, des personnes) et que le fournisseur prend conscience de ce risque, il recherche les causes, en collaboration avec le

	déployeur à l'origine du signalement et, le cas échéant, informe les autorités de surveillance du marché, compétentes pour le SIA à risque élevé et, le cas échéant, l'organisme notifié qui a délivré un certificat pour ce SIA à risque élevé.
Preuve de la conformité du SIA à la demande des autorités	*Voir art. 21* Coopération avec les autorités compétentes : • À la demande motivée d'une autorité compétente, les fournisseurs de SIA à risque élevé doivent fournir toutes les informations et tous les documents nécessaires pour démontrer la conformité du SIA à risque élevé dans une langue aisément compréhensible par l'autorité ; • À la demande motivée d'une autorité compétente, les fournisseurs accordent l'accès aux journaux générés automatiquement par le SIA à risque élevé.
Vérification de la conformité aux directives (UE) 2016/2102 et (UE) 2019/882	Le fournisseur doit vérifier la conformité aux exigences en matière d'accessibilité conformément aux directives (UE) 2016/2102 et (UE) 2019/882.

Selon l'article 22§1

Désignation d'un mandataire par mandat écrit	Avant de mettre leurs SIA à disposition sur le marché de l'UE, les fournisseurs établis dans des pays tiers doivent désigner, par mandat écrit, un mandataire établi dans l'UE.
Autorisation attribuée à son mandataire	Le fournisseur doit autoriser son mandataire à exécuter les tâches indiquées dans le mandat que lui a confié le fournisseur.

FICHE 2

Obligations pour les déployeurs de SIA à risque élevé

Article 26

Mesures techniques et organisationnelles	Les déployeurs de SIA à risque élevé doivent prendre des mesures techniques et organisationnelles appropriées pour garantir qu'ils utilisent ces SIA conformément aux notices d'utilisation accompagnant les systèmes.
Contrôle humain	Les déployeurs doivent confier le contrôle humain à des personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaires ainsi que du soutien nécessaire.
Vérification des données d'entrée	Lorsque les déployeurs exercent un contrôle sur les données d'entrée, ils doivent veiller à ce que ces dernières soient pertinentes et suffisamment représentatives au regard de la destination du SIA à hrisque élevé.
Devoir d'alerte	• Obligation de surveillance : les déployeurs doivent surveiller le fonctionnement du SIA à risque élevé sur la base de la notice et, le cas échéant, informer les fournisseurs. • Obligation d'information en cas de risque : lorsque les déployeurs ont des raisons de considérer que l'utilisation du SIA à risque élevé présente un risque, ils en informent le fournisseur ou le distributeur ainsi que l'autorité de surveillance du marché concerné. • Obligation d'information en cas d'incident grave : lorsque les déployeurs ont détecté un incident grave, ils informent immédiatement d'abord le fournisseur, puis l'importateur ou le distributeur et les autorités de surveillance du marché concernées, de cet incident.

Tenue des journaux générés automatiquement	Les déployeurs doivent assurer la tenue des journaux générés automatiquement par ce SIA à risque élevé dans la mesure où ces journaux se trouvent sous leur contrôle, pendant une période adaptée à la destination du SIA à risque élevé, d'au moins six mois.
Informations des salariés	Les employeurs utilisant un SIA doivent informer les représentants des travailleurs et les travailleurs concernés qu'ils seront soumis à l'utilisation du SIA à risque élevé.
Enregistrement pour les autorités publiques ou des institutions, organes ou organismes de l'UE	Les déployeurs de SIA qui sont des autorités publiques ou des institutions, organes ou organismes de l'UE, respectent les obligations en matière d'enregistrement prévues à l'article 49. Si les déployeurs constatent que le SIA à risque élevé qu'ils envisagent d'utiliser n'a pas été enregistré dans la base de données de l'UE (voir art. 71), ils ne doivent pas utiliser ce système et informent le fournisseur ou le distributeur.
Analyse d'impact du SIA	Les déployeurs de SIA à risque élevé utilisent les informations fournies en application de l'article 13 pour se conformer à leur obligation de procéder à une analyse d'impact relative à la protection des données.
Identification biométrique à distance dans le cadre d'enquête	En cas d'enquête en vue de la recherche ciblée d'une personne soupçonnée d'avoir commis une infraction pénale ou condamnée pour avoir commis une infraction pénale, le déployeur d'un SIA à risque élevé destiné à l'identification biométrique à distance *a posteriori,* demande l'autorisation, *ex ante* ou sans retard injustifié et au plus tard dans les 48 heures, d'une autorité judiciaire ou administrative dont la décision est contraignante et soumise à un contrôle juridictionnel, pour l'utilisation de ce système, sauf lorsqu'il est utilisé pour l'identification initiale d'un suspect potentiel sur la base de faits objectifs et vérifiables directement liés à l'infraction.

Information des personnes soumises à l'utilisation de SIA à risque élevé	Les déployeurs de SIA à risque élevé visés à l'annexe III, qui prennent des décisions ou facilitent les prises de décision concernant les personnes physiques, les informent qu'elles sont soumises à l'utilisation du SIA à risque élevé.
Coopération avec les autorités compétentes	Les déployeurs doivent coopérer avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard du système d'IA à risque élevé.

