Comment gérer la confidentialité des données d'entreprise lors de l'utilisation d'outils d'IA générative ?

Réponse courte

L'utilisation d'outils d'IA générative (ChatGPT, Copilot, Gemini) en entreprise au Luxembourg expose à des risques majeurs de **fuite de données confidentielles**. Toute information saisie dans un outil d'IA générative peut être stockée, réutilisée pour l'entraînement du modèle ou accessible à des tiers, ce qui constitue un **transfert de données** soumis au obligations RGPD.

L'employeur doit mettre en place une **charte d'utilisation de l'IA générative** définissant les catégories de données autorisées et interdites. Les données personnelles, les secrets d'affaires, les informations financières non publiées et les données clients ne doivent jamais être saisies dans un outil d'IA externe. Des solutions d'IA **hébergées en interne** ou avec des garanties contractuelles de non-réutilisation des données constituent des alternatives conformes. La CNPD recommande une **analyse d'impact** préalable au déploiement.

Définition

La **confidentialité des données d'entreprise face à l'IA générative** recouvre l'ensemble des mesures juridiques, techniques et organisationnelles visant à empêcher la divulgation involontaire d'informations sensibles lors de l'utilisation de modèles de langage ou d'outils de génération automatique.

Le risque principal réside dans le fait que les outils d'IA générative en mode cloud traitent les données saisies sur des serveurs externes, souvent hors de l'Union européenne. Cette situation peut constituer un **transfert international de données** au sens du RGPD (chapitre V) et une violation potentielle du secret des affaires protégé par la directive (UE) 2016/943.

Questions fréquentes

Comment gérer la confidentialité des données d'entreprise face à l'IA générative ?

En adoptant une charte d'utilisation interdisant la saisie de données personnelles, secrets d'affaires et données financières dans les outils externes. Privilégier des solutions hébergées en interne ou avec garanties contractuelles de non-réutilisation et de localisation UE. La CNPD recommande une AIPD préalable.

Faut-il une analyse d'impact avant de déployer un outil d'IA générative ?

Oui, fortement recommandée. La CNPD préconise une AIPD pour tout outil d'IA générative. Elle est obligatoire (article 35 RGPD) si le traitement présente un risque élevé pour les droits et libertés des personnes concernées. L'AIPD doit précéder le déploiement.

Les versions gratuites d'IA générative offrent-elles des garanties de confidentialité ?

Non. Les versions grand public ou gratuites ne fournissent généralement aucune garantie de non-réutilisation des données saisies. Seules les versions entreprise (Azure OpenAI, AWS Bedrock) avec contrat de traitement RGPD offrent un niveau de protection adapté au cadre européen.

Quel est le principe du zero data appliqué à l'IA générative ?

Le principe consiste à partir du postulat que toute information saisie dans un outil d'IA générative externe est potentiellement compromise. Les salariés doivent saisir uniquement des contenus pouvant être considérés comme publics, sans contexte permettant l'identification d'informations sensibles.

Quelles données ne jamais saisir dans un outil d'IA générative externe ?

Les données personnelles (salariés, clients, candidats), secrets d'affaires, code source propriétaire, données financières non publiées et informations couvertes par le secret professionnel. Ces saisies constituent des transferts de données soumis au chapitre V du RGPD.

Quelles mesures techniques mettre en place contre les fuites par IA générative ?

Filtrage des données sortantes (DLP), journalisation des requêtes, blocage des outils non approuvés sur le réseau d'entreprise, classification automatique des données sensibles. Ces contrôles complètent les mesures organisationnelles (charte, formation, audits trimestriels).

Conditions d’exercice

La mise en place d'un cadre de confidentialité pour l'IA générative en entreprise repose sur des exigences juridiques et organisationnelles cumulatives.

