cestly

Politique de confidentialité

Liste d’attente Cestly

dernière mise à jour : 5 novembre 2026

Dernière modification : Le cookie de contrôle dure 90 jours au maximum. Historique des modifications

cestly.app/confidentialite · Version 2026-11-05.6

Cette page explique comment nous traitons les données que vous fournissez en rejoignant la liste d’attente de Cestly ou en utilisant le formulaire de contact. Nous collectons le strict minimum. Nous n’utilisons ni outils d’analyse, ni mesure d’audience, ni publicité.

Responsable

Le responsable du traitement est **Lucas Ezequiel Palma**, personne physique qui dirige le projet Cestly depuis l’Andorre. Cette personne relève de la loi qualifiée andorrane 29/2021 sur la protection des données personnelles (LQPD). Le règlement général sur la protection des données de l’UE (RGPD) peut aussi s’appliquer si nous adressons intentionnellement notre offre à des personnes situées dans l’UE. Le fait que le site soit accessible depuis l’UE, gratuit ou en prélancement ne suffit pas, à lui seul, à trancher cette question.

Nous n’avons pas désigné de représentant dans l’UE. Avant d’y orienter le lancement ou nos campagnes, nous terminerons d’analyser si le RGPD s’applique. Si son article 27 l’exige, nous publierons ici les coordonnées de ce représentant. Nous n’avons pas non plus désigné de délégué à la protection des données (DPD). Motif : le périmètre actuel ne comprend ni décision automatisée produisant des effets juridiques, ni traitement à grande échelle de catégories particulières, ni aucun autre traitement massif à haut risque. Nous réévaluerons ce point avant tout changement important.

Pour exercer vos droits ou nous poser une question sur la confidentialité, écrivez à privacy@cestly.app ou utilisez la page de désinscription et de contact (cestly.app/desinscription).

Données collectées

- **Liste d'attente** : l'adresse e-mail et la case de consentement sont obligatoires ; sans elles, nous ne pouvons pas enregistrer l'inscription ni vous prévenir du lancement. En cochant la case, vous déclarez avoir 16 ans ou plus. Pour prouver votre consentement, nous conservons aussi la version de cette politique en vigueur lors de votre inscription et la date d'inscription. Dans le même but, nous conservons aussi la date du dernier e-mail de confirmation envoyé, ainsi que la date et le mode de votre confirmation. Les inscriptions faites avant la mise en place de cette confirmation par e-mail, pour lesquelles la case de consentement a été cochée, sont enregistrées comme confirmées à leur date d'inscription.
- **Langue et pays** : la langue du site et votre pays (code à 2 lettres). Le pays est déduit de votre connexion, *sans que nous conservions votre adresse IP*.
- **Contact** : l'adresse e-mail, le type de demande et le message sont obligatoires ; sans eux, nous ne pouvons ni recevoir la demande, ni l'acheminer, ni y répondre. N'indiquez aucune donnée de santé ou biométrique, croyance, orientation sexuelle ni autre information particulièrement sensible.

Finalité et base juridique

Pour la liste d'attente, nous utilisons vos données afin de **gérer votre inscription et de vous prévenir du lancement**. La base juridique est votre **consentement**, que vous donnez explicitement en cochant la case du formulaire et que vous pouvez retirer à tout moment. Avant de vous inscrire, nous vérifions que l'adresse vous appartient : nous vous envoyons un e-mail de confirmation et l'inscription reste en attente jusqu'à ce que vous ouvriez son lien et sélectionniez le bouton de confirmation sur notre site. Ouvrir le lien ne suffit pas : un programme qui analyse vos e-mails ne peut donc pas

vous inscrire. Vous pouvez aussi saisir sur notre site le code à 6 chiffres de ce même e-mail, valable 24 heures. Si vous vous désinscrivez puis vous réinscrivez, vous devrez confirmer à nouveau.

Si vous utilisez le formulaire pour une question générale, nous traitons l'adresse e-mail et le message afin de la recevoir, de la gérer et d'y répondre. La base juridique est notre intérêt légitime à répondre à la demande dont vous êtes à l'origine.

