

**LSI**LEARNY SOCIETY
INTERNATIONAL

PLAQUETTE 2026

IA & TECHNOLOGIES · GOUVERNANCE & TRANSFORMATION

IA responsable, confidentialité et sécurité des données

Savoir ce que l'on peut confier à une IA, anonymiser ce qui doit l'être, régler son outil et réagir à un incident, avec une première charte d'usage pour son équipe.

● Cours disponible · sur devis

DURÉE

1 jour (7h)

FORMAT

Présentiel · Distanciel · Hybride

PUBLIC

Tous salariés, managers et équipes qui utilisent ou vont utiliser l'IA générative et manipulent des données clients, RH, financières ou internes ; référents IA, assistants de direction et fonctions support de l'entreprise.

PRÉREQUIS

Aucun prérequis technique ni juridique.
Disposer d'un accès à l'outil d'IA autorisé par l'entreprise (ou à un compte gratuit, utilisé uniquement avec des données fictives).
Apporter, si elles existent, la charte informatique ou la politique d'usage de l'IA de l'entreprise, et la liste des types de documents manipulés au quotidien – sans les documents eux-mêmes.

Pourquoi cette formation.

Une journée pour acquérir les réflexes qui protègent les données de l'entreprise quand on utilise l'IA générative : ce que l'on peut saisir, comment anonymiser, quel outil utiliser, qui valide et quelle trace conserver. Les participants repartent avec une première charte pratique d'utilisation de l'IA, écrite pour leur équipe.

Le risque le plus courant n'est pas technique : c'est un contrat client collé dans un compte personnel, une conversation partagée par lien sans le savoir, un entretien RH transcrit par un outil que personne n'a validé, une réponse erronée envoyée telle quelle. Ces gestes sont rarement malveillants ; ils viennent d'une absence de règles claires et de réflexes partagés.

La journée alterne apports courts et exercices sur des situations professionnelles fictives ou anonymisées : trier des données, anonymiser des documents, vérifier les réglages d'un outil, réagir à un incident, décider qui valide une production. Le RGPD et le règlement européen sur l'IA sont présentés comme des cadres à connaître : il s'agit d'une sensibilisation professionnelle, pas d'un conseil juridique personnalisé — les questions propres à votre situation relèvent de votre DPO, de votre service juridique ou de votre conseil.

OBJECTIFS

À l'issue de la formation.

01 Identifier les principaux risques d'un usage non encadré de l'IA générative : fuite de données, IA fantôme, erreur diffusée, manipulation

02 Classer une information selon sa sensibilité avant toute saisie dans un outil d'IA

03 Anonymiser un document en supprimant les éléments directement et indirectement identifiants

04 Vérifier les paramètres d'historique, de mémoire, de partage et de connexion d'un outil d'IA autorisé

05 Repérer les tentatives de manipulation qui passent par l'IA : consignes cachées, hameçonnage, voix imitée

06 Déterminer le niveau de validation humaine et la trace à conserver selon l'usage d'une production

07 Rédiger une première charte pratique d'utilisation de l'IA adaptée à son équipe

Le programme.

MODULE 01 • 1 H

Ce que deviennent les données saisies dans une IA

- Le trajet d'une donnée saisie : conversation, historique, conservation, usage éventuel pour améliorer les modèles selon l'outil et l'offre
- Compte personnel, compte professionnel, outil interne : ce qui change pour l'entreprise
- Les risques d'un usage non encadré : fuite, IA fantôme, erreur diffusée, biais, atteinte à la réputation
- Cadres à connaître, en sensibilisation : RGPD, règlement européen sur l'IA, secret des affaires, engagements de confidentialité, politique interne
- Qui consulter pour une question précise : DPO, juriste, responsable de la sécurité informatique, référent IA

MODULE 02 • 1 H 15

Classer les données avant de les saisir

- Données personnelles directes et indirectes : nom et courriel, mais aussi poste, site, date, numéro de dossier
- Données à protéger en priorité : santé, vie privée, évaluations et dossiers RH, coordonnées bancaires
- Informations de l'entreprise : documents internes, données clients, tarifs, contrats, stratégie, code source
- Le feu tricolore : vert transmissible, orange à anonymiser ou réservé à un outil validé, rouge jamais saisi
- Cas limites : captures d'écran, pièces jointes, transcriptions de réunion, métadonnées des fichiers

