Eigenflow

GUIDE EIGENFLOW

Les 6 pièges juridiques d'une app faite avec l'IA

Le prompt testé et les vrais textes

PAR

Abyane Nabeebaccus

INSTAGRAM

@abyane_nb

ÉDITION

novembre 2026

Tu as commenté PROMPT. Voici le prompt, ce qu'il a changé sur une app de test, puis chaque piège avec son texte, son chiffre et sa limite.

À savoir avant de lire

- Ce guide vise une app française qui vend à des particuliers. Si tu ne vends qu'à des professionnels, le piège 5 change, et le prompt a besoin de le savoir.

- Il ne remplace pas un avocat. On est une agence d'automatisation : on a lu les textes et testé le prompt, on ne plaide pas.

- Les montants sont des plafonds ou des décisions isolées. Ils ne s'additionnent pas et ne disent pas ce que toi tu paierais.

- Textes relus le 4 novembre 2026. La CNIL annonce sa recommandation sur le rejeu de session pour les prochaines semaines, avec un webinaire le 17 novembre : si tu lis après cette date, revérifie le piège 3.

1. Le prompt

Ouvre Claude Code dans le dossier de ton app, sinon il ne verra ni tes fichiers ni tes requêtes. Colle ça :

> Audite mon site pour la loi française et corrige ce qui peut l'être : 1) consentement des moins de 15 ans (newsletter, cookies) ; 2) polices et scripts chargés depuis Google ou un CDN avant tout clic : héberge-les chez moi ; 3) aucun cookie, pixel ou session replay avant « Accepter », et « Tout refuser » aussi visible ; 4) nom de l'expéditeur et lien de désinscription dans chaque e-mail marketing ; 5) prix, durée et renouvellement juste avant un bouton « Commande avec obligation de paiement », rétractation 14 jours, bouton Résilier ; 6) licences des images, formulaire de signalement, mentions légales. Pour chaque point : statut, preuve, correction. Dis ce que tu ne peux pas vérifier. Ce travail ne remplace pas un avocat.

Il existe une version plus longue. Elle ajoute les pages de rétractation et le rappel avant la reconduction d'un abonnement annuel, et elle interdit à Claude de citer des montants dans sa réponse. Si ton app vend des abonnements, prends celle-ci :

> Voici [le lien de mon site / le code de mon app]. C'est un site ou une app française qui vend à des particuliers [ou : à des professionnels]. Vérifie les six points ci-dessous et corrige dans le code tout ce qui peut l'être. Règles de travail : - Pour chaque point, donne un statut : conforme, à corriger, ou impossible à vérifier d'ici. Montre la preuve : fichier et ligne, ou requête réseau. - Si tu n'as que le lien et aucun moyen d'ouvrir la page et de voir ses requêtes réseau, dis-le et demande-moi le code. - Ne cite aucun article de loi absent de cette liste et ne donne aucun montant d'amende. Ce travail ne remplace pas un avocat : à la fin, liste les questions à lui poser. 1. Mineurs. Repère ce qui repose sur le consentement (newsletter, cookies non essentiels, publicité, profil public). En France, sous 15 ans, ce consentement exige aussi celui d'un parent (art. 45 de la loi Informatique et Libertés). Dis-moi si des moins de 15 ans peuvent s'inscrire et propose une solution : question d'âge avec accord parental, ou service réservé aux 15 ans et plus. Si je vends, rappelle-moi qu'une case « j'ai 18 ans » ne protège pas un contrat (art. 1149 du Code civil). 2. Ressources externes. Liste tout ce que la page charge depuis un autre domaine avant le moindre clic (Google Fonts, CDN, scripts, vidéos, cartes). Héberge les polices sur mon serveur et retire ce qui ne sert à rien. 3. Traceurs. Liste les cookies, le localStorage et les pixels posés au chargement. Rien qui ne soit strictement nécessaire avant le consentement (art. 82 de la loi Informatique et Libertés). Mets un bandeau où « Tout refuser » est aussi visible que « Tout accepter ». Coupe le session replay (Hotjar, Clarity, PostHog ou autre) ou place-le derrière le consentement, avec tous les champs de saisie masqués. 4. E-mails. Le formulaire d'inscription doit avoir une case non cochée pour recevoir des e-mails commerciaux. Chaque e-mail marketing doit indiquer qui l'envoie et contenir un lien de désinscription qui marche en un clic, sans compte (art. L34-5 du Code des postes et des communications électroniques). Vérifie qu'une personne désinscrite ne reçoit plus rien. Coupe le suivi d'ouverture tant que je n'ai pas le consentement. 5. Paiement et abonnement. Juste avant le bouton de paiement : prix, durée, renouvellement automatique, durée minimale. Le bouton dit « Commande avec obligation de paiement » ou une formule aussi claire (art. L221-14 du Code de la consommation). Ajoute l'information sur les 14 jours de rétractation, une case de demande expresse si le service démarre tout de suite, un bouton pour se rétracter en ligne et un bouton « Résilier » facile à trouver. Si l'abonnement est