Si vous exercez un droit relatif à la protection des données, nous traitons les informations nécessaires pour vérifier votre identité de manière proportionnée. Nous traitons aussi celles nécessaires pour instruire la demande, documenter la décision et répondre. La base juridique est le respect de nos obligations légales.

Nous traitons des signaux techniques de sécurité, des identifiants pseudonymisés de tentatives et des événements d'audit afin de prévenir les abus et de protéger le service. Nous les traitons aussi pour démontrer les opérations réalisées et pouvoir nous défendre en cas de litige. La base juridique est notre intérêt légitime à maintenir un service sûr et responsable, avec minimisation et durées de conservation spécifiques.

Conservation

Les données de la liste d'attente quittent l'usage courant après 24 mois, ou plus tôt si vous vous désinscrivez ou si la finalité prend fin. Si vous ne confirmez pas votre adresse, l'inscription quitte l'usage courant 7 jours après le dernier e-mail de confirmation. Les messages de contact, y compris les demandes de confidentialité, et l'adresse e-mail associée le quittent après 12 mois.

À leur sortie de l'usage courant, toutes ces données sont bloquées. Elles passent dans un coffre chiffré, séparé de la base active, limité à la juridiction de données de l'UE et invisible depuis l'espace d'administration. Dès lors, elles ne peuvent être mises qu'à la disposition des tribunaux, du ministère public, des administrations compétentes ou de l'APDA. Cette mise à disposition a pour seul objet la mise en jeu d'éventuelles responsabilités découlant du traitement. La base juridique du blocage est l'obligation légale

prévue à l'article 30 de la LQPD. En règle générale, la destruction est prévue 36 mois après le blocage. Ce n'est pas un délai légal universel : une réclamation, une action formelle ou une procédure peut le modifier. Après expiration de tous les délais applicables, et en l'absence de toute obligation légale de les conserver, nous les supprimons des systèmes en service. Nous ne considérons pas leur destruction comme achevée tant qu'une copie technique de récupération peut les réintroduire. En cas de restauration, le service reste fermé, maintient le blocage et applique de nouveau la suppression. En outre, Cloudflare permet de récupérer la base de données telle qu'elle était jusqu'à 7 jours auparavant.

Pour identifier les nouvelles tentatives et les restaurations, le coffre conserve pendant 30 jours un reçu HMAC pseudonymisé. Il reprend la référence de l'opération, la date de la destruction, la politique et la version de clé. Il ne contient ni adresse e-mail ni message et ne permet pas de les reconstituer à lui seul. Il peut ensuite être purgé. Ce reçu est pseudonymisé, pas anonyme. Les métadonnées techniques d'audit, minimisées, ont leur propre durée maximale de conservation : 36 mois. L'alerte facultative que nous recevons dans notre messagerie professionnelle (Google) lorsque vous écrivez via le formulaire est générique et ne contient ni votre adresse e-mail ni votre message. Nous ne promettons pas que Gmail la supprime automatiquement. Si le produit n'est pas lancé, nous bloquerons la liste, puis la détruirons de la même manière.

Brouillon dans cet onglet

Si, depuis le formulaire, vous ouvrez l'une des pages juridiques ou changez de langue dans le même onglet, nous conservons temporairement l'adresse e-mail saisie et la langue. Nous les conservons dans le stockage de session de cet onglet (sessionStorage). Cela sert uniquement à restaurer ce que vous aviez saisi : ce brouillon n'est ni envoyé à nos serveurs ni inclus dans l'URL. Le consentement n'est pas conservé. Le brouillon est supprimé à sa restauration, une fois l'inscription bien envoyée ou après 30 minutes. Si le navigateur suspend la page, les brouillons expirés sont supprimés à votre retour. La limite de 30 minutes ne concerne que cette copie enregistrée : nous ne vidons pas le champ e-mail du formulaire que votre navigateur garde

ouvert. Si le navigateur ne conserve pas ce formulaire et qu'aucun brouillon valide n'est disponible, vous devrez saisir à nouveau votre adresse e-mail. Un brouillon peut manquer parce qu'il a expiré ou que le stockage est bloqué. Après l'envoi de l'inscription, la page garde votre adresse uniquement en mémoire, pour les boutons « Renvoyer l'e-mail » et « Corriger l'adresse ». Elle ne l'enregistre pas sur votre appareil.

