

# CHARTRE D'USAGE DE L'IA EN ENTREPRISE

Du Shadow AI à la gouvernance active : cadrer sans briser l'innovation

## 1 - L'IA personnelle au bureau : une fausse bonne idée hautement contre-productive

### LE CONSTAT

Pensant gagner en rapidité, les collaborateurs intègrent l'IA de manière informelle et individuelle sur leurs postes de travail.

### LE PIÈGE

Sans cadre, ce gain individuel immédiat se transforme en dette technique, juridique et managériale : perte d'homogénéité des méthodes, fuites de données invisibles, hallucinations non vérifiées dans les livrables clients et absence de capitalisation collective.

### LA RÉALITÉ

Une entreprise ne devient pas plus performante parce que ses salariés « bricolent » avec des comptes gratuits ; elle le devient lorsqu'elle organise l'usage collaboratif et maîtrise de l'outil.

## 2 - Comprendre le phénomène de « Shadow AI »

### 1 - La règle trop générale

Un interdit flou et déconnecté du terrain (« Interdiction formelle d'utiliser l'IA générative avec des données de l'entreprise »).

### 2 - Le besoin métier incompressible

Synthétiser 40 pages de réunion, traduire un document technique, générer du code, préparer une présentation client.

### 3 - L'absence d'alternative claire

Aucun outil validé fourni par la DSI, aucune consigne opérationnelle, aucun canal officiel de demande.

### 4 - Le passage dans l'ombre (Shadow AI)

Utilisation de comptes personnels hors SSO, recours à des outils tiers gratuits non vérifiés, installation d'extensions navigateur aspiratrices de données.

### L'ALERTE GOUVERNANCE

Le Shadow AI ne naît presque jamais d'une volonté délibérée de contourner les règles, mais d'un besoin métier bien réel laissé sans solution concrète. **Encadrer l'IA ne signifie pas interdire : cela consiste à rendre les bons usages plus simples et accessibles que les mauvais.**

## 3 - Pourquoi la charte est indispensable

Même si elle n'est pas obligatoire : le Règlement européen sur l'IA (AI Act) n'impose aucun document formel intitulé « Charte IA ». En revanche, l'obligation de conformité impose un cadre d'opposabilité immédiat.

### Socle AI Act

**Maîtrise de l'IA (Art. 4)** : obligation d'assurer la littératie et la formation des collaborateurs.

**Usages interdits (Art. 5)** : proscription absolue des systèmes biométriques ou scoring social.

**Transparence (Art. 50)** : obligation de signaler les contenus générés ou modifiés par IA.

**Statut de Déployeur** : responsabilité engagée sur les biais et erreurs d'exécution.

### Socle RGPD & données personnelles

**Données personnelles** : interdiction stricte de copier des identifiés ou données sensibles dans des modèles publics.

**Sécurité (Art. 32 RGPD)** : mesures techniques contre les fuites vers des tiers non identifiés.

**Décisions automatisées (Art. 22)** : droit à l'intervention humaine et interdiction du tout-automatisé pour le recrutement ou l'évaluation.

### Risques métiers, propriété & cybersécurité

**Propriété intellectuelle** : non-cession automatique des droits, risque de plagiat ou perte de confidentialité des brevets/code source. Un contenu entièrement généré par IA n'est en principe pas protégeable par le droit d'auteur.

**Sécurité entrante** : injection de prompts indirecte via des documents externes, code généré à contrôler.

**Secret des affaires** : risque de réentraînement des LLM sur le savoir-faire interne.

**Droit social** : encadrement des impacts sur les conditions de travail et articulation disciplinaire.

# CONCEVOIR, DÉPLOYER ET FAIRE VIVRE SA CHARTE IA

**Formule directrice** : la règle d'or repose sur le croisement de 3 variables :

### Outil x Donnée x Configuration

**Configuration** : veiller à la désactivation explicite de l'historique d'entraînement (Data Sharing Opt-Out) ou privilégier les accès API / environnements cloisonnés (Private Tenants). Les conditions diffèrent selon l'offre (interface web / SaaS, licence entreprise, API) : à vérifier dans les CGU.

## Le parcours d'implémentation en 6 étapes clés



01

### Cartographier

Usages & Shadow AI



02

### Qualifier

Outils & risques



03

### Associer

Métiers, IT, CSE



04

### Formaliser

Matrice d'action



05

### Déployer

Adjonction & formation



06

### Faire vivre

Audit & revue



### 1 - Cartographier sans juger

AUDIT DES PRATIQUES RÉELLES

- Lancer un audit flash anonyme auprès des équipes pour recenser les outils réellement utilisés (ChatGPT, Claude, Gemini, plugins Copilot, extensions Chrome, outils de transcription audio).
- Cartographier les cas d'usage spontanés : génération de texte, extraction de données de bilans financiers, revue de code, rédaction d'emails commerciaux.
- Identifier les blocages actuels qui incitent au contournement (absence de licences entreprise, lourdeur des outils existants).

#### COMMENT MESURER L'USAGE RÉEL ?

Par un **questionnaire anonyme de cinq questions, renouvelé tous les six mois**, plutôt que par une surveillance réseau, qui ne capte pas les téléphones personnels et détruit la confiance.



### 2 - Qualifier et analyser les risques

LE RÔLE CLÉ DU BINÔME DSI / JURISTE

- Évaluer les conditions contractuelles (CGU)** : les prompts servent-ils à réentraîner les modèles ? L'infrastructure garantit-elle une rétention zéro des données (Zero Data Retention) ?
- Bon à savoir** : les offres entreprise des grands fournisseurs garantissent contractuellement que vos données ne servent pas à entraîner les modèles, et offrent une administration centralisée.
- Classifier les données manipulables** :

**Zone Verte (Publique)** : données déjà publiques, éléments marketing généraux.

**Zone Orange (Interne)** : données professionnelles sans données personnelles ni secrets industriels (utilisation sous licence entreprise uniquement).