MODULE 03 • 1 H 15

Anonymiser et minimiser

- Minimiser d'abord : ne donner à l'outil que ce dont la tâche a besoin
- Trois techniques : remplacer par des repères (Client A, Salarié 1), généraliser (fourchettes, périodes, régions), supprimer
- Le piège du recoupement : poste, site et ancienneté suffisent souvent à reconnaître une personne
- Anonymiser ou pseudonymiser : tant qu'une table de correspondance existe, la personne reste identifiable
- Ne jamais confier un document brut à un outil non autorisé pour qu'il l'anonymise : la saisie est déjà la fuite
- Vérifier le résultat : relecture, recherche des identifiants restants, test d'utilité de la version anonymisée

Outils autorisés, permissions et nouvelles menaces

- Outils autorisés, tolérés, interdits : lire la politique de l'entreprise et savoir à qui demander
- Paramètres à vérifier : historique, mémoire, utilisation des conversations, liens de partage, espaces partagés
- Connecteurs et permissions : un assistant relié à la messagerie ou aux fichiers voit tout ce que voit l'utilisateur
- Extensions de navigateur, applications mobiles, outils de transcription de réunion : les accès accordés sans y penser
- Menaces qui passent par l'IA : consignes cachées dans un document ou une page web, hameçonnage mieux rédigé, voix ou vidéo imitant un dirigeant

Vérifier, valider, tracer

- Proportionner la relecture au risque : usage personnel, diffusion interne, envoi externe, document engageant
- Qui valide quoi : l'auteur, le manager, l'expert métier, le juriste — jamais l'outil
- La trace minimale : outil utilisé, sources fournies, date, personne qui a validé
- Transparence : quand et comment indiquer qu'un contenu a été préparé avec l'IA
- Signaler une erreur ou un usage inadapté sans chercher de coupable

Atelier final : une première charte pratique d'utilisation de l'IA

- La structure d'une charte utile : outils, données, anonymisation, vérification, validation, trace, incidents, contacts
- Écrire des règles applicables : phrases courtes, exemples du métier, réponses « oui », « non » ou « à demander »
- Relier la charte aux documents existants : charte informatique, politique de sécurité, procédures du service
- Préparer la validation et la diffusion : qui relit, qui approuve, comment la faire vivre

Comment on travaille.

PÉDAGOGIE

- Études de cas tirées de situations professionnelles réelles, anonymisées, analysées en groupe
- Démonstrations commentées des paramètres de confidentialité et de partage des outils autorisés
- Plus de la moitié du temps en pratique : tri de données, anonymisation, traitement d'incidents, rédaction de la charte
- Mises en situation de manipulation (consigne cachée, message frauduleux) pour ancrer les réflexes
- Production accompagnée de la charte, relue par un autre sous-groupe puis commentée par le formateur
- Chaque exercice se fait avec l'outil autorisé dans l'entreprise ; à défaut, avec les versions gratuites de ChatGPT, Claude ou Copilot et des cas fictifs fournis par le formateur.

ÉVALUATION

Auto-positionnement avant la formation, exercices corrigés et quiz en cours de journée, charte finale évaluée sur grille et testée sur des situations tirées au sort. Attestation de formation remise à l'issue du parcours.

VOUS REPORTEZ AVEC

- Votre première charte pratique d'utilisation de l'IA, une à deux pages, prête à être soumise à validation
- Le tableau feu tricolore pour classer une information avant de la saisir
- La méthode d'anonymisation, avec la liste des identifiants indirects à rechercher
- La check-list de réglage d'un outil d'IA : historique, mémoire, partage, connecteurs, extensions
- La fiche réflexe incident : que faire, qui prévenir, comment éviter la récurrence
- La grille des niveaux de validation et le modèle de trace d'usage

INTRA, INTER OU SUR MESURE

Construisons votre session.

TARIF

Sur devis, communiqué avant tout engagement

RÉPONSE

Sous 48 à 72 h ouvrées

MODALITÉS

Présentiel, classe virtuelle ou hybride

CONTACT

contact@lsi-society.com · 06 69 53 48 71

Demander un devis → lsi-society.com/catalogue/ia-responsable-confidentialite

LSI — Learnly Society International — Entreprise individuelle Marcus Détrez, 135 avenue du 24 avril 1915, Bâtiment E2, 13012 Marseille, France · SIRET 897 775 094 00039. Déclaration d'activité enregistrée sous le n° 93132113413 auprès du préfet de région Provence-Alpes-Côte d'Azur. Cet enregistrement ne vaut pas agrément de l'État. Exonération de TVA en application de l'article 261-4-4°-a du code général des impôts (formation professionnelle continue).