



• PLAYBOOK DIRIGEANTS · MIS À JOUR JUILLET 2026

Confidentiality Playbook for Claude

Ce que deviennent réellement vos données quand vous les confiez à Claude — et comment travailler sur **vos vrais dossiers** sans exposer votre entreprise.

5 ans

Compte grand public

Rétention si vous laissez l'entraînement activé.

30 jours

Modèles sous surveillance

Rétention imposée — même sous accord « zéro rétention ».

0

Sous accord ZDR

Rien n'est stocké après la réponse. Sous conditions.

Trois chiffres, un seul outil. **La même phrase, tapée dans deux comptes Claude différents, n'a pas le même destin.** Tout ce playbook tient dans cette idée — et dans les décisions qu'elle impose à votre direction.

Trois craintes arrêtent 80 % des projets IA. Une seule est fondée.



« Nos données ne sortent pas d'ici. »

— La phrase entendue dans chaque comité de direction, juste avant que le projet ne s'arrête.

1

« Claude va s'entraîner sur nos contrats. »

VRAI — MAIS SEULEMENT CHEZ VOUS

Sur un compte **Free, Pro ou Max**, si l'option d'entraînement est laissée active, les conversations peuvent servir à entraîner les futurs modèles. Sur un compte **Team, Enterprise ou API**, c'est non par défaut, contractuellement. Le risque n'est pas l'outil : c'est le collaborateur qui utilise son abonnement personnel au bureau.

2

« Nos échanges seront stockés pour toujours. »

FAUX

Aucune durée n'est « pour toujours ». Elles sont écrites, bornées et publiques : **5 ans, 30 jours, ou rien du tout**. Le problème n'est pas qu'elles soient longues — c'est que **personne dans l'entreprise ne sait laquelle s'applique** à ce qui a déjà été tapé.

3

« De toute façon, on serait hors-la-loi. » (RGPD, loi 09-08)

NI VRAI NI FAUX — ÇA DÉPEND DE VOUS

Aucun outil ne vous met en conformité, et aucun ne vous met hors-la-loi tout seul. Ce sont **votre cadre d'usage, votre base légale et votre information des personnes** qui décident. C'est une bonne nouvelle : c'est la seule des trois craintes que **vous maîtrisez à 100 %**.

La bonne question n'est pas « Claude est-il sûr ? ».
C'est « par quelle porte êtes-vous entré ? »

Poser la question autrement débloque la décision : on ne cherche plus à évaluer un outil dans l'absolu, on choisit une configuration. Et une configuration, ça se décide en une réunion.

La confidentialité ne dépend pas de Claude. Elle dépend de la porte d'entrée.

Même modèle. Même prompt. Même réponse. **Quatre destins différents pour vos données**, selon le compte utilisé pour taper la phrase. C'est le point que 9 dirigeants sur 10 ignorent — et c'est celui qui décide de tout.

PORTE
1

Compte grand public

Free · Pro · Max — y compris Claude Code depuis ces comptes

Entraînement possible

5 ans de rétention si l'option est active · 30 jours si elle est coupée

PORTE
2

Claude Team & Enterprise

Claude for Work — comptes gérés par l'entreprise

Pas d'entraînement

Rétention pilotée par votre politique d'organisation

PORTE
3

API & Claude Code commercial

Clés API d'une organisation sous conditions commerciales

Pas d'entraînement

Le contenu des échanges n'est pas conservé par défaut

PORTE
4

Zero Data Retention (+ HIPAA)

Sur demande et validation — API / Enterprise, par organisation

Rien stocké après la réponse

Le niveau des données réglementées — avec des exceptions (p. 5 et 6)

EXPOSITION



MAÎTRISE



Le vrai risque n'est presque jamais technique. Il est organisationnel.

Vous pouvez avoir signé le meilleur contrat du marché : si votre responsable commercial colle le fichier clients dans **son abonnement Pro personnel** depuis son téléphone, vous êtes revenu porte 1. **Ouvrir la bonne porte ne suffit pas — il faut fermer les autres**, et c'est un travail de direction, pas de DSI.

Les quatre régimes, ligne par ligne

À imprimer et à poser sur la table du prochain comité. Une colonne = une décision.