Critère	Détail
Données interdites	Données personnelles (salariés, clients, candidats), secrets d'affaires, code source propriétaire, données financières non publiées, informations couvertes par le secret professionnel
Données autorisées	Informations publiques, données anonymisées, questions génériques sans contexte identifiant, textes à reformuler sans contenu sensible
Base légale RGPD	Consentement ou intérêt légitime pour le traitement ; interdiction de transfert hors UE sans garanties appropriées (chapitre V RGPD)
Charte IA obligatoire	Document interne définissant les usages autorisés, les outils approuvés, les catégories de données, les responsabilités et les sanctions
Analyse d'impact (AIPD)	Obligatoire si le traitement présente un risque élevé pour les droits et libertés (article 35 RGPD) ; recommandée par la CNPD pour tout outil d'IA générative
Clauses contractuelles	Vérifier les conditions d'utilisation du fournisseur : réutilisation des données, localisation des serveurs, durée de conservation, sous-traitants
Consultation sociale	Information de la délégation du personnel sur l'introduction d'un nouvel outil technologique (art. L.414-3 et suivants)

Modalités pratiques

Le déploiement sécurisé d'outils d'IA générative en entreprise suit un processus structuré.

Étape	Détail
Inventaire des risques	Cartographier les flux de données, identifier les informations sensibles susceptibles d'être saisies, évaluer les risques de fuite par service
Sélection des outils	Privilégier les versions entreprise (Azure OpenAI, AWS Bedrock) avec garanties contractuelles de non-réutilisation ; exiger l'hébergement UE
Rédaction de la charte	Définir précisément les usages autorisés et interdits, les outils approuvés, les procédures d'escalade et les sanctions disciplinaires
Formation des salariés	Sessions obligatoires sur les risques de fuite de données, les bonnes pratiques de saisie, les réflexes de vérification avant soumission
Contrôles techniques	Filtrage des données sortantes (DLP), journalisation des requêtes, blocage des outils non approuvés sur le réseau d'entreprise
Audit régulier	Vérification trimestrielle du respect de la charte, analyse des incidents, mise à jour des règles en fonction des évolutions technologiques

Pratiques et recommandations

Adopter le principe du "zero data" pour les outils d'IA générative externes en partant du postulat que toute information saisie est potentiellement compromise et en formant les salariés à cette approche.

Mettre en place des solutions d'IA générative hébergées en interne ou dans un cloud privé européen, avec des garanties contractuelles explicites de non-réutilisation des données pour l'entraînement des modèles.

Sensibiliser régulièrement les équipes aux risques spécifiques de l'IA générative en illustrant par des cas concrets de fuites de données et en rappelant les conséquences disciplinaires et juridiques.

Intégrer la gouvernance de l'IA générative dans la politique de sécurité de l'information existante, en désignant un référent IA chargé de coordonner les usages et de veiller à la conformité.

Documenter l'ensemble du dispositif pour démontrer la conformité en cas de contrôle de la CNPD et conserver les preuves de formation et de sensibilisation des salariés.

Cadre juridique

Référence	Objet
RGPD - Articles 5 et 6	Principes de licéité, loyauté, minimisation ; bases légales du traitement
RGPD - Article 28	Obligations du sous-traitant (fournisseur d'IA) ; contrat de traitement obligatoire
RGPD - Article 35	Analyse d'impact relative à la protection des données (AIPD)
RGPD - Chapitre V (art. 44-49)	Transferts de données vers des pays tiers ; garanties appropriées
AI Act (UE 2024/1689)	Obligations de transparence pour les systèmes d'IA à usage général
Directive (UE) 2016/943	Protection des secrets d'affaires
Art. L.261-1	Traitement des données à caractère personnel des salariés
Art. L.414-3 et suivants	Information et consultation de la délégation du personnel sur les nouvelles technologies

La confidentialité des données face à l'IA générative constitue un enjeu majeur pour les entreprises luxembourgeoises. Les versions gratuites ou grand public des outils d'IA générative ne fournissent généralement aucune garantie de non-réutilisation des données saisies. Seules les versions entreprise avec contrat de traitement RGPD offrent un niveau de protection adapté au cadre juridique luxembourgeois et européen.