Charte d'usage de Copilot

Deux extraits du modèle complet : l'article 4 de la charte (données et confidentialité) et l'annexe RSSI, les 12 contrôles à faire avant d'ouvrir les licences. Les passages entre crochets sont à adapter à votre entreprise.

Article 4 · Données et confidentialité

4.1. **Vérifiez vos partages.** Avant d'utiliser Copilot, assurez-vous que les dossiers, sites et équipes dont vous êtes propriétaire ne sont partagés qu'avec les personnes qui doivent y accéder. Signalez à [support / adresse] tout document sensible que vous trouvez via Copilot alors que vous ne devriez pas y avoir accès. Ne le diffusez pas.

4.2. **Classification.** Les documents classés [« Confidentiel » / « Strictement confidentiel » / libellés de votre politique] ne doivent pas être utilisés comme source de demandes à Copilot, sauf [exception à définir, par exemple pour les membres de l'équipe propriétaire du document].

4.3. **Données personnelles.** Vous pouvez traiter avec Copilot des données personnelles uniquement dans le cadre de vos missions habituelles et pour la même finalité. Vous ne devez pas l'utiliser pour :

- établir un profil d'une personne à partir de sources dispersées ;
- traiter des données de santé, d'opinions syndicales, politiques ou religieuses, ou des données relatives à des infractions, sauf si votre mission l'exige et que le DPO l'a validé ;
- prendre une décision produisant des effets sur une personne (recrutement, évaluation, sanction, octroi d'un crédit ou d'une garantie) sans examen humain réel de chaque cas.

4.4. **Autres outils d'IA.** Il est interdit de saisir dans un outil d'intelligence artificielle extérieur à l'environnement Microsoft 365 de l'entreprise (outil grand public, extension de navigateur, application mobile) :

- des données relatives à des clients, des salariés ou des partenaires ;
- des informations financières non publiées ;
- tout document classé [« Interne »] ou au-dessus ;
- du code source ou des identifiants techniques.

Annexe 2 · RSSI : 12 contrôles avant d'ouvrir les licences

#	Contrôle	Responsable	Statut
1	Lister les sites SharePoint et équipes Teams ouverts à « Tout le monde » ou « Tout le monde sauf les utilisateurs externes »		☐
2	Revoir les liens de partage « toute personne disposant du lien » encore actifs		☐
3	Vérifier que les étiquettes de confidentialité existent et sont appliquées aux espaces sensibles (RH, finance, juridique, direction)		☐
4	Restreindre la recherche sur les sites les plus sensibles le temps de la revue des droits		☐
5	Désactiver les comptes des personnes parties ; revoir les comptes de service et partagés		☐
6	Revoir les propriétaires des sites et équipes sans propriétaire actif		☐
7	Définir la durée de conservation de l'historique Copilot et des transcriptions		☐
8	Activer la journalisation et l'audit des usages Copilot ; définir qui peut y accéder et dans quels cas		☐
9	Décider de l'activation des extensions et des connecteurs vers des sources externes		☐
10	Bloquer ou encadrer l'accès aux outils d'IA grand public depuis le poste de travail, selon l'article 4.4		☐
11	Préparer la procédure de signalement d'un document trouvé par erreur (article 4.1)		☐
12	Tester le pilote sur un groupe restreint et vérifier ce qu'un utilisateur standard peut retrouver avec 10 questions types (« salaires », « licenciement », « mot de passe », « confidentiel »…)		☐

Ce modèle ne remplace pas l'avis de votre juriste, de votre DPO ni la procédure d'information-consultation de votre CSE.

La version complète : 9 articles, 4 annexes (DPO, RSSI, CSE, annonce aux salariés), Word modifiable. 290 € HT.

algs.eu/boutique/charte-usage-copilot/