	GRAND PUBLIC FREE · PRO · MAX	TEAM & ENTERPRISE CLAUDE FOR WORK	API COMMERCIAL + CLAUDE CODE	ZDR SUR VALIDATION
Entraînement des modèles sur vos échanges	Oui, si l'option est active — c'est un choix laissé à l'utilisateur.	Non par défaut, au titre des conditions commerciales.	Non par défaut, au titre des conditions commerciales.	Non — et le contenu n'est même pas stocké.
Rétention du contenu prompts & réponses	5 ans si entraînement actif ; 30 jours s'il est coupé.	Selon la politique de rétention de votre organisation (paramétrable).	Contenu non conservé par défaut ; exception : les modèles à 30 jours (p. 5).	Rien n'est conservé après l'envoi de la réponse.
Qui décide du réglage	Le salarié , sur son compte, sans que vous le sachiez.	L'administrateur de l'organisation.	L'organisation , par workspace.	Contrat — activé par organisation, jamais automatique.
Données que vous pouvez y mettre	Publiques uniquement. Rien de client, rien de RH.	Interne et confidentiel, une fois la politique posée.	Interne et confidentiel — cadre à privilégier pour l'industrialisation.	Réglementé : santé, données sensibles, secret professionnel.
Coût d'entrée ordre de grandeur	Gratuit à ~20 \$/mois. Le moins cher, le plus coûteux en risque.	Par siège, engagement annuel. Le standard PME.	À l'usage. Le cadre des workflows automatisés.	Négocié avec l'équipe commerciale Anthropic.

LE DÉTAIL QUE TOUT LE MONDE OUBLIE

Le **pouce ↑ / pouce ↓** sous une réponse est un **consentement explicite**. Un salarié qui clique « pouce en bas » sur une réponse contenant un extrait de contrat vient d'autoriser l'utilisation de ce contenu — **même sur un compte commercial** — et les données liées à ce retour sont conservées 5 ans. C'est la seule fuite qui traverse toutes les portes. À dire en formation, à écrire dans la charte.

Sources : Anthropic — *Updates to Consumer Terms and Privacy Policy* ; Centre de confidentialité Anthropic — *Is my data used for model training?, How long do you store my data?* ; Claude Platform Docs — *API and data retention*. Vérifié le 15/07/2026. Les politiques évoluent : revalidez avant tout engagement contractuel.

« Zéro rétention » ne veut pas dire zéro. Et ça, c'est nouveau.

Si vous ne deviez retenir qu'une page de ce playbook, prenez celle-ci. C'est l'information qui manque dans 100 % des notes internes que nous lisons chez nos clients.

LE MÉCANISME

Covered Models

Les modèles les plus capables sont placés sous **surveillance de sécurité renforcée**. Aujourd'hui : **Claude Mythos 5** et **Claude Fable 5**.

LA CONSÉQUENCE

30 jours, imposés

Les prompts envoyés à ces modèles et les réponses produites sont **conservés 30 jours**. Ce n'est pas une option : c'est la condition d'accès.

LA RAISON

Voir le motif

Certains détournements — jailbreak par répétition, attaques étatiques — ne se voient **qu'en regardant à travers de nombreuses requêtes**. Une seule ne dit rien.

× CE QU'ON LIT PARTOUT

« Depuis peu, tout est conservé 30 jours pour raisons de sécurité, **sauf si on a un accord ZDR**. »

✓ CE QUI EST VRAI

C'est **l'inverse**. La règle vise **certains modèles**, pas toutes les plateformes — et elle **prime sur le ZDR** au lieu de l'épargner.

Le retournement : cette règle ne change rien pour le compte Pro de votre stagiaire.

Elle ne touche que les organisations les plus prudentes.

Les comptes **Free, Pro et Max** sont **inchangés** — leurs contenus étaient déjà conservés. Les concernés sont précisément ceux qui avaient négocié le **zéro rétention** : ils doivent désormais **activer une rétention de 30 jours** pour accéder à ces modèles. Ceux qui ont fait l'effort de conformité sont les seuls à devoir agir.

```
// Ce que renvoie l'API si la rétention n'est pas activée :
{ "type": "error", "error": { "type": "invalid_request_error",
  "message": "In order to access this model, your organization or
  workspace must have data retention enabled." } }

// La porte de sortie : activer la rétention 30 j sur UN SEUL workspace.
// Les autres workspaces de l'organisation restent en zéro rétention.
```



Action immédiate : si votre note interne dit « ZDR = aucune donnée stockée, point », elle est fausse.

Corrigez-la cette semaine. La formulation juste : « **zéro rétention par défaut, sauf modèles sous surveillance renforcée (30 jours) et sauf contenu signalé** ». Un DPO qui découvre l'écart six mois après la signature ne vous le pardonnera pas — et il aura raison.