Article 27

Analyse d'impact des SIA à risque élevé sur les droits fondamentaux	Les déployeurs qui sont des organismes de droit public ou des entités privées fournissant des services publics et les déployeurs de SIA à risque élevé visés à l'annexe III, points 5, b) et c), doivent analyser l'impact de ces SIA sur les droits fondamentaux que l'utilisation de ce système peut produire.

Article 50

Conformité aux autres directives UE	Les déployeurs d'un système de reconnaissance des émotions ou d'un système de catégorisation biométrique informent les personnes physiques qui y sont exposées du fonctionnement du système et traitent les données à caractère personnel conformément au règlement (UE) 2016/679, au règlement (UE) 2018/1725 et à la directive (UE) 2016/680, selon le cas.

FICHE 3

Obligations pour les mandataires des fournisseurs de systèmes d'IA à risque élevé

Selon l'article 22

Vérification de la déclaration UE de conformité et de la documentation technique	Vérifier que la déclaration UE de conformité et la documentation technique ont été établies et que le fournisseur a suivi une procédure appropriée d'évaluation de la conformité.
Mise à disposition de divers documents aux autorités compétentes, aux autorités ou organismes nationaux	Tenir à la disposition des autorités compétentes et des autorités ou organismes nationaux, pendant une période de dix ans après la mise sur le marché ou la mise en service du SIA à risque élevé, les coordonnées du fournisseur ayant désigné le mandataire, une copie de la déclaration UE de conformité, la documentation technique et, le cas échéant, le certificat délivré par l'organisme notifié.
Communication d'informations et de documents à la demande des autorités compétentes	Communiquer à l'autorité compétente, conformément à l'article 22§3, a), toutes les informations et tous les documents pour démontrer la conformité d'un SIA à risque élevé, et notamment lui donner accès aux journaux générés automatiquement par le système d'IA à risque élevé.

Coopération avec les autorités compétentes à l'égard du SIA à risque élevé	Coopérer avec les autorités compétentes à toute mesure prise par ces dernières à l'égard du SIA à risque élevé, en particulier pour réduire et atténuer les risques posés par celui-ci.
Respect des obligations en matière d'enregistrement	Respecter les obligations en matière d'enregistrement ou, si l'enregistrement est effectué par le fournisseur lui-même, vérifier que les informations sont correctes.
Fin du mandat	Mettre fin au mandat s'il considère ou a des raisons de considérer que le fournisseur agit de manière contraire aux obligations qui lui incombent.

FICHE 4

Obligations pour les importateurs de SIA à risque élevé

Selon l'article 23

Vérification de la conformité du SIA à risque élevé à l'*AI Act*	L'importateur doit vérifier que : 1) La procédure d'évaluation de la conformité a été effectuée par le fournisseur du SIA à risque élevé (voir art. 43) ; 2) Le fournisseur a établi la documentation technique (voir art. 11 et annexe IV) ; 3) Le SIA porte le marquage CE requis et est accompagné de la déclaration UE de conformité (voir art 47) et de la notice d'utilisation ; 4) Le fournisseur doit désigner par mandat écrit le mandataire (art 22 paragraphe 1).
Principe de précaution	Lorsqu'il existe un doute sur la conformité du SIA, s'il n'est pas conforme ou s'il a été falsifié ou s'il est accompagné de documents falsifiés, l'importateur ne peut mettre le SIA sur le marché qu'après sa mise en conformité. Lorsque le SIA présente un risque au sens de l'article 79§1, l'importateur en informe le fournisseur du SIA, les mandataires et les autorités de surveillance du marché.
Indication de son identité sur le SIA	L'identité, c'est-à-dire, le nom, la raison sociale ou la marque déposée, ainsi que l'adresse à laquelle ils peuvent être contactés doit être indiquée sur le SIA à risque élevé et sur son emballage ou dans la documentation l'accompagnant.
Conditions de stockage ou de transport	L'importateur doit vérifier, lorsque le SIA est sous sa responsabilité, que les conditions de stockage ou de transport ne compromettent pas la conformité de celui-ci.

Conservation d'une copie du certificat, de la notice d'utilisation et de la déclaration UE de conformité (selon le cas) délivrés par l'organisme notifié	Ces copies doivent être conservées pendant 10 ans après la mise sur le marché ou la mise en service du SIA à risque élevé.
Preuve de la conformité du SIA et coopération avec les autorités	Les importateurs doivent communiquer aux autorités compétentes toutes les informations et les documents nécessaires pour démontrer la conformité du SIA à risque élevé dans une langue aisément compréhensible par les autorités nationales compétentes.
Coopération avec les autorités compétentes concernées	Les importateurs doivent coopérer avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard d'un SIA à risque élevé que ces premiers ont mis sur le marché.

