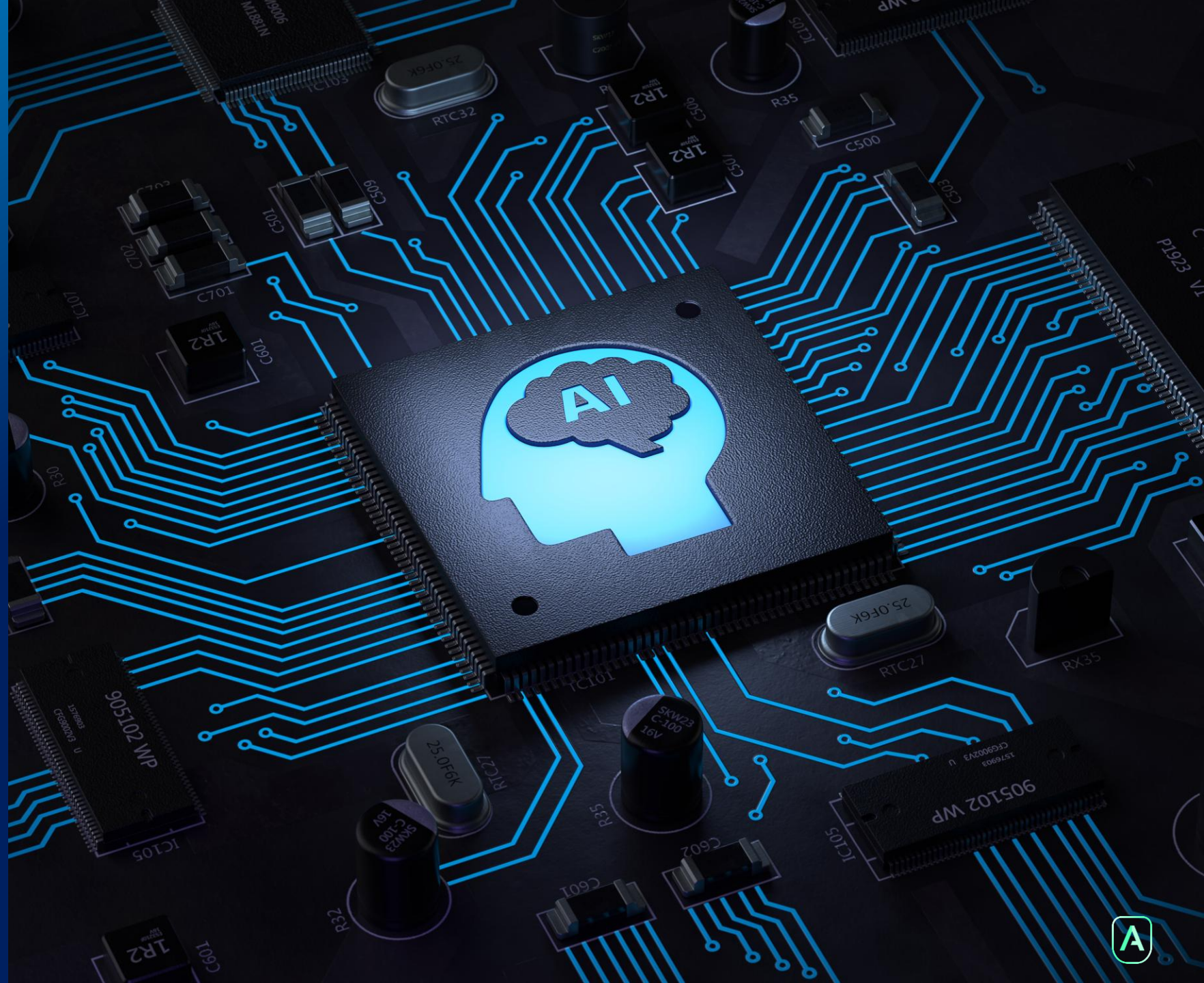
ADEQUACY

Du RGPD à l'AI ACT

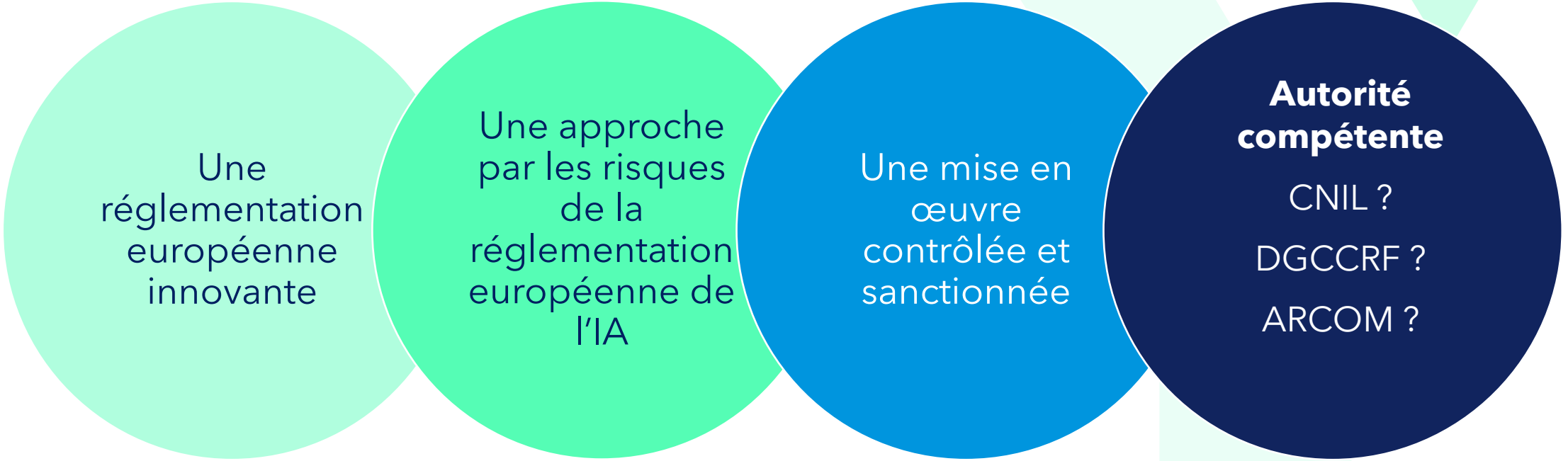
Comprendre la logique de mise en conformité pour rester dans le « Game »

AI ACT
Le contexte



Qu’est-ce que l’AI Act?

Un règlement qui vise à créer un cadre global de confiance ayant pour objectif le développement et le déploiement d’une IA respectueuse de valeurs essentielles.



Champs d'application de l'AI Act

Champ d'application matériel

- Chatbots (comme ChatGPT)
- Systèmes de reconnaissance faciale
- IA pour la notation de crédit
- Systèmes de recrutement automatisé
- Voitures autonomes

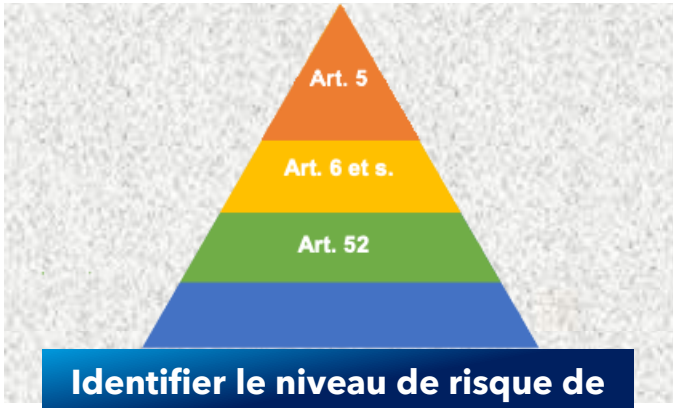
Champ d'application territorial

- À **toute entreprise qui met sur le marché ou utilise** un système d'IA **dans l'UE**
- Aux **fournisseurs et déployeurs** d'IA dans l'Union européenne.
- Aux **importateurs, distributeurs, utilisateurs** professionnels.
- Les autorités publiques utilisant ou développant de l'IA

Exclusions

- Aux systèmes utilisés à des fins militaires ou de défense.
- Aux recherches non mises sur le marché (si elles ne sont pas encore utilisées ou proposées).
- Aux activités strictement personnelles ou domestiques.

Les principales obligations



Identifier le niveau de risque de chaque système d'IA

Le rôle de votre organisation

Assurer les obligations en fonction du rôle et du niveau de risque

Des sanctions financières GRADUELLES ...

Fourniture d'informations incorrectes, incomplètes ou trompeuses aux organismes notifiés et aux autorités nationales compétentes

7,5 millions d'euros

OU

1,5% du CA annuel mondiale

Amende pour le non-respect des exigences ou des obligations concernant les Systèmes d'IA à haut risque