annuel avec reconduction tacite, prépare l'e-mail de rappel à envoyer entre 3 mois et 1 mois avant l'échéance (art. L215-1 du même code). 6. Contenus. Liste les images du site et leur source, et signale celles dont je ne peux pas prouver la licence. Si mes utilisateurs publient des contenus, ajoute un formulaire de signalement et une adresse de contact visibles. Vérifie la page de mentions légales : éditeur, adresse, téléphone, numéro d'immatriculation, directeur de la publication, hébergeur (art. 1-1 de la loi pour la confiance dans l'économie numérique). À la fin : ce que tu as corrigé (avec le diff), ce qui reste à faire, ce que tu n'as pas pu vérifier, et les questions pour un avocat.

Ce que ce prompt ne fait pas :

- Il voit le code et la page. Les consentements déjà recueillis, un fichier d'adresses acheté ou un contrat signé lui échappent.

- Il signale une image sans source. Prouver une licence reste ton travail.

- Avec un simple lien et sans navigateur, il ne voit ni les cookies ni les requêtes réseau. Donne-lui le code.

2. Ce qu'il a changé sur notre app de test

Le 25 octobre 2026, on a fabriqué Forma, une fausse app de sport par abonnement, avec les six pièges dedans. Un agent Claude neuf (Opus 5.5), seul dans une copie du dossier, a reçu le prompt court mot pour mot.

Résultat : les six pièges trouvés, cinq corrigés dans le code, le sixième à compléter par le propriétaire (infos de la société, licences des images). 1 159 lignes de modifications sur 17 fichiers. La version longue a fait 1 354 lignes sur 24 fichiers.

Le formulaire, avant :

Le même après le prompt. Date de naissance obligatoire, âge recalculé côté serveur, case décochée :

Il a aussi laissé des décisions au propriétaire : choisir entre « 7 jours gratuits » et « premier mois offert », promis tous les deux sans rien derrière, et écrire l'e-mail de confirmation après paiement.

Limite du test : une seule app, faite exprès, et aucun avocat n'a relu le résultat.

3. Piège 1 : le formulaire qui ne demande jamais l'âge

En France, sous 15 ans, un traitement fondé sur le consentement n'est licite que si le mineur et un titulaire de l'autorité parentale consentent tous les deux. C'est l'article 45 de la loi Informatique et Libertés.

La newsletter, c'est notre lecture : la CNIL prend pour exemples le profil public et la géolocalisation. Un site qui ne vise que des adultes en B2B est dans une zone grise qu'on n'a pas su trancher.

Une case « j'ai 18 ans » ne te protège pas. L'article 1149 du Code civil dit que la simple déclaration de majorité faite par le mineur n'empêche pas l'annulation. Annulable ne veut pas dire annulé : un acte courant à des conditions normales reste valable, et il faut que le mineur le demande.

Ce que fait le prompt : date de naissance ou service réservé aux 15 ans et plus, case décochée.

4. Piège 2 : les polices chargées depuis Google

Quand ta page appelle fonts.googleapis.com, le navigateur du visiteur envoie son adresse IP à Google avant le moindre clic.

Le 20 janvier 2022, le tribunal régional de Munich (LG München I, 3 O 17493/20) a condamné un site à verser 100 € plus intérêts à un visiteur, et lui a interdit de recommencer sous peine d'une astreinte pouvant aller jusqu'à 250 000 € par infraction. Son raisonnement : la police pouvait être hébergée sur place, donc aucun intérêt légitime.