FICHE 5

Obligations pour les distributeurs de SIA à risque élevé

Selon l'article 24

Vérification des documents de conformité	Le distributeur doit vérifier la présence du marquage CE, de la copie de la déclaration UE de conformité (voir art. 47), de la notice d'utilisation et s'assurer du respect des obligations par le fournisseur et l'importateur de ce système.
Principe de précaution	Lorsqu'il existe un doute sur la conformité du SIA, le distributeur ne peut mettre le SIA sur le marché qu'après sa mise en conformité.
Conditions de stockage ou de transport	L'importateur doit vérifier, lorsque le SIA est sous sa responsabilité, que les conditions de stockage ou de transport ne compromettent pas la conformité de celui-ci.
Devoir de correction et devoir d'information	Le distributeur qui considère le système comme non conforme doit prendre des mesures correctives, retirer le SIA ou le rappeler, ou veiller à ce que le fournisseur ou l'importateur du SIA ou tout autre opérateur concerné prenne des mesures correctives. Lorsque le SIA présente un risque au titre de l'article 79§1, le distributeur doit informer le fournisseur ou l'importateur du SIA ainsi que les autorités compétentes.
Preuve de la conformité du SIA	Les distributeurs du SIA à risque élevé doivent communiquer à l'autorité compétente toutes les informations et tous les documents nécessaires pour démontrer la conformité de ce SIA.
Coopération avec les autorités	Les distributeurs doivent coopérer avec les autorités compétentes.

FICHE 6

Obligations pour les fournisseurs de SIA à risque spécifique en matière de transparence

Selon l'article 50

Obligations de transparence	Ces obligations se traduisent par diverses injonctions : • Pour les SIA destinés à interagir directement avec des personnes physiques : les fournisseurs veillent à ce que ces SIA soient conçus et développés de manière à ce que les personnes physiques concernées soient informées qu'elles interagissent avec un système d'IA, sauf si cela ressort clairement compte tenu des circonstances et du contexte d'utilisation ; • Pour les SIA destinés à générer du contenu de synthèse (audio, image, vidéo ou texte) : les fournisseurs veillent à ce que les sorties des systèmes d'IA soient marquées dans un format lisible par machine et identifiables comme ayant été générées ou manipulées par une IA ; • Pour les SIA destinés à générer du contenu : les fournisseurs veillent à ce que leurs solutions techniques soient aussi efficaces, interopérables, solides et fiables que la technologie le permet (sauf si le SIA n'a qu'une fonction d'assistance pour la mise en forme ou ne modifie pas de manière substantielle les données d'entrée fournies par le déployeur ou leur sémantique, ou lorsque leur utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière) ; • Les informations qui doivent être indiquées doivent l'être de manière claire et reconnaissable au plus tard au moment de la première interaction ou de la première exposition ; • Des codes de bonnes pratiques relatifs à la détection et à l'étiquetage des contenus générés ou manipulés par une IA pourront être adoptés.

FICHE 7

Obligations pour les déployeurs de SIA à risque spécifique soumis à des obligations de transparence

Selon l'article 50

Obligations de transparence	Ces obligations se traduisent par diverses injonctions : • Pour les SIA de reconnaissance des émotions ou qui comportent un système de catégorisation biométrique : les déployeurs doivent informer les personnes qui y sont exposées. • Pour les SIA qui génèrent ou manipulent du contenu constituant un *deepfake* (hypertrucage en français) : le déployeur doit indiquer que ce contenu a été généré ou manipulé par une IA. Lorsque le contenu fait partie d'une œuvre ou d'un programme manifestement artistique, créatif, satirique, fictif ou analogue, les obligations de transparence énoncées au présent paragraphe se limitent à la divulgation de l'existence de tels contenus générés ou manipulés d'une manière appropriée qui n'entrave pas l'affichage ou la jouissance de l'œuvre. • Pour les SIA qui génèrent ou manipulent des textes publiés dans le but d'informer le public sur des questions d'intérêt public : les déployeurs indiquent que le texte a été généré ou manipulé par une IA sauf si le contenu généré par l'IA a fait l'objet d'un processus d'examen humain ou de contrôle éditorial ou lorsqu'une personne physique ou morale assume la responsabilité éditoriale de la publication du contenu. • Ces informations doivent être indiquées de manière claire et reconnaissable au plus tard au moment de la première interaction ou de la première exposition. • Des codes de bonnes pratiques relatifs à la détection et à l'étiquetage des contenus générés ou manipulés par une IA pourront être adoptés.

FICHE 8

SIA à risque minime : code de bonnes pratiques pour tous les opérateurs

L'*AI Act* établit plusieurs outils pour encadrer le développement et l'utilisation des SIA. Parmi les outils prévus, il convient de distinguer les **codes de bonnes pratiques** et les **codes de conduite** (pour l'application volontaire de certaines exigences), qui sont deux mécanismes distincts :

- Les codes de bonnes pratiques (voir art. 56) :

Le Bureau de l'IA et le Comité IA s'efforcent de veiller à ce que les codes de bonnes pratiques couvrent au moins les obligations prévues aux articles 53 (relatif aux « *obligations incombant aux fournisseurs de modèles d'IA à usage général* ») et 55 (relatif aux « *obligations incombant aux fournisseurs de modèles d'IA à usage général présentant un risque systémique* »). Ces codes doivent notamment inclure les questions suivantes :

- Les moyens de s'assurer que les informations (visées à l'article 53§1, points a) et b)) sont mises à jour à la lumière des évolutions du marché et des technologies ;
- Le niveau approprié de détail pour le résumé du contenu utilisé pour l'entraînement ;
- L'identification du type et de la nature des risques systémiques au niveau de l'UE, y compris leurs origines, le cas échéant ;
- Les mesures, procédures et modalités d'évaluation et de gestion des risques systémiques au niveau de l'UE, y compris la documentation y afférent, qui sont proportionnées aux risques, prennent en considération leur gravité et leur probabilité, et tiennent compte des défis spécifiques que pose la maîtrise de ces risques à la lumière des différentes façons dont ils peuvent apparaître ou se concrétiser tout au long de la chaîne de valeur de l'IA.