Ce qui reste, **quoi qu'il arrive**

Quatre cas survivent à tous les contrats, y compris au ZDR. Les connaître, c'est pouvoir répondre en réunion sans bluffer — et **ne rien promettre que vous ne puissiez tenir**.

2 ans
MAXIMUM

Le contenu signalé par les systèmes de sécurité

Si une conversation est **signalée automatiquement** par les systèmes de confiance et sécurité, les entrées et les sorties peuvent être conservées jusqu'à 2 ans — **même sous accord ZDR**.

7 ans
MAXIMUM

Les scores de classification

Les **scores** attribués par les classificateurs de sécurité (pas le contenu lui-même) peuvent être conservés jusqu'à 7 ans. C'est de la métadonnée — mais c'en est.

5 ans
APRÈS LE CLIC

Le feedback — le pouce ↑ / ↓

Cliquer sur le pouce, c'est **consentir explicitement**. Les données associées à ce retour sont conservées 5 ans et peuvent servir à l'entraînement, **y compris pour un client commercial**. C'est le geste le plus anodin du produit et le plus lourd de conséquences.

Légal
DURÉE REQUISE

L'obligation légale et la conservation à titre conservatoire

Comme chez **tout fournisseur** — votre banque, votre hébergeur, votre opérateur — une obligation légale prime sur le contrat. Aucun prestataire sérieux ne vous promettra le contraire.

Le ZDR réduit la surface d'exposition. Il ne fabrique pas **de l'invisibilité**.

C'est exactement ce qu'il faut dire à un comité. Un dirigeant qui promet « zéro trace » perd sa crédibilité au premier audit. Un dirigeant qui annonce « voici les quatre exceptions, elles sont documentées, voici notre position sur chacune » **gagne l'arbitrage**. La précision est un actif politique.

Ce que vos équipes doivent faire avant d'appuyer sur Entrée

1

Vérifier la porte avant de taper

Le premier réflexe n'est pas d'écrire : c'est de **regarder dans quel compte on est**. Un abonnement Pro personnel et un compte entreprise ont la même interface — et deux régimes juridiques opposés.

À faire cette semaine : sur tout compte grand public utilisé au travail, ouvrir les paramètres de confidentialité et **désactiver l'entraînement**. Deux minutes. C'est la seule action de ce playbook qui protège rétroactivement les prochaines conversations.

2

Minimiser — le prompt n'est pas un dossier

Ne mettre que **le strict nécessaire**. On n'a presque jamais besoin du vrai nom, du numéro de contrat ou de l'email complet pour obtenir une excellente réponse. Le réflexe « je colle tout, il triera » est un réflexe de moteur de recherche, pas d'IA.

3

Pseudonymiser par automatisme

Remplacer noms, identifiants et montants sensibles par des variables : « **Client A** », « **[MONTANT]** », « **[CONTACT]** ». Les vraies valeurs se ré-injectent après coup, en local, dans le document final. Voir la démonstration page 9.

4

Ne jamais coller de secrets

Mots de passe, clés d'API, coordonnées bancaires, données de santé, pièces d'identité. Jamais, quelle que soit la porte.

Pourquoi celui-là est différent : les six autres réflexes se rattrapent. Un secret collé ne se corrige pas — il se **révoque**. Une clé d'API exposée doit être régénérée, pas regrettée. Traitez cette règle comme le port du casque : non négociable, sans exception « juste cette fois ».

Puis les trois qui font la différence en audit

5

Classer avant de coller

Appliquer la classification de l'entreprise — **public / interne / confidentiel / réglementé** — et en déduire la porte. Le confidentiel et le réglementé ne sortent jamais du cadre entreprise. La grille de décision est page 10.

6

Se méfier des fichiers plus que des phrases

Un Excel « anodin » contient souvent **un onglet masqué, un filtre qui cache 4 000 lignes, des commentaires, un historique de révisions** ou des métadonnées d'auteur. Le collaborateur envoie ce qu'il voit ; l'outil lit ce qui est là.

Le cas classique : le tableau de bord commercial envoyé pour « faire une synthèse des ventes », avec l'onglet *Salaires_équipe* masqué en position 7. Personne n'a menti. Personne n'a vérifié. **Ouvrir le fichier avant de l'envoyer** — vraiment l'ouvrir, tous les onglets.