Tickets techniques et nouvelles tentatives

Lorsqu'une inscription à la liste d'attente, une prise de contact ou une désinscription commence, ce site obtient un ticket signé pour cette action. Il conserve aussi temporairement dans le sessionStorage de l'onglet le ticket, son UUID aléatoire et un horodatage. Le ticket identifie Cestly, l'action et sa durée de validité ; il ne contient ni adresse e-mail, ni message, ni profil. Il autorise une nouvelle opération pendant 10 minutes. Si le résultat est incertain, le même onglet peut le conserver jusqu'à 24 heures uniquement pour faire correspondre cette même demande. Il est supprimé plus tôt si la demande est confirmée ou définitivement rejetée, ou à la fermeture de l'onglet. Le serveur conserve pendant 24 heures un reçu comprenant des références HMAC pseudonymisées de la demande et de son contenu normalisé. Le reçu comprend aussi l'action, l'état et les horodatages. Il y est noté si la première réponse annonçait un e-mail, afin qu'une nouvelle tentative de cette même demande reçoive la même réponse. Ce reçu ne conserve ni le ticket, ni l'UUID en clair, ni l'adresse e-mail, ni le message. La purge quotidienne le supprime ensuite. Ces références sont pseudonymisées, pas anonymes.

Si vous ouvrez le lien de confirmation ou de désinscription reçu par e-mail, ce site le retire de la barre d'adresse. Il conserve le lien et, lors de la confirmation, le résultat dans l'historique de cet onglet (history.state). Ainsi, vous ne perdez pas l'étape si vous rechargez la page, revenez en arrière ou changez de langue. Ces données restent uniquement dans cet onglet, et ce site ne s'en sert que pour reprendre l'étape.

Cookie technique de contrôle de la liste

Après une tentative d'inscription, nous pouvons déposer notre propre cookie technique de contrôle. Il est strictement nécessaire. Depuis ce navigateur, il vous permet de vous désinscrire sans lien. Il vous permet aussi de vous réinscrire en mettant à jour votre inscription (la langue, le pays et la version de la politique). Personne d'autre ne peut le faire en connaissant seulement votre adresse e-mail. Si vous vous réinscrivez depuis ce navigateur et qu'aucun autre e-mail ne peut être envoyé à cette adresse pour l'instant, ce site vous le dit. Sans ce cookie, il ne dit rien. Lorsque nous donnons accès à une inscription réelle, le nom du cookie est dynamique : il commence par __Host-cestly-waitlist-control- et se termine par l'UUID aléatoire de cet accès. Lorsque la réponse ne peut pas donner accès à une inscription existante, nous pouvons déposer un cookie factice, identique en apparence au vrai. Son nom est aléatoire et se répète si vous relancez la même demande. Ainsi, nous ne révélons pas si l'adresse est inscrite. Les deux types de cookies sont limités au domaine cestly.app, Secure, HttpOnly et SameSite=Strict ; JavaScript ne peut pas les lire. Le jeton contient un UUID aléatoire et ses horodatages authentifiés d'émission (iat) et d'expiration (exp), jamais l'adresse e-mail ni un dérivé réversible. Le cookie et le jeton durent au maximum 90 jours, et le serveur vérifie la signature et l'expiration avant de l'accepter. Ils ne sont utilisés ni pour l'analyse, ni pour la publicité, ni pour le suivi intersite, et ne sont communiqués qu'aux sous-traitants qui font fonctionner ce site. Cette section vous informe de leur caractère strictement nécessaire et de leur fonctionnement. Vous pouvez les supprimer dans votre navigateur. Si vous supprimez le cookie qui donne accès à votre inscription, vous ne pourrez plus vous désinscrire ni mettre à jour votre inscription depuis ce navigateur sans lien. Vous pourrez toutefois toujours utiliser « Demande relative à mes données » ou écrire à privacy@cestly.app.