À noter que la Commission peut, au moyen d'un acte d'exécution, approuver un code de bonnes pratiques et lui conférer une validité générale au sein de l'UE.

Les codes de bonnes pratiques seront prêts au plus tard **le 2 mai 2025**. Si, à la date du 2 août 2025, un code de bonnes pratiques n'a pas pu être mis au point, ou si le Bureau de l'IA estime qu'il n'est pas approprié, la Commission peut prévoir, au moyen d'actes d'exécution, des règles communes pour la mise en œuvre des obligations prévues aux articles 53 et 55.

- Les codes de conduite (voir art. 95) :

Le Bureau de l'IA et les États membres encouragent et facilitent l'élaboration de codes de conduite pour favoriser leur application volontaire aux SIA autres que les SIA à risque élevé, en tenant compte des solutions techniques disponibles et des bonnes pratiques du secteur.

Le Bureau de l'IA et les États membres facilitent l'élaboration de codes de conduite concernant l'application volontaire, y compris par les déployeurs, d'exigences spécifiques à tous les SIA, sur la base d'objectifs clairs et d'indicateurs de performance clés permettant de mesurer la réalisation de ces objectifs, y compris des éléments tels que mais sans s'y limiter :

- Les éléments applicables prévus dans les lignes directrices de l'UE en matière d'éthique pour une IA digne de confiance ;
- L'évaluation et la réduction au minimum de l'incidence des SIA sur la durabilité environnementale, y compris en ce qui concerne la programmation économe en énergie et les techniques pour la conception, l'entraînement et l'utilisation efficace de l'IA ;
- La promotion de la maîtrise de l'IA, en particulier chez les personnes chargées du développement, du fonctionnement et de l'utilisation de l'IA ;
- La facilitation d'une conception inclusive et diversifiée des systèmes d'IA, notamment par la mise en place d'équipes de développement inclusives et diversifiées et la promotion de la participation des parties prenantes à ce processus ;
- L'évaluation et la prévention de l'impact négatif des systèmes d'IA sur les personnes ou groupes de personnes vulnérables, y compris en ce qui concerne l'accessibilité pour les personnes handicapées, ainsi que sur l'égalité de genre.

Ces codes de bonne conduite peuvent être élaborés par des fournisseurs ou déployeurs individuels de SIA ou par des organisations les représentant ou par les deux, y compris avec la participation de toute partie intéressée, et de leurs organisations représentatives, y compris des organisations de la société civile et du monde universitaire. Les codes de bonne conduite peuvent porter sur un ou plusieurs SIA, compte tenu de la destination des systèmes concernés.

Au plus tard le 2 août 2028 et tous les trois ans par la suite, la Commission évalue l'impact et l'efficacité des codes de conduite volontaires destinés à favoriser l'application des exigences énoncées au chapitre III, section 2, pour les systèmes d'IA autres que les systèmes d'IA à risque élevé, et fixe éventuellement d'autres exigences supplémentaires pour les systèmes d'IA autres que les systèmes d'IA à risque élevé, y compris en ce qui concerne la durabilité environnementale (article 112§7).

FICHE 9

Tableau récapitulatif des obligations de l'*AI Act* selon les risques et les opérateurs concernés

	Risque inacceptable	Risque élevé	Risque spécifique en matière de transparence	Risque minime
Fournisseur	Interdiction	**Article 16** • Veiller au respect des exigences • Indiquer son identité sur le SIA • Mettre en place un système de gestion de la qualité • Assurer la conservation de la documentation • Assurer la tenue des journaux automatiques lorsqu'ils sont sous son contrôle • Soumettre le SIA à la procédure d'évaluation de la conformité avant sa mise sur le marché ou sa mise en service • Élaborer une déclaration UE de conformité • Apposer un marquage CE • Respecter les obligations en matière d'enregistrement • Prendre des mesures correctives et fournir des informations • Prouver la conformité du SIA à la demande d'une autorité nationale • Veiller à la conformité du SIA à risque élevé aux directives (UE) 2016/2102 et 2019/882	**Article 50** Obligations de transparence	Application de codes de conduite