7

Documenter les usages autorisés

Une **charte d'une page** — « ce qu'on peut / ce qu'on ne peut pas mettre dans l'IA » — protège mieux que dix slides de théorie. C'est le seul livrable qu'un auditeur, un client ou un DPO vous demandera. Le vôtre est page 11, prêt à signer.

L'OUTIL DE TERRAIN

Le test des 3 questions — cinq secondes, avant chaque envoi

01

Suis-je dans le bon compte ?

Si je ne sais pas répondre en une seconde, je m'arrête et je vérifie.

02

Ce prompt en dit-il plus que nécessaire ?

Un nom propre, un montant exact, un email : chacun doit justifier sa présence.

03

Serais-je à l'aise si ça se retrouvait dans un audit ?

Pas « sur la place publique » — dans un audit. C'est le bon niveau d'exigence.

Trois « oui » : envoyez. **Un seul « je ne sais pas » : c'est un non.**

Le même travail, sans la donnée sensible. Et sans perdre en qualité.

L'objection suivante est toujours la même : « si on enlève les détails, la réponse sera nulle ». Voici pourquoi c'est faux. Cas réel : une relance de facture impayée.

✗ LE PROMPT QUI EXPOSE

« Rédige une relance pour **SOCIÉTÉ MAROCAINE D'INDUSTRIE**, facture **F-2026-1187** de **487 000 Dhs** impayée depuis 62 jours. Contact : **Karim Benjelloun**, **k.benjelloun@smi.ma**, **+212 661 XX XX XX**. Il avait promis un virement le **3 juin**. Notre marge sur ce compte est de **12 %**. »

Ce que vous venez de sortir de l'entreprise : l'identité d'un client, une donnée personnelle de contact, votre encours, votre taux de marge — et la preuve écrite d'un litige commercial en cours.

✓ LE PROMPT QUI TRAVAILLE

« Rédige une relance ferme mais commerciale, en français, ton professionnel marocain. Contexte : **client industriel de longue date**, facture à **6 chiffres**, retard de **62 jours**, **engagement verbal de paiement non tenu il y a 6 semaines**. Enjeu : **obtenir une date ferme sans casser la relation** — le compte est stratégique. Utilise les variables **[CLIENT]**, **[CONTACT]**, **[N°FACTURE]**, **[MONTANT]**, **[DATE_PROMISE]**. »

Qualité de la réponse : identique — souvent meilleure. Le modèle a reçu ce qui pilote vraiment le texte : le **rapport de force**, l'**historique**, l'**objectif** et le **ton**.

LA TROISIÈME ÉTAPE, CELLE QU'ON OUBLIE

Vous recevez un modèle de lettre avec des variables. **Le remplacement des vraies valeurs se fait chez vous** — dans Word, dans votre CRM, dans un publipostage. La donnée sensible n'a jamais quitté votre système d'information. **C'est ça, industrialiser proprement** : le raisonnement sort, les identités restent.

Claude n'a pas besoin de savoir **qui**. Il a besoin de savoir **quoi**.

C'est le passage qui débloque les équipes en formation : elles découvrent que la pseudonymisation n'est pas une contrainte de conformité subie — **c'est une discipline de prompt qui améliore le résultat**, parce qu'elle force à expliciter la situation au lieu de déverser un dossier.

Quelle donnée passe par quelle porte

À afficher près des postes de travail. Un collaborateur ne doit pas avoir à réfléchir : **il doit lire une ligne et savoir.**

Public Déjà publié ou publiable sans nuire	Contenus marketing, plaquettes, offres d'emploi, textes de loi , documentation publique, communiqués. Aucune information non publiée.	PORTE MINIMALE N'importe laquelle
Interne Fuite = gênant, pas grave	Notes de réunion, procédures, organigrammes , supports de formation internes, plannings. Rien de nominatif sensible, rien de chiffré stratégique.	PORTE MINIMALE Team / Entreprise
Confidentiel Fuite = préjudice réel	Contrats, fichier clients , prix et marges, comptes, stratégie, litiges, dossiers RH nominatifs, code source propriétaire.	PORTE MINIMALE Entreprise ou API commercial + pseudonymisation systématique
Réglementé Fuite = sanction + plainte	Données de santé , données personnelles sensibles, secret bancaire , secret professionnel (avocat, expert-comptable, médecin), données de mineurs, biométrie.	PORTE MINIMALE ZDR ou cadre HIPAA + base légale + information des personnes



Au Maroc et en Europe : la porte technique ne suffit pas

Le choix du régime Anthropic règle **l'hébergement et la rétention**. Il ne règle ni la **base légale** du traitement, ni **l'information des personnes concernées**, ni le **transfert hors du pays**. Au Maroc, la **loi 09-08** et la **CNDP** encadrent ces points ; en Europe, c'est le **RGPD**. Deux réflexes suffisent pour être sérieux : **écrire la finalité** de chaque usage IA, et **ajouter l'IA à votre registre des traitements**. C'est une demi-journée de travail — et c'est la différence entre « on utilise l'IA » et « on assume l'usage de l'IA ».

