DOCUMENTATION TECHNIQUE DU SYSTÈME D'IA

DÉFINITION

Conformément à l'Article 11 et à l'Annexe IV du RIA, les fournisseurs de systèmes d'IA à **Haut Risque** doivent établir une **documentation technique avant la mise sur le marché ou la mise en service** du système. Le déployeur doit, quant à lui, vérifier que le fournisseur a bien mis en place la documentation technique. Cette documentation doit être tenue à jour de manière continue. Les exigences relatives aux informations minimales à inclure dans le document figurent à l'Annexe IV. Toutefois, si nécessaire, ces exigences peuvent être modifiées par des actes délégués de la Commission européenne (Art. 97) en fonction des évolutions technologiques.

1. Description générale du système d'IA

- ❑ **Destination et informations d'identification** : Comprend l'objectif visé, le nom du fournisseur, la version du système et son lien avec les versions précédentes.
- ❑ **Compatibilité** : Explication de la manière dont le système interagit avec d'autres matériels ou logiciels, y compris d'autres systèmes d'IA.
- ❑ **Formats disponibles** : Description des différentes formes sous lesquelles le système est proposé, comme les logiciels téléchargeables ou les API.

2. Aspects techniques et développement

- ❑ **Processus de développement** : Méthodes utilisées, incluant l'intégration de systèmes préexistants/pré-entraînés ou d'outils tiers.
- ❑ **Conception et logique** : Spécifications des algorithmes, objectifs d'optimisation et choix techniques effectués pour respecter les exigences réglementaires.
- ❑ **Architecture** : Organisation des composants logiciels et ressources informatiques utilisées pour l'entraînement et la validation.
- ❑ **Stress-Test et Cyber** : Liste des techniques visant à assurer la robustesse, la résilience et la cybersécurité des systèmes (Art. 15 – voir focus).

Focus *Article 15 - Exactitude, robustesse et cybersécurité*

Cet article exige que les SIA à haut risque soient déployés avec des niveaux d'exactitude, de robustesse et de cybersécurité appropriés et alignés sur leurs risques. Voici une liste des principaux éléments requis par cet article :

- *Élaborer un système, résilient face aux erreurs, aux défaillances ou aux incohérences, visant à atteindre un niveau approprié de précision, de robustesse et de cybersécurité, en s'appuyant sur des critères de référence et des méthodes de mesure appropriés.*
- *Pour les systèmes qui continuent à apprendre tout au long de leur cycle de vie, accorder une attention particulière à la dégradation de la performance et l'apparition potentielle des biais.*
- *Assurer que le système soit résistant aux tentatives de modification de son utilisation, de ses résultats ou de ses performances par des tiers non autorisés et malveillants qui tentent d'exploiter les faiblesses du système.*
- *Documenter les mesures visant à remédier aux vulnérabilités propres à l'IA qui comprennent, le cas échéant, des mesures de prévention, de détection, de réponse, de résolution et de contrôle de l'empoisonnement des données et des modèles, des attaques adverses et de l'évasion de modèle.*

Ces informations doivent figurer dans la documentation technique. Néanmoins, le niveau de détail de ces éléments n'a pas été spécifié, laissant la porte ouverte à l'interprétation dans l'attente d'éventuelles clarifications fournies par les normes harmonisées (à date prévues pour S2 2026) .

DOCUMENTATION TECHNIQUE DU SYSTÈME D'IA

DÉFINITION

3. Données et gestion (Art. 10)

- ❑ **Bases de données** : Informations et exigences relatives aux données d'entraînement, validation et d'essai, avec description de leur provenance, caractéristiques principales et méthode de sélection.
- ❑ **Collecte/Traitement des données** : Fiches techniques détaillant les méthodes utilisées pour collecter et traiter les données.

4. Compatibilité et interface utilisateur (production)

- ❑ **Matériel supporté** : Description des équipements sur lesquels le système d'IA peut fonctionner.
- ❑ **Interface utilisateur** : Présentation des fonctionnalités mises à disposition des utilisateurs finaux, avec des guides d'utilisation pour les déployeurs.
- ❑ **Contrôle humain** : Évaluation des mesures de contrôle humain nécessaires (Art. 14).