Limite : c'est un jugement allemand de première instance, sans portée directe en France. Le RGPD est le même des deux côtés. On n'a pas trouvé de trace d'appel, sans pouvoir l'exclure.

Ce que fait le prompt : il liste ce qui part vers un autre domaine et héberge les polices chez toi. Ça prend quelques minutes et ça ne coûte rien.

5. Piège 3 : les stats qui rejouent la session

Un outil de rejeu reconstitue le parcours du visiteur : souris, clics, saisies. La CNIL le décrit ainsi sur sa propre page.

Son projet de recommandation du 25 février 2026 dit que ces outils sont soumis au consentement préalable. C'est encore un projet, sans valeur réglementaire : la consultation a fermé le 22 avril et l'adoption est annoncée. Son outil d'auto-évaluation de juillet 2025 va dans le même sens : pour rester exempté de consentement, un outil de mesure d'audience doit désactiver le rejeu.

Sur les mots de passe : la plupart des outils les masquent par défaut, et le prompt demande de masquer tous les champs. Vérifie le réglage du tien.

Pour les cookies, la CNIL sanctionne déjà. En procédure simplifiée, réservée aux dossiers sans difficulté juridique et plafonnée à 20 000 €, les amendes cookies relevées vont de 2 000 € (décembre 2025) à 20 000 € (décembre 2024 et octobre 2025).

Hors de cette procédure, on change d'échelle : 7 millions d'euros contre Fnac Darty et Fnac Direct, décision du 22 octobre 2026, pour un traceur sans consentement dans une appli mobile.

Ce que fait le prompt : rien avant le choix du visiteur, « Tout refuser » aussi visible que « Tout accepter ».

6. Piège 4 : l'e-mail « on est en ligne »

L'article L34-5 du Code des postes et des communications électroniques impose un moyen de s'opposer à la prospection. L'amende prononcée par la répression des fraudes (DGCCRF) peut atteindre 75 000 € pour une personne physique et 375 000 € pour une société. La CNIL peut aussi sanctionner ces faits, avec ses propres plafonds.

Ça tient encore malgré la décision du Conseil constitutionnel du 25 juin 2026 (2026-1210 QPC). Elle reporte l'abrogation au 31 octobre 2027, et jusque-là une seule autorité peut poursuivre un même fait.

Un cas réel : dans sa décision SAN-2020-008, la CNIL a retenu un manquement pour un seul courriel, envoyé par erreur à plus de 350 000 personnes. Le lien de désinscription menait à la page de connexion d'un compte client, et les destinataires sans compte ne pouvaient pas s'opposer. L'amende de 2,25 millions d'euros couvrait tout le dossier, cet e-mail n'en était qu'une petite partie.

Correction : notre vidéo du 25 octobre parlait d'un « lien cassé ». C'était inexact, le lien marchait mais demandait un compte.

L'e-mail de Forma, avant :

Le prompt ajoute l'identité de l'expéditeur et un lien de désinscription en un clic, sans compte :

7. Piège 5 : le bouton de paiement

Pour un consommateur, le bouton de commande doit dire « commande avec obligation de paiement » ou une formule analogue (article L221-14 du Code de la consommation). Sinon le contrat encourt la nullité (article L242-2). Il peut être annulé, ça ne se fait pas tout seul.

Le bouton de Forma avant le prompt disait « Payer », sans renouvellement écrit à côté :

Après, le récapitulatif donne le prix, la durée, le renouvellement, la résiliation et la rétractation juste avant le bon bouton :

Le droit de rétractation pèse encore plus lourd. Si tu n'en informes pas ton client particulier, ses 14 jours sont prolongés de 12 mois (article L221-20). Et en principe, il ne te doit rien pour le service déjà utilisé s'il se rétracte : c'est la lecture de la Cour de justice de l'Union européenne dans l'arrêt C-97/22, rendu sur un contrat hors établissement. L'étendre à une vente en ligne passe par la même directive, c'est une extension de lecture.

Depuis le 19 juin 2026, un bouton de rétractation en ligne est aussi attendu (article L221-21, relu le 25 octobre).