Votre charte d'usage, prête à signer

Dix règles. Une page. C'est le document qui vous protège vraiment — celui que vous pourrez montrer à un client, à un auditeur ou à un juge.

Charte d'usage responsable de l'IA

Applicable à tous les collaborateurs · Version 1.0 · À adapter à votre contexte



- ☒ 1. J'utilise exclusivement le **compte IA fourni par l'entreprise**. Je n'utilise jamais mon abonnement personnel pour un sujet professionnel, même « juste pour dépanner ».
- ☒ 2. Je ne colle **jamais** de mot de passe, clé d'API, coordonnée bancaire, donnée de santé ou pièce d'identité. Sans exception.
- ☒ 3. Avant d'envoyer, je **classe** l'information : public, interne, confidentiel, réglementé — et j'en déduis si j'ai le droit.
- ☒ 4. Je **pseudonymise** par défaut : noms, identifiants, montants sensibles deviennent des variables. Je ré-injecte les vraies valeurs dans le document final, en local.
- ☒ 5. Je **minimise** : je ne donne que le contexte nécessaire à la tâche, jamais le dossier entier « au cas où ».
- ☒ 6. Avant d'uploader un fichier, je **l'ouvre et je le vérifie** : onglets masqués, lignes filtrées, commentaires, métadonnées. J'envoie un extrait, pas un classeur.
- ☒ 7. Je n'utilise **pas le pouce ↑ / ↓** sur une réponse contenant des informations de l'entreprise : ce clic vaut consentement à l'utilisation du contenu.
- ☒ 8. Je reste **responsable du résultat**. Je vérifie les faits, les chiffres et les citations avant tout usage externe. L'IA propose ; je signe.
- ☒ 9. Je ne fais **pas décider l'IA seule** sur une personne : recrutement, sanction, crédit, tarif client. Elle prépare, un humain tranche.
- ☒ 10. En cas de doute, je **demande avant d'envoyer**. Une question coûte deux minutes ; une fuite coûte un client.

Nom et fonction du collaborateur

Date

Signature

Comment s'en servir : ne la diffusez pas telle quelle. Prenez 45 minutes avec votre direction pour **y ajouter vos trois interdits maison** et **nommer un référent IA** qui répond aux doutes. Une charte adoptée en réunion est appliquée ; une charte envoyée par email est archivée.

30 jours pour passer de « on n'ose pas » à « on maîtrise »

SEMAINE 1

L'inventaire

Qui utilise quoi, avec quel compte, sur quelles données ? La réponse honnête surprend toujours la direction.

SEMAINE 2

La porte

Choisir le régime, ouvrir les comptes entreprise, couper l'entraînement partout ailleurs.

SEMAINE 3

La charte + la formation

Une page signée, une session pratique. Sans la formation, la charte n'est qu'un papier.

SEMAINE 4

Un workflow en prod

Un cas réel, livré, sur données réelles et dans le bon cadre. La preuve par l'usage.

CE QUE NOUS FAISONS POUR VOUS

Atelier Décideurs — ½ journée, 8 personnes max

Le cadre posé, la porte choisie, la charte écrite avec vous. Se déduit du Pack si vous continuez.

3 900 Dhs

HT

Formation Équipe — 1 ou 2 jours

Vos équipes, vos cas réels, les réflexes ancrés en pratique. Certifiante.

7 900 / 13 900

Dhs HT

LE PLUS DEMANDÉ

Pack Transformation — 2 jours + 1 workflow livré en production + 30 jours d'accompagnement

On ne vous laisse pas avec des slides : on repart avec un usage qui tourne, dans le bon cadre.

24 900 Dhs

HT

AI Ops en continu — retainer mensuel

Votre équipe IA externalisée : nouveaux workflows, veille réglementaire, mise à jour de la charte.

6 500 Dhs

HT / mois

Financement CSF / OFPPT : nos formations sont éligibles — votre entreprise récupère une grande partie du coût. **Nous fournissons le dossier complet.** Posez-nous la question dès le premier appel.