OUTIL PRATIQUE · ADOPTION RESPONSABLE DE L'IA

Atelier Shadow AI

Une ligne = un usage IA concret. · Pas de charte vague. · Pas de zone grise.

Cet outil rend visibles les usages IA déjà présents ou envisagés dans une PME. L'objectif est simple : décider, usage par usage, ce qui est autorisé, autorisé sous conditions ou interdit.

Consignes d'utilisation

1 Lister les usages réels
Une ligne par usage. Formule : « J'utilise [outil + compte] pour [tâche] avec [données] ». Ex. : ChatGPT (compte perso) pour reformuler un e-mail client.

2 Classer les données
Cocher le type de données utilisées dans la ligne — voir la légende des types ci-dessous.

3 Dire à quoi sert la sortie IA
Indiquer l'usage de la sortie : idée, document interne, message externe, recommandation… — voir la légende.

4 Décider
Oui (autorisé) · Oui sous conditions (si conditions écrites respectées) · Non (interdit). Si l'équipe ne sait pas trancher : « Non pour l'instant » + question ouverte.

Registre des usages IA

TYPES DE DONNÉES : Publiques · Internes non sensibles · Clients / prospects / fournisseurs · RH / personnes · Contrats / finance · Secrets d'affaires · Sensibles · Accès / sécurité

SORTIE UTILISÉE POUR : Idée · Document interne · Message externe · Recommandation · Décision sensible · Action automatique

Responsable du registre _____ **Prochaine revue** _____

USAGE IA	OUTIL + COMPTE	DONNÉES UTILISÉES	SORTIE IA UTILISÉE POUR	DÉCISION (CONDITIONS / RESPONSABLE)
Reformuler un e-mail client	ChatGPT (compte perso)	Client / e-mail	Message externe relu	**Oui sous conditions** — Anonymiser + relire avant envoi
Importer une base clients pour générer des segments	Outil marketing IA gratuit	Clients / prospects	Segmentation commerciale	**Non** — Pas d'import de base client dans un outil non validé
Préparer des idées de posts LinkedIn	Notion AI	Publiques / non sensibles	Idée / brouillon	**Oui** — Relire exactitude et ton

SOURCES

Silic, M., Silic, D., & Kind-Trüller, K. (2025). *From Shadow IT to Shadow AI — Threats, Risks and Opportunities for Organizations.* DOI : https://doi.org/10.1002/jsc.2682

NIST (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0).* DOI : https://doi.org/10.6028/NIST.AI.100-1