15 millions d'euros

OU

3% du CA annuel mondiale

PLAFOND des amendes administratives prévues par le règlement

35 millions d'euros

OU

7% du CA annuel mondiale

Calendrier de l'AI Act

Se positionner en tant qu'acteur responsable et innovant

1er Aout 2024	2 Février 2025	Mai 2025	2 Août 2025	Août 2026	Août 2027
Entrée en vigueur de l'AI Act	Interdiction de certains systèmes d'IA (SIA) sur le marché européen	Publication des codes de pratique pour les systèmes d'IA à usage général (GPAI)	Application des exigences relatives aux systèmes d'IA à usage général (GPAI)	Application des exigences pour les systèmes d'IA à haut risque de l'annexe III et les SIA de l'Article 50	Application des règles pour les risques élevés de l'annexe NLF Jouets, Radio, Equipements, Dispositifs médicaux de diagnostic
			Sanctions applicables aux systèmes d'IA à risque inacceptable	Sanctions applicables à ces SIA (annexe III + Article 50)	
			Nomination des autorités nationales compétentes	Application des regles de transparence	

01 Mettre en conformité le SIA au RGPD

Déterminer le régime juridique applicable

RGPD

Directive Police-Justice

Défense nationale

Evaluer la compatibilité de la finalité ultérieure

Existence d'un lien entre les finalités initiales et finalités envisagés.

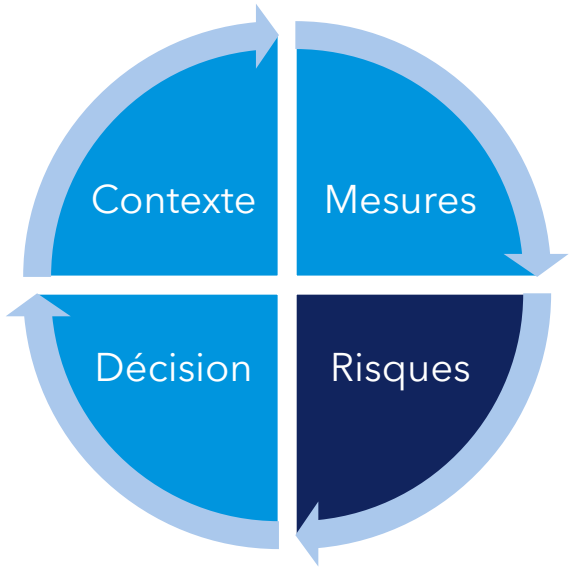
Contexte & Base juridique

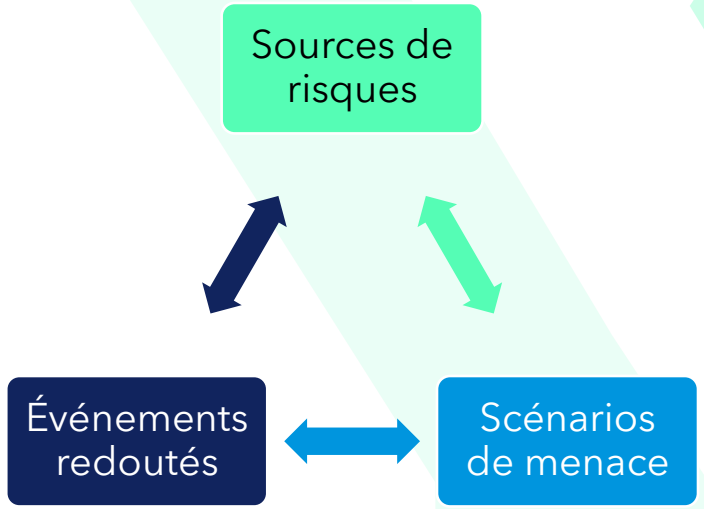
La nature des données

Les conséquences possibles du traitement ultérieur

L'existence de garanties appropriées

Analyse d'Impact relative à la Protection des Données





Prendre en compte les scénarios adaptés

- Attaque par manipulation
- Attaque par infection
  - Attaque par empoisonnement
  - Attaqué par porte dérobée
- Attaque par exfiltration
  - Attaques par inférence d'appartenance
  - Attaque par inversion de modèle

02 Identifier le niveau de risque de chaque système d'IA

Risque inacceptable

Pour les IA qui ne respectent aux valeurs de l'UE et portent atteinte aux droits fondamentaux

Interdiction

Exemples :

Techniques subliminales, manipulatrices ou trompeuses, exploitation de vulnérabilités avec pour objectif d’altérer le comportement susceptible de causer un préjudice important sur une personne ou à un tiers, prédiction du risque d'infraction pénale sur la base du profilage, bases de données de reconnaissance faciale provenant d'internet ou de la vidéosurveillance…

Risque élevé

Pour les IA qui peuvent avoir une incidence négative sur la sécurité des personnes ou sur leurs droits fondamentaux et qui répondent à l'une des deux hypothèses visées à l'article 6.1 et 6.2

Paquet d'obligations pour tous les opérateurs

Exemples :

Systèmes de scoring social : bancaire, tri de CV, identifications biométriques, manipulation de contenu, système de navigation dans les transports, IA de chirurgie…

