Bonnes pratiques d’usage de l’assistant IA

Version 2026-04-27 — AI Act Art. 4

Cette fiche présente les règles essentielles à suivre lors de l’utilisation des assistants IA mis à votre disposition par votre organisation, conformément à l’article 4 du Règlement européen sur l’IA (« AI Act »). Elle est destinée à toute personne opérant un système d’IA pour le compte de l’organisation.

Règles essentielles

• Vérification humaine obligatoire : l’IA peut se tromper. Toute décision ou livrable produit avec l’assistance d’une IA doit être relu et validé par un humain compétent avant utilisation.

• Ne pas soumettre de données sensibles (santé, bancaire) ni d’informations hautement confidentielles sans autorisation interne et mesures adaptées (anonymisation, espace dédié, accord du DPO).

• Pour les chatbots publics : informer l’utilisateur final qu’il parle à une IA et fournir un canal humain de recours.

• Ne pas utiliser l’IA pour des décisions RH/recrutement, du scoring de personnes, ou des décisions à fort impact (juridique, financier, médical) sans cadrage et validation préalable.

• Signaler les abus et comportements anormaux : tentatives de prompt injection, demandes illicites, exfiltration de données, sorties manifestement biaisées ou dangereuses.

Limites à connaître

• Hallucinations : l’IA peut inventer des sources, des chiffres, des références juridiques. Ne jamais citer un contenu généré sans l’avoir vérifié à la source.

• Biais : les modèles reproduisent les biais de leurs données d’entraînement. Soyez particulièrement attentif sur les sujets sensibles (genre, origine, opinions).

• Confidentialité : les prompts envoyés peuvent transiter par des fournisseurs tiers. Voir la Politique de confidentialité et le DPA pour le détail.

• Actualité : la connaissance des modèles est limitée à leur date d’entraînement. Toujours croiser les informations factuelles récentes avec une source fiable.

En cas d’incident ou d’abus

• Cessez immédiatement l’usage en cas de comportement anormal, de fuite de donnée ou de sortie illicite.

• Notifiez l’administrateur de votre tenant (admin Bulle) et, le cas échéant, le DPO de votre organisation.

• En cas de violation de données personnelles, l’administrateur déclenchera la procédure de notification au sens des articles 33 et 34 du RGPD.

Votre organisation tient un registre interne des formations AI Literacy. Si vous avez suivi une session de sensibilisation, vérifiez auprès de votre administrateur que vous y figurez.