8. Piège 6 : les images et les mentions légales

Le 22 juin 2023, le tribunal judiciaire de Paris (RG 23/04240) a jugé la reprise d'une seule photo sur un site, restée en ligne environ 17 mois, sans autorisation ni nom de l'auteur. Total : 1 500 € de préjudice patrimonial, 1 500 € de préjudice moral, 1 000 € de préjudice collectif et 5 000 € de frais de procédure, soit 9 000 €. Les dépens s'ajoutent. Le jugement est réputé contradictoire, les défendeurs n'étaient pas représentés.

Pour les mentions légales, l'article 1-2 de la loi pour la confiance dans l'économie numérique prévoit jusqu'à un an de prison et 75 000 € d'amende pour une personne physique ou un dirigeant. L'obligation naît à la publication, donc avant ta première vente.

C'est le plafond de notre accroche, et il faut le lire comme un plafond. Les décisions qu'on a trouvées, à travers des résumés de cabinets d'avocats qu'on n'a pas pu vérifier à la source, tournent autour de 5 000 à 6 000 €. On n'a trouvé aucune condamnation proche du maximum.

Le prompt crée la page et surligne ce qu'il ne peut pas inventer. Ces champs restent à toi :

9. Les questions à poser à ton avocat

- Mon app s'adresse-t-elle à des mineurs au sens de l'article 45, et comment recueillir l'accord d'un parent sans collecter trop de données ?

- Ma liste d'attente vaut-elle consentement à la prospection, et pour combien de temps ?

- Mes prestataires américains (polices, statistiques, envoi d'e-mails) sont-ils couverts par un transfert valable ?

- Mes CGV et mon parcours de rétractation tiennent-ils pour mon type de service ?

- Pour chaque image, quelle licence puis-je prouver ?

Sources

Relu le 4 novembre 2026, sauf mention contraire. Légifrance bloque les lectures automatiques : ses articles ont été vérifiés sur extraits, avec leur mention de version.

- [Article 45 de la loi Informatique et Libertés](https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037823135) et [la recommandation 4 de la CNIL](https://www.cnil.fr/fr/recommandation-4-rechercher-le-consentement-dun-parent-pour-les-mineurs-de-moins-de-15-ans).

- [Article 1149 du Code civil](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032041050/).

- [LG München I, 20/01/2022, 3 O 17493/20](https://www.gesetze-bayern.de/Content/Document/Y-300-Z-GRURRS-B-2022-N-612).

- [Le webinaire de la CNIL sur le rejeu de session](https://cnil.fr/fr/evenement/webinaire-recommandation-outils-rejeu-de-session), [le projet de recommandation](https://www.cnil.fr/sites/default/files/2026-02/projet_de_recommandation_rejeu_session.pdf) et [l'outil d'auto-évaluation](https://www.cnil.fr/sites/default/files/2025-07/outil_d_auto-evaluation_mesure_d_audience.pdf).

- [La liste des sanctions de la CNIL](https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil), [le bilan des sanctions simplifiées](https://cnil.fr/fr/23-nouvelles-sanctions-simplifiees) et [la sanction Fnac](https://www.cnil.fr/fr/sanction-cookies-app-fnac).

- [Article L34-5 du CPCE](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042155961/), [la décision 2026-1210 QPC](https://www.conseil-constitutionnel.fr/decision/2026/20261210QPC.htm) et [la décision SAN-2020-008](https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756).

- [Article L221-14](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032226854), [L242-2](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032226382), [L221-20](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000044563199) et [L221-25](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000044563179) du Code de la consommation, et [l'arrêt C-97/22](https://www.droit-technologie.org/wp-content/uploads/2023/05/CURIA-Arret-rendu.pdf).

- [Le jugement du TJ de Paris du 22/06/2023](https://www.legifrance.gouv.fr/juri/id/JURITEXT000047878978).

- [Articles 1-1](https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000049568614) et [1-2 de la LCEN](https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000049568616).

- Le test : deux agents Claude neufs du 25/10/2026 sur l'app Forma, diffs dans notre dossier de production.

- Script d'origine : le reel d'adilet.fndr, adapté au droit français.