Risque en matière de transparence

Pour les IA qui interagissent avec des personnes physiques et qui ne sont ni à risque acceptable, ni à risque élevé. Il faut indiquer aux utilisateurs qu'ils interagissent avec une machine et/ou indiquer que certains contenus sont générés par l'IA

Obligations de transparence

Ex: Techniques de synthèse multimédia reposant sur l'intelligence artificielle (deepfakes), ou les chatbots…

Risque minime

Pour les IA qui peuvent être développés et utilisés à condition de respecter la législation en vigueur et qui ne sont soumis à aucune obligation supplémentaire au titre de l'AI Act

Adoption volontaire de codes de conduite supplémentaires

Ex: Tous les autres systèmes d'IA n’entrant pas dans les autres catégories (applications de jeux utilisant des systèmes d’IA, filtres anti-spam)…

03 Rôle et Obligations

Le rôle de votre organisation

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.

Obligations pour les SIA selon le rôle et le niveau de risque

	Fournisseur	Déployeur	Mandataire	Importateur	Distributeur
Risque inacceptable	Interdiction	Interdiction	Interdiction	Interdiction	Interdiction
Risque élevé	Obligations pour les fournisseurs d'IA à risque élevé	Obligations pour les déployeurs d'IA à risque élevé	Obligations pour les mandataires d'IA à risque élevé	Obligations pour les importateurs d'IA à risque élevé	Obligations pour les distributeurs d'IA à risque élevé
Risque spécifique en matière de transparence	Obligations pour les fournisseurs d'IA à risque spécifique en matière de transparence	Obligations pour les déployeurs d'IA à risque spécifique en matière de transparence	Aucune obligation	Aucune obligation	Aucune obligation
Risque minime	Adoption volontaire de codes de conduite supplémentaires	Adoption volontaire de codes de conduite supplémentaires	Adoption volontaire de codes de conduite supplémentaires	Adoption volontaire de codes de conduite supplémentaires	Adoption volontaire de codes de conduite supplémentaires

Obligations pour les modèles selon le rôle et le niveau de risque

	Fournisseur UE		Fournisseur Hors-UE		Mandataire	
	Licence ouverte	**Licence propriétaire**	**Licence ouverte**	**Licence propriétaire**	**Licence ouverte**	**Licence propriétaire**
Modèle à usage général avec risques systémiques	Article 52 Article 53 Article 55		Article 52 Article 53 Article 54 Article 55		Article 54.3 Article 54.4 Article 54.5	
Modèle à usage général sans risque systémique	Aucune Obligation	Article 53	Aucune Obligation	Article 53 Article 54	Article 54.3	

Capitaliser sur des attendus communs

Pour l'AI Act	Pour le RGPD
La mise en conformité des SIA nécessite d'avoir une vision sur **la cartographie applicative**	**Vous avez déjà recensé les supports**
La mise en conformité des modèles d'IA nécessite de recenser **les jeux de données utilisés** pour l'entrainement	**L'ensemble des jeux de données contenant des données personnelles sont des traitements**
L'usage de données personnelles au sein d'un SIA nécessite un cadrage RGPD	**Les évaluations de compatibilité des finalités initiales et des finalités ultérieurs seront assurez coté « Privacy »**
Les « Fondamental Right Impact Assessment » sont une démarche qui sera très proches des AIPD	**Vous avez déjà réalisé des AIPD**
La documentation technique nécessite de recenser l'ensemble des garanties en termes de **sécurité**	**Les mesures de sécurité** sont déjà recensées en fonction **des supports et des politiques pour les AIPD**

A1 Le détail des obligations en fonction des rôles

Obligations pour les SIA selon le rôle et le niveau de risque

	Risque inacceptable	Risque élevé	Risque en matière de transparence	Risque minime
Fournisseur	Interdiction	**Article 16** • 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 • 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

Obligations pour les SIA selon le rôle et le niveau de risque

	Risque inacceptable	Risque élevé	Risque en matière de transparence	Risque minime
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

Obligations pour les SIA selon le rôle et le niveau de risque

	Risque inacceptable	Risque élevé	Risque en matière de transparence	Risque minime
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 • 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	Aucune obligation	Application de codes de conduite

Obligations pour les SIA selon le rôle et le niveau de risque

	Risque inacceptable	Risque élevé	Risque en matière de transparence	Risque minime
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

Obligations pour les SIA selon le rôle et le niveau de risque

	Risque inacceptable	Risque élevé	Risque en matière de transparence	Risque minime
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

ADEQUACY

6 rue d'Antin
75002, Paris

41 quai Fulchiron
69005, Lyon

Tél : +33 (0) 1 55 35 36 36
Mail : contact@infhotep.com