Destinataires

Cloudflare (Cloudflare, Inc., des États-Unis) traite des données pour notre compte afin d'héberger le site, de l'exécuter et de recevoir les formulaires, via Workers, D1 et Queues. Via Email Routing, il reçoit aussi la copie de l'e-mail direct qui sert à préparer l'accusé de réception. Workers peut

s'exécuter dans n'importe quel centre de données de Cloudflare dans le monde, généralement le plus proche de votre connexion. La base de données D1 se trouve aujourd'hui en Europe de l'Ouest (WEUR), mais elle n'est pas limitée à la juridiction de données de l'UE. Queues (dans son offre gratuite) reçoit un UUID de notification, généré à part à cette fin. Il arrive dans une enveloppe technique identique pour tous les messages (la version du format et le type d'événement), sans adresse e-mail, message ni type de demande. Queues le conserve jusqu'à 24 heures. Cloudflare publie son contrat de sous-traitance (DPA) (https://www.cloudflare.com/cloudflare-customer-dpa/) et la liste de ses sous-traitants ultérieurs (https://www.cloudflare.com/gdpr/subprocessors/cloudflare-services/). Les transferts vers les États-Unis reposent sur les clauses contractuelles types de l'UE de ce DPA ; vous pouvez nous en demander une copie à privacy@cestly.app. Pour horodater le journal d'audit, nous envoyons aux calendriers publics d'OpenTimestamps un condensat cryptographique sans données personnelles.

L'alerte facultative envoyée pour chaque nouveau message du formulaire de contact utilise **Google Workspace et Google Apps Script**. Nous ne l'activons qu'après avoir accepté, au niveau du compte, l'avenant de Google relatif au traitement des données (CDPA, selon son sigle anglais) (https://knowledge.workspace.google.com/admin/compliance/privacy-compliance-and-records-for-google-workspace-and-cloud-identity). Nous ne l'activons également qu'après avoir documenté l'entité contractante, les sous-traitants ultérieurs (https://workspace.google.com/terms/subprocessors/) et les garanties de transfert international. Cet e-mail d'alerte est générique : il ne contient ni votre adresse e-mail, ni votre message, ni l'UUID, ni la date. Nous ne nous fondons pas uniquement sur le cadre de protection des données UE-États-Unis pour protéger les personnes en Andorre. Vous pouvez demander la référence ou une copie des garanties applicables via notre canal de confidentialité.

Détail technique de l'alerte facultative : pour la générer, ce site n'envoie à Google que cet UUID de notification (event_id), le nom du site et le type de demande. L'enveloppe technique de cet envoi ajoute la version, l'identifiant de clé, un horodatage, un nombre aléatoire à usage unique et la signature

HMAC. Apps Script programme la suppression de l'empreinte de l'UUID après 70 heures. L'heure et le type de demande de l'alerte peuvent être indirectement rapprochés du message conservé dans D1. C'est le cas pendant les 12 mois de conservation du message, et jusqu'à la purge quotidienne suivante (moins de 24 heures plus tard, tant que la tâche planifiée fonctionne normalement).

Via **Google Workspace** (Google Cloud EMEA Limited, en Irlande), le fournisseur de notre messagerie professionnelle, soumis au même CDPA, nous envoyons ces e-mails depuis support@cestly.app :

- la confirmation d'inscription (aussi lorsque vous sélectionnez « Renvoyer l'e-mail ») ;
- l'e-mail « Vous êtes déjà sur la liste d'attente », lorsque quelqu'un saisit de nouveau une adresse déjà confirmée ;
- le lien de confirmation de désinscription ;
- l'accusé de réception du formulaire de contact, qui ne porte qu'une référence neutre, sans aucune donnée de votre message ;
- l'accusé de réception des e-mails que vous nous écrivez à support@ ou privacy@.

Ces e-mails sont préparés par ce site. **Supabase** (Supabase Pte. Ltd., de Singapour), le fournisseur de serveurs de nos apps, les remet à Google principalement depuis sa région de l'UE (Francfort), sans les conserver. Supabase publie son DPA (https://supabase.com/legal/dpa) et la liste de ses sous-traitants ultérieurs (https://supabase.com/legal/subprocessors). Les transferts vers Singapour reposent sur les clauses contractuelles types de l'UE de ce DPA ; vous pouvez nous en demander une copie à privacy@cestly.app. Google reçoit votre adresse, la langue, les liens signés, le code de confirmation et, dans l'accusé de réception d'un e-mail direct, l'objet de votre e-mail. Nous ne gardons aucune copie de ces e-mails dans nos boîtes aux lettres, et Google conserve des journaux techniques de remise conformément à son CDPA. Nous ne vendons pas vos données et ne les partageons pas à des fins commerciales.