Déployeur	Interdiction	**Article 22 : pour les fournisseurs établis à l'étranger** • Désigner un mandataire, par mandat écrit, établi dans l'Union **Article 26** • Mettre en place les mesures techniques et organisationnelles • Effectuer un contrôle humain • Vérifier les données d'entrée • Assurer le devoir d'alerte • Tenir des journaux générés automatiquement • Informer les salariés et leurs représentants • Respecter les obligations en matière d'enregistrement • Analyser l'impact du SIA sur les droits fondamentaux • Cas spécifique lié à l'identification à distance dans le cadre d'enquêtes • Informer les personnes soumises à l'utilisation de SIA à risque élevé • Coopérer avec les autorités compétentes concernées **Article 27** • Effectuer une analyse d'impact des SIA à risque élevé sur les droits fondamentaux **Article 50** • Conformité aux autres directives UE	**Article 50** Obligations de transparence	Application de codes de conduite
Mandataire	Interdiction	**Article 22** • Vérifier l'établissement de la déclaration UE de conformité et la documentation technique et que le fournisseur a suivi une procédure appropriée d'évaluation de la conformité	Aucune obligation	Application de codes de conduite

		• Tenir à la disposition des autorités compétentes et organismes nationaux, pendant une période de dix ans après la mise sur le marché ou la mise en service du SIA à risque élevé, les coordonnées du fournisseur, une copie de la déclaration UE de conformité, la documentation technique et le certificat • Communiquer les documents nécessaires pour prouver la conformité sur demande • Coopérer avec les autorités compétentes pour réduire et atténuer les risques posés par le SIA à risque élevé • Respecter les obligations d'enregistrement ou vérifier les informations enregistrées par le fournisseur		
Importateur	Interdiction	**Article 23** • Vérifier la conformité du système d'IA à l'*AI Act* • Lorsqu'il existe des raisons suffisantes de considérer qu'un SIA à risque élevé n'est pas conforme à l'*AI Act* ou qu'il a été falsifié ou qu'il est accompagné de documents falsifiés, ne mettre le SIA sur le marché qu'après sa mise en conformité • Indiquer son identité sur le SIA et sur l'emballage ou dans la documentation l'accompagnant • Vérifier, lorsque le SIA est sous sa responsabilité, que les conditions de stockage ou de transport ne compromettent pas la conformité du SIA • Conserver une copie du certificat délivré par l'organisme notifié pendant une période de dix ans après la mise sur le marché ou la mise en service du SIA à risque élevé • Prouver la conformité du SIA • Coopérer avec les autorités compétentes concernées	Aucune obligation	Application de codes de conduite

Distributeur	Interdiction	**Article 24** • Vérifier les documents attestant de la conformité du SIA à risque élevé • Lorsqu'il existe un doute sur la conformité du SIA à risque élevé, ne mettre le SIA à disposition du marché qu'après sa mise en conformité • Vérifier, lorsque le SIA est sous sa responsabilité, que les conditions de stockage ou de transport ne compromettent pas la conformité du SIA • Prendre des mesures correctives et informer le fournisseur ou l'importateur du SIA et les autorités compétentes • Prouver la conformité du SIA et coopérer avec les autorités • Coopérer avec les autorités compétentes concernées	Aucune obligation	Application de codes de conduite

1.1.3 Les modèles d'IA à usage général

Dans un premier temps, il est nécessaire d'identifier s'il s'agit d'un modèle à usage général **à risque systémique** ou d'un modèle à usage général **sans risque systémique** (1). Il faut ensuite prendre connaissances des obligations correspondantes (2). Cette classification se justifie par les incidences significatives que ces modèles peuvent avoir sur le marché de l'UE, notamment en raison de leur portée ou des effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûreté publique et les droits fondamentaux, ou la société dans son ensemble.

1.1.3.1 Distinction entre un modèle d'IA à usage général à risque systémique et un modèle d'IA à usage général sans risque systémique

L'*AI Act* distingue, en particulier dans son chapitre V, deux types de modèles d'IA à usage général : les modèles d'IA à usage général et les modèles d'IA à usage général présentant un risque systémique.

- Les modèles d'IA à usage général **à risque systémique** :

L'article 3§65 de l'***AI Act*** définit le risque systémique comme « *un risque spécifique aux capacités à fort impact des modèles d'IA à usage général, ayant une incidence significative sur le marché de l'Union en raison de leur portée ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûreté, la sécurité publique, les droits fondamentaux ou la société dans son ensemble, pouvant être propagé à grande échelle tout au long de la chaîne de valeur* ».

Un modèle à usage général est dit **à risque systémique** dans ces deux cas (voir art. 51) :

- S'il dispose de capacités à fort impact évaluées sur la base de méthodologies et d'outils techniques appropriés, y compris des indicateurs et des critères de référence ;
- S'il est désigné comme tel par une décision de la Commission, d'office ou à la suite d'une alerte qualifiée du groupe scientifique.

À noter que l'*AI Act* pose une présomption : un modèle d'IA à usage général est présumé avoir des capacités à fort impact lorsque la quantité cumulée de calcul, autrement dit la puissance de calcul, utilisée pour son entraînement est supérieure à 10^{25} FLOPS - *Floating-Point Operations per Second* -

en français nombre d'opérations en virgule flottante par seconde. Le FLOPS est une unité de mesure de la rapidité de calcul d'un système informatique et donc d'une partie de sa performance, mesurée en opérations en virgule flottante par seconde.