**Zone Rouge (Interdite hors environnement validé)** : données personnelles (clients, salariés), codes sources propriétaires, données de santé, secrets de fabrication ou de R&D. Jamais dans un outil grand public ou non validé ; traitement possible uniquement dans un environnement d'entreprise validé (cloisonné, droits d'accès limités, journal d'audit).

#### LE TEST ULTIME

« Est-ce que je l'enverrais par email à un inconnu ? »

La question à toujours se poser avant de partager un document dans un LLM. Si la réponse est non, c'est rouge.

- Sécurité entrante** : sensibiliser au risque d'injection de prompts (attaques via l'analyse de documents externes non sécurisés) et au contrôle du code généré (dépendances inexistantes ou malveillantes).



### 3 - Associer et co-construire

DIALOGUE SOCIAL ET TRANSVERSALITÉ

- Parties prenantes obligatoires** : DSI (sécurité, SSO, API), DPO / Juriste (RGPD, AI Act, PI), Direction RH et représentants des métiers.
- Dialogue social (CSE)** : anticiper impérativement les questions relatives à l'évaluation du travail, la surveillance éventuelle de l'activité numérique et l'impact sur les compétences.



### 4 - Formaliser une matrice de décision opérationnelle

- Remplacer les longs paragraphes par une grille lisible par chaque salarié :
- Cas autorisés** : quels outils, pour quelles tâches précises, avec quelles typologies de données.
- Cas sous validation** : procédure à suivre pour tester une nouvelle IA générative ou un nouvel agent autonome.
- Cas strictement interdits** : usages contraires à l'éthique, soumission de données confidentielles à des outils gratuits, automatisation complète sans validation humaine sur les actions sensibles ou les décisions produisant des effets juridiques.
- Le principe du « Human in the Loop »** : rappel formel que l'IA ne porte aucune responsabilité juridique ; chaque collaborateur demeure l'unique garant et signataire de l'exactitude de ses livrables.
- Rappel PI** : un livrable entièrement généré par IA n'est en principe pas protégeable par le droit d'auteur. Seule une intervention humaine créative peut conférer une protection aux créations de l'entreprise.
- Traçabilité** : documenter et consigner la part d'IA dans les processus critiques (traçabilité de l'usage pour répondre aux exigences d'audit et de transparence client).



### 5 - Déployer et conférer une valeur juridique

L'OPPOSABILITÉ

- Document pédagogique vs norme disciplinaire** : une charte simplement partagée sur l'intranet est un guide de bonnes pratiques, mais elle n'a aucune valeur pour sanctionner un manquement grave (fuite de données).
- Pour être **opposable**, la charte doit être annexée au **Règlement Intérieur** de l'entreprise, soumise à consultation préalable du CSE, transmise à l'Inspection du Travail et diffusée formellement à l'ensemble du personnel.
- Mettre en place un plan de formation pratique adapté aux métiers plutôt qu'une communication descendante unique.

#### LE FORMAT QUI FONCTIONNE

La charte tient sur **deux pages** et répond à **trois questions** : quels outils sont autorisés, quelles données ne doivent jamais y entrer, et à qui poser une question en cas de doute.

Elle est présentée lors d'une **session de 45 minutes** avec les collaborateurs, puis signée.

Ce qui change les comportements, c'est l'**implication du manager** : il montre comment il utilise l'IA validée, partage un bon prompt en réunion et rappelle la règle des couleurs en cas de doute.

#### QUE DIT L'AI ACT SUR CE SUJET ?

Depuis **février 2025**, le règlement impose une obligation de « **maîtrise de l'IA** » par le personnel (article 4) : les entreprises doivent s'assurer que leurs collaborateurs qui utilisent des systèmes d'IA en ont un niveau de compréhension suffisant.

Une charte et une session de sensibilisation en sont la **première brique**.



### 6 - Faire vivre et auditer

GOUVERNANCE CONTINUE

- Désigner un **Référent IA** (ou Comité IA) clairement identifié, contactable immédiatement en cas de doute.
- Intégrer une **clause de revoyure périodique** (tous les 6 à 12 mois) pour réévaluer les outils acceptés face au rythme des sorties technologiques et réglementaires.

## La double check-list d'efficacité opérationnelle

### Côté collaborateur (au quotidien)

- Quel outil ai-je le droit d'ouvrir pour cette tâche ?
- Pour quel cas d'usage précis est-ce validé ?
- Mes données contiennent-elles des éléments confidentiels ou personnels ?
- Ce traitement nécessite-t-il l'accord de mon manager ou du référent ?
- Ai-je vérifié et validé moi-même chaque résultat (zéro hallucination) ?
- Qui dois-je contacter immédiatement si j'ai un doute ?

### Côté organisation (gouvernance)

- Les usages réels ont-ils été audités (sortis de l'ombre) ?
- Les CGU et politiques de confidentialité des outils sont-elles vérifiées ?
- La charte a-t-elle été soumise au CSE et annexée au Règlement Intérieur ?
- Les équipes on-elles reçu une formation pratique (Art. 4 AI Act) ?
- Une procédure claire d'expérimentation de nouveaux outils est-elle définie ?
- Le cycle de révision semestriel est-il planifié ?

Une charte IA réussie ne se mesure pas à son nombre de pages, mais aux réflexes qu'elle installe au quotidien.