E-mail direct à support@ et privacy@

Si vous choisissez d'écrire directement à privacy@cestly.app ou à support@cestly.app au lieu d'utiliser le formulaire, votre service de messagerie transmet à **Google Workspace** votre adresse. Il transmet aussi tout ce que vous incluez : objet, corps, signature et pièces jointes. Nous utilisons ce contenu uniquement pour recevoir, traiter et documenter la demande, et pour y répondre. La base juridique est le respect de nos obligations légales lorsque vous exercez un droit et notre intérêt légitime pour une question générale. Ce contenu n'est pas utilisé à des fins de marketing. Nous supprimons chaque message direct, avec notre réponse, lors de la première revue mensuelle une fois écoulés 365 jours depuis sa réception. Avant cela, nous en gardons une copie chiffrée, hors de la messagerie, bloquée comme le reste de ces données. Elle ne peut être mise qu'à la disposition des tribunaux, du ministère public, des administrations compétentes ou de l'APDA. En règle générale, nous la détruisons au bout de 36 mois. Seule une obligation légale ou fiscale documentée de le conserver peut reporter cette suppression, et ces exceptions sont vérifiées lors de cette même revue mensuelle. Une fois la suppression irréversible, le CDPA (https://cloud.google.com/terms/data-processing-addendum) permet à Google d'achever l'effacement des données dans ses systèmes dès que cela est raisonnablement possible. Le délai maximal qu'il permet est de 180 jours, sauf obligation légale. N'incluez pas de données particulièrement sensibles ni de pièces jointes sauf si elles sont strictement nécessaires ; le formulaire est la voie qui collecte le moins de données.

À la réception de votre e-mail à l'une ou l'autre adresse, nous vous envoyons un accusé de réception automatique pour que vous sachiez qu'il est bien arrivé. Pour le préparer, une copie passe par **Cloudflare** (Email Routing et l'un de nos Workers). Il la lit uniquement pour vérifier qu'il ne s'agit ni d'un envoi automatique ni d'un expéditeur usurpé, voir dans quelle langue vous avez écrit et en reprendre l'objet. L'accusé de réception vous parvient ainsi dans le même fil. La copie est ensuite supprimée et son texte n'est conservé nulle part. Chaque nouvel e-mail reçoit son accusé de réception (pas les réponses dans une même conversation), jusqu'à 10 par personne et par heure. Il en reste deux traces. D'une part, des compteurs pseudonymisés qui

empêchent les boucles entre machines et sont supprimés en moins de 2 jours. D'autre part, le journal d'activité d'Email Routing. Cloudflare y enregistre, pour chaque copie, la date et l'heure, l'expéditeur, le destinataire, l'objet et l'identifiant du message. Il y enregistre aussi le résultat de ses contrôles d'authenticité et anti-spam. Il conserve ce journal 31 jours. Nous ne le consultons que depuis notre compte Cloudflare, pour vérifier que l'accusé de réception fonctionne ou enquêter sur un abus. La base juridique de ce traitement est notre intérêt légitime. Cet intérêt consiste à vous confirmer que votre e-mail est bien arrivé, sans que quiconque puisse utiliser l'accusé de réception pour écrire à des tiers.

Langue du site

Chaque langue a sa propre adresse : cestly.app est la version espagnole, et /en, /ca, /fr et /pt, les autres. L'adresse fixe la langue et vous la changez avec le sélecteur. Ce n'est que si l'adresse ne l'indique pas (par exemple, pour une page qui n'existe pas) que le site utilise la première langue compatible de votre navigateur. Ce choix se fait **sur votre appareil**. Nous n'enregistrons pas la langue de façon permanente sur votre appareil (seulement dans le brouillon de l'onglet, expliqué plus haut) et n'utilisons pas la géolocalisation.