- Les modèles d'IA à usage général **sans risque systémique** :

L'article 3§63 de l'*AI Act* définit un modèle d'IA à usage général comme « *un modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval, à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché* ».

Un modèle d'IA à usage général est dit **sans risque systémique** dans ces deux cas **:**

- S'il ne répond à aucun des deux critères précédents ;
- S'il répond au critère de l'article 51§1, a) (c'est-à-dire « *s'il dispose de capacités à fort impact évaluées sur la base de méthodologies et d'outils techniques appropriés, y compris des indicateurs et des critères de référence* ») mais qu'il a été démontré que, exceptionnellement, bien qu'il remplisse ce critère, le modèle d'IA à usage général ne présente pas, en raison de ses caractéristiques spécifiques, de risque systémique et ne devrait donc pas être classé comme modèle d'IA à usage général présentant un risque systémique (Art 52 §2).

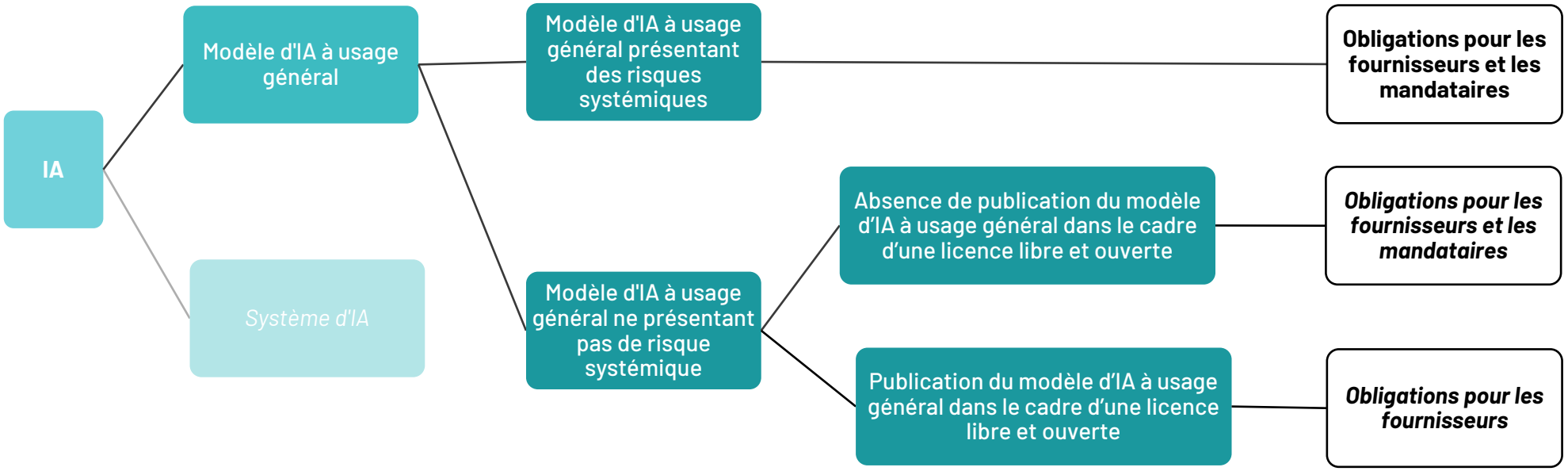

Figure 4: Arbre de décision des obligations pour les modèles d'IA à usage général

1.1.3.2 Obligations incombant aux fournisseurs et aux mandataires de modèles à usage général

L'*AI Act* ne définit pas ce qu'est une licence libre et ouverte. Cependant le considérant 102 ci-après, permet d'en comprendre le principe: « *Les logiciels et les données, y compris les modèles, publiés dans le cadre d'une* ***licence libre et ouverte*** *grâce à laquelle ils peuvent être partagés librement et qui permet aux utilisateurs de librement consulter, utiliser, modifier et redistribuer ces logiciels et données ou leurs versions modifiées, peuvent contribuer à la recherche et à l'innovation sur le marché et offrir d'importantes possibilités de croissance pour l'économie de l'Union. Les modèles d'IA à usage général diffusés sous licence libre et gratuite devraient être considérés comme garantissant des niveaux élevés de transparence et d'ouverture si leurs paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle sont mis à la disposition du public.* »

Type de modèle d'IA	Opérateur concerné	ABSENCE de publication dans le cadre d'une licence libre et ouverte	Publication dans le cadre d'une licence libre et ouverte
Modèle d'IA à usage général	Fournisseur	Conformément à l'article 53§1 de l'*AI Act* : • Élaborer et tenir à jour la documentation technique du modèle ; • Élaborer, tenir à jour et mettre à disposition des informations et de la documentation à l'intention des fournisseurs de SIA qui envisagent d'intégrer le modèle d'IA à usage général dans leurs SIA ; • Mettre en place une politique visant à se conformer au droit de l'Union en matière de droit d'auteur et droits voisins et notamment à identifier et à respecter, y compris au moyen de technologies de pointe, une réservation de droits exprimée conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790 ; • Élaborer et mettre à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner le modèle d'IA à usage général Conformément à l'article 54§1 de l'*AI Act*, avant de mettre un modèle d'IA à usage général sur le marché de l'UE, le fournisseur	Les obligations énoncées au paragraphe 1, points a) et b) ne s'appliquent pas aux fournisseurs de modèles d'IA qui sont publiés dans le cadre d'une licence libre et ouverte (article 53§2, *AI Act*). L'obligation de désigner par mandat écrit un mandataire établi dans l'UE ne s'applique pas aux fournisseurs de modèles d'IA à usage général qui sont publiés dans le cadre d'une licence libre et ouverte (article 54§6, *AI Act*).