5. Conformité et mise à jour

- ❑ **Déclaration de conformité** : Copie de la déclaration UE de conformité (Art.47).
- ❑ **Gestion des risques** : Description détaillée du système de gestion des risques (Art. 9).
- ❑ **Mises à jour** : Exigences relatives aux versions logicielles et aux micrologiciels, y compris les besoins en mises à jour.
- ❑ **Références** : Liste des normes harmonisées appliquées, en cas d'absence description détaillée des solutions adoptées pour satisfaire aux exigences relatives aux SIA à haut risque, avec des références à d'autres normes ou références techniques utilisées.
- ❑ **Photographies et illustrations** : Documentation visuelle pour identifier les caractéristiques externes et internes des produits intégrant le système d'IA (si applicable).

6. Monitoring et suivi du système

- ❑ **Modifications et incidents** : Enregistrement des modifications apportées au SIA tout au long de son cycle de vie, incidents observés et test effectués.
- ❑ **Surveillance après commercialisation** : Description de la solution de contrôle des performances après commercialisation et son plan de surveillance.

CAS PARTICULIERS

- Pour les PME et les jeunes entreprises, il est possible d'établir une **version simplifiée** de la documentation, en suivant un modèle qui sera établi par la Commission.
- Pour les systèmes déjà couverts par une législation d'harmonisation de l'UE (section A, Annexe I), il convient de noter que la documentation à produire doit contenir les informations requises par le RIA (Annexe IV) ainsi que les informations requises en vertu de ces réglementations sectorielles.

NOTICE D'UTILISATION

DÉFINITION

L'Article 13 du Règlement sur l'intelligence artificielle (RIA) impose aux fournisseurs de systèmes d'IA à **Haut Risque** de fournir un guide détaillé pour l'utilisateur final : la « notice d'utilisation » (Art. 3 pt. 15), incluant les éléments suivants :

1. Description générale

- **Finalités** : Description claire des tâches que le système d'IA est conçu pour accomplir.
- **Informations de contact** : L'identité et les coordonnées du fournisseur (ou mandataire).
- **Performance attendue** : Documentation du niveau d'exactitude, de robustesse et de cybersécurité (visé à l'Art. 15), référence pour les tests et la validation du système d'IA, incluant les circonstances pouvant influencer ces niveaux.
- **Data** : Spécifications concernant les données d'entrée, ainsi que toute autre information pertinente sur les jeux de données d'entraînement, de validation et de test utilisés.

2. Instructions pour une utilisation correcte

- **Conditions d'utilisation et limitations** : Indication des cas d'utilisation prévus et des contextes dans lesquels le système peut être utilisé et liste des scénarios connus d'utilisation inappropriée potentiellement risquée pour l'utilisateur.
- **Evolutions** : Liste des modifications du système d'IA et de sa performance qui ont été prédéterminées par le fournisseur au moment de l'évaluation initiale de la conformité afin de qualifier une potentielle modification substantielle.

3. Ressources et maintenance

- **Ressources et durée de vie** : Les ressources informatiques et matérielles nécessaires pour le bon fonctionnement du système et sa durée de vie attendue.
- **Entretien** : Instructions pour assurer le bon fonctionnement du système sur le long terme, y compris les mises à jour logicielles.

4. Transparence et traçabilité

- **Explicabilité** : Capacités techniques du système d'IA de produire des informations pertinentes pour expliquer ses sorties, ainsi que des éléments permettant aux déployeurs d'interpréter et d'utiliser ces sorties de manière appropriée.
- **Contrôle humain (Art. 14)** : Mesures techniques mises en place pour permettre la supervision des sorties des systèmes d'IA.
- **Process de journalisation** : Collecte, stockage et interprétation des logs générés pour assurer la traçabilité des décisions prises par le système d'IA.