Protection contre les robots

Pour empêcher les robots d'envoyer les formulaires (inscription, contact et désinscription), nous utilisons notre propre **preuve de travail**. Votre navigateur résout un petit calcul lié à cet envoi et notre serveur le vérifie. Elle n'utilise pas de cookies, n'analyse pas votre navigateur et n'envoie aucune donnée à des tiers. Pour limiter les abus des formulaires d'inscription et de contact, nous conservons dans D1 une référence HMAC pseudonymisée de l'adresse IP, jamais l'adresse IP en clair. Nous conservons aussi, avec le même mécanisme, une référence HMAC pseudonymisée de l'adresse e-mail. Elle sert pour les e-mails d'inscription, la page de désinscription et l'accusé de réception du formulaire de contact. Nous la conservons, que l'adresse figure ou non sur la liste, mais jamais l'adresse en clair. Avec elle, nous limitons ce que nous envoyons à chaque adresse. Toutes les 24 heures, au plus 3 e-mails de confirmation d'inscription (le premier compris) et 1 e-mail

« Vous êtes déjà sur la liste d'attente ». Toutes les 10 minutes, 3 liens de désinscription (et 5 toutes les 24 heures). Toutes les heures, 3 accusés de réception (et 6 toutes les 24 heures). Pour l'accusé de réception et le code de confirmation, nous conservons en outre, avec le même mécanisme, une référence qui combine l'adresse e-mail et l'adresse IP. Ainsi, le site n'indique que ce qui a été fait depuis votre adresse IP. Cela représente au plus 3 accusés de réception toutes les heures et 5 tentatives de saisie du code toutes les 24 heures. Il n'indique jamais ce qui a été fait avec cette adresse e-mail depuis d'autres adresses IP. Toutes adresses IP confondues, nous autorisons pour chaque adresse e-mail au plus 10 tentatives de saisie du code toutes les 24 heures. Chaque référence peut être supprimée après 24 heures. La purge quotidienne la supprime lors de son exécution suivante, moins de 24 heures plus tard tant que la tâche planifiée fonctionne normalement. La preuve de travail, les limites de tentatives et les contrôles automatisés décident seulement si un envoi précis est techniquement accepté. Ils ne font pas de profilage, ne décident de rien concernant le futur service et ne produisent pas d'effets juridiques ni d'effets similaires vous affectant. En cas de faux positif, réessayez ou écrivez à privacy@cestly.app.

Vos droits

Vous pouvez vous **désinscrire**, exercer vos droits (accès, rectification, effacement, opposition, limitation et portabilité) et retirer votre consentement en écrivant à privacy@cestly.app ou via notre page de désinscription et de contact (cestly.app/desinscription). Vous pouvez demander par le même canal une copie de notre registre des activités de traitement. Vous pouvez aussi saisir l'Agence andorrane de protection des données (APDA) (https://www.apda.ad/) et, le cas échéant, l'autorité de contrôle du pays de votre résidence habituelle. Le service ne s'adresse pas aux moins de 16 ans : ils ne doivent utiliser ni la liste ni le formulaire de contact sans l'autorisation de leur représentant légal. Si nous détectons un envoi émanant d'un mineur, nous limiterons le traitement à la vérification proportionnée de cette autorisation ou à la suppression de cet envoi ; le mineur et son représentant conservent leurs droits.

Vous pouvez vous désinscrire depuis n’importe quel appareil. L’e-mail de confirmation d’inscription et l’e-mail « Vous êtes déjà sur la liste d’attente » contiennent votre lien de désinscription signé. Sur la page de désinscription, si vous saisissez votre adresse e-mail, nous vous envoyons un lien pour confirmer la désinscription. Les liens de désinscription continuent de fonctionner même une fois leur délai écoulé (730 jours pour les liens actuels), tout comme le bouton de désinscription de votre messagerie. Si vous ouvrez la page depuis l’un de ces liens, nous indiquons quelle adresse quittera la liste, en partie masquée. Si ce navigateur conserve encore l’identifiant technique de l’inscription, la désinscription s’exécute sans lien. Dans les deux cas, la réponse de la page est générique : elle ne révèle pas si l’adresse était inscrite, et seuls le lien ou l’identifiant peuvent exécuter la désinscription. Pour tout autre droit, ou si le lien n’arrive pas, choisissez « Demande relative à mes données » sur la même page. Nous vérifierons votre identité de façon proportionnée et traiterons la demande.

Document d’information pour une liste d’attente. Il ne constitue pas un conseil juridique.