		établi dans un pays tiers doit désigner, par mandat écrit, un mandataire établi dans l'UE.	
	Mandataire	<u>Conformément à l'article 54§3 de l'*AI Act* :</u> • Exécuter les tâches indiquées dans le mandat que lui a confié le fournisseur : o Vérifier que la documentation technique prévue à l'annexe XI a été rédigée et que toutes les obligations visées à l'article 53 et, le cas échéant, à l'article 55 ont été remplies par le fournisseur ; o Tenir à la disposition du Bureau de l'IA et des autorités nationales compétentes une copie de la documentation technique prévue à l'annexe XI, pendant une période de dix ans après la mise sur le marché du modèle d'IA à usage général et les coordonnées du fournisseur ayant désigné le mandataire ; o Communiquer au Bureau de l'IA, sur demande motivée de sa part, toutes les informations et tous les documents nécessaires pour démontrer qu'il respecte ses obligations ; o Coopérer avec le Bureau de l'IA et les autorités compétentes, sur demande motivée de leur part, à toute mesure qu'ils prennent à l'égard d'un modèle d'IA à usage général, y compris lorsque le modèle est intégré dans ces SIA mis sur le marché ou mis en service. <u>Conformément à l'article 54§5 de l'*AI Act*</u>, le mandataire met fin au mandat s'il considère ou a des raisons de considérer que le	En l'absence d'obligation pour le fournisseur de désigner un mandataire par mandat écrit, ce dernier n'est pas tenu aux obligations prévues à l'article 54§3 de l'*AI Act*.

		fournisseur agit de manière contraire aux obligations qui lui incombent.	
Modèle d'IA à usage général à risque systémique	Fournisseur	Conformément à l'article 52 de l'*AI Act* : Lorsqu'un modèle d'IA à usage général remplit la condition visée à l'article 51§ 1 point a) [c'est-à-dire qu'il dispose de capacités à fort impact évaluées sur la base de méthodologies et d'outils techniques appropriés, y compris des indicateurs et des critères de référence]: le fournisseur doit en informer la Commission sans tarder et, en tout état de cause, dans un délai de deux semaines après la date à laquelle ce critère est rempli ou après qu'il a été établi qu'il le sera. Cette notification doit comprendre les informations nécessaires pour démontrer que le critère pertinent a été rempli. En plus du respect des articles 53 et 54, les fournisseurs de modèles d'IA à usage général présentant un risque systémique doivent (article 55§1 de l'*AI Act*) : • Effectuer une évaluation des modèles sur la base de protocoles et d'outils normalisés reflétant l'état de la technique, y compris en réalisant et en documentant des essais contradictoires des modèles en vue d'identifier et d'atténuer les risques systémiques ; • Évaluer et atténuer les risques systémiques éventuels au niveau de l'UE, y compris leurs origines, qui peuvent découler du développement, de la mise sur le marché ou de l'utilisation de modèles d'IA à usage général présentant un risque systémique ; • Suivre, documenter et communiquer sans retard injustifié au Bureau de l'IA et, le cas échéant, aux autorités nationales compétentes les informations pertinentes concernant les incidents graves ainsi que les éventuelles mesures correctives pour y remédier ;	Conformément à l'article 52 de l'*AI Act* : Lorsqu'un modèle d'IA à usage général remplit la condition visée à l'article 51§ 1 point a) [c'est-à-dire qu'il dispose de capacités à fort impact évaluées sur la base de méthodologies et d'outils techniques appropriés, y compris des indicateurs et des critères de référence]: le fournisseur doit en informer la Commission sans tarder et, en tout état de cause, dans un délai de deux semaines après la date à laquelle ce critère est rempli ou après qu'il a été établi qu'il le sera. Cette notification doit comprendre les informations nécessaires pour démontrer que le critère pertinent a été rempli. Pour rappel, les fournisseurs de modèles d'IA à usage général présentant un risque systémique doivent également respecter les articles 53 et 54 de l'*AI Act*. Ainsi, l'obligation de désigner par mandat écrit un mandataire établi dans l'UE ne s'applique pas aux fournisseurs de modèles d'IA à usage général qui sont publiés dans le cadre

		• Garantir un niveau approprié de protection en matière de cybersécurité pour le modèle d'IA à usage général présentant un risque systémique et l'infrastructure physique du modèle.	d'une licence libre et ouverte (article 54§6, *AI Act*).
	Mandataire	Pour rappel, les fournisseurs de modèles d'IA à usage général présentant un risque systémique doivent également respecter les articles 53 et 54 de l'*AI Act*. <u>Conformément à l'article 54§3 de l'*AI Act*</u> : • Exécuter les tâches indiquer dans le mandat que lui a confié le fournisseur : o Vérifier que la documentation technique prévue à l'annexe XI a été rédigée et que toutes les obligations visées à l'article 53 et, le cas échéant, à l'article 55 ont été remplies par le fournisseur ; o Tenir à la disposition du Bureau de l'IA et des autorités nationales compétentes une copie de la documentation technique prévue à l'annexe XI, pendant une période de dix ans après la mise sur le marché du modèle d'IA à usage général et les coordonnées du fournisseur ayant désigné le mandataire ; o Communiquer au Bureau de l'IA, sur demande motivée de sa part, toutes les informations et tous les documents nécessaires pour démontrer qu'il respecte ses obligations ; o Coopérer avec le Bureau de l'IA et les autorités compétentes, sur demande motivée de leur part, à toute mesure qu'ils prennent à l'égard d'un modèle d'IA à usage général, y compris lorsque	Pour rappel, les fournisseurs de modèles d'IA à usage général présentant un risque systémique doivent également respecter les articles 53 et 54 de l'*AI Act*. Ainsi, en l'absence d'obligation pour le fournisseur de désigner un mandataire par mandat écrit, ce dernier n'est pas tenu aux obligations prévues à l'article 54§3 de l'*AI Act*.

		le modèle est intégré dans ces SIA mis sur le marché ou mis en service. Conformément à l'article 54§5 de l'*AI Act*, le mandataire met fin au mandat s'il considère ou a des raisons de considérer que le fournisseur agit de manière contraire aux obligations qui lui incombent.	

En résumé, le **mandataire** devient l'**interlocuteur privilégié des autorités** compétentes pour les fournisseurs non établis dans l'UE, garantissant que ces derniers respectent bien les obligations du règlement.

Conclusion

Cette « cartographie des obligations applicables aux organisations » est accompagnée d'un recueil de notes thématiques conçu pour fournir une vision claire et concise des principaux enjeux juridiques liés à l'*AI Act*. Chacune de ces notes souligne des points d'attention spécifiques à avoir sur différents thèmes : le risque cyber, la protection des données, la propriété intellectuelle et le secret des affaires. Ce document « cartographie » est voué à être mis à jour au fur et à mesure des précisions des textes d'application apportées à l'*AI Act*. Par ailleurs, la gouvernance au niveau national va bientôt être définie et les codes de conduites, actuellement en cours de rédaction, devraient être publiés en mai 2025. Le Cigref et Numeum prévoient de partager avec la Commission européenne et la Direction Générale des Entreprises, les difficultés rencontrées par leurs membres, et de proposer des solutions pour les résoudre. Nous souhaitons ainsi répondre aux enjeux de l'*AI Act* de manière efficace et sans excès.

Pour rappel, ce guide est composé de plusieurs parties, indépendantes et complémentaires :

Points clés de l'*AI Act* - Introduction

Partie 1 - Obligations

- Cartographie des obligations applicables aux organisations selon l'*AI Act*, en fonction de la nature de l'IA, de son niveau de risque, et de la place de l'organisation dans la chaîne de valeur
- Recueil de notes thématiques sur les principaux enjeux juridiques

Partie 2 - Gouvernance

- Mode d'emploi et outils pour mettre en place une gouvernance

Partie 3 - Contrat et responsabilités

- Identification des responsabilités et mise en place des contrats adéquats

Une **annexe** permettra de lister des recommandations et mesures à mettre en place, de traduire opérationnellement les obligations légales, et enfin de présenter quelques cas pratiques pour faciliter la compréhension.

Remerciements

Le Cigref et Numeum souhaitent remercier chaleureusement les pilotes du groupe de travail « Mise en œuvre de l'*AI Act* », côté Cigref, **Lionel Chaine**, DSI de BPI France et **Jean-Claude Laroche**, Directeur de Mission auprès de la Présidence du COE France d'EDF, côté Numeum, **Katya Lainé**, CEO de TALKR.ai et **Thibault de Tersant**, *Senior executive Vice President* de Dassault Système.

Nous remercions également les différents participants, membres de nos deux associations, qui ont contribué à l'élaboration des livrets de ce guide.

Nous avons eu le plaisir d'être accompagnés tout au long de notre démarche par l'expertise de quatre grands cabinets d'avocats : August Debouzy, DLA Piper, Racine et Bird & Bird. Nous remercions plus particulièrement **Mahasti Razavi**, managing partner chez August Debouzy, **Anne-Sophie Lampe**, IT/IP Partner chez Bird & Bird, **Jeanne Dauzier** Partner et **Maria Aouad**, avocate chez DLA Piper et **Charles Bouffier**, avocat associé, et **Naomi Meynle-Hamza**, juriste doctorante, chez Racine.

Rédaction :
Marine de Sury, Directrice de mission, Cigref
Anissa Kemiche, Déléguée aux affaires européennes, Numeum

Relecture : Chantal de Bardies, Directrice de la qualité des contenus, Cigref

Direction artistique et graphisme :
Emilie Grange, Chargée de communication, Cigref
Laura Pineau, Chargée du digital et du graphisme, Numeum

Cigref
RÉUSSIR
LE NUMÉRIQUE

numeum
Engager
le numérique