cestly

Privacy policy

Cestly waiting list · last updated: 5 November 2026

Last change: The control cookie lasts 90 days at most.
Change history

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

This page explains how we handle the data you provide when joining the Cestly waiting list or using the contact form. We collect only the bare minimum. We use no analytics, audience measurement or advertising.

Controller

The controller is **Lucas Ezequiel Palma**, an individual who runs the Cestly project from Andorra. This individual is subject to Andorra's Llei 29/2021 on personal data protection (LQPD). The EU General Data Protection Regulation (GDPR) may also apply if we intentionally target our offer at people in the EU. The fact that the website is accessible from the EU, free or in pre-launch does not, on its own, settle whether it applies.

We have not appointed an EU representative. Before targeting the launch or our campaigns at the EU, we will finish assessing whether the GDPR applies. If its Article 27 requires it, we will publish the contact details of that representative here. Nor have we appointed a data protection officer (DPO). The reason is that the current scope involves no automated decisions with legal effects, no large-scale processing of special-category data and no other high-risk mass processing. We will reassess before material changes.

To exercise your rights or ask us about privacy, write to privacy@cestly.app or use the unsubscribe and contact page (cestly.app/unsubscribe).

What we collect

- **Waiting list**: your email address and the consent tickbox are required; without them we cannot register you or notify you at launch. By selecting the tickbox you confirm you are 16 or older. As proof of your consent we also keep the version of this policy in force when you sign up and the sign-up date. For the same purpose we also keep the date of the last confirmation email we sent you, and when and how you confirmed. Sign-ups made before this email confirmation existed, in which the consent tickbox was selected, are recorded as confirmed on their sign-up date.
- **Language and country**: the site language and your country (2-letter code). We derive the country from your connection *without storing your IP address*.
- **Contact**: your email address, request type and message are required; without them we cannot receive, route or answer the request. Do not include information about your health, biometric data, beliefs or sexual orientation, or any other especially sensitive information.

Purpose and legal basis

For the waiting list, we use your data to **manage your sign-up and notify you at launch**. The legal basis is your **consent**, which you give expressly by selecting the tickbox in the form and can withdraw at any time. Before adding you, we check that the address is yours: we send you a confirmation email, and your sign-up stays pending until you open its link and select the confirm button on our website. Opening the link is not enough, so a program that scans your email cannot sign you up. You can also enter that email's 6-digit code on our website; the code is valid for 24 hours. If you unsubscribe and sign up again, you will need to confirm again.

If you use the form for a general enquiry, we process your email address and message to receive and manage it and to reply to you. The legal basis is our legitimate interest in responding to the enquiry you initiated.

If you exercise a data protection right, we process the information needed to verify your identity proportionately. We also process the information needed to handle the request, document the decision and respond. The legal basis is

compliance with our legal obligations.

We process technical security signals, pseudonymised attempt identifiers and audit events to prevent abuse and protect the service. We also process them to demonstrate the operations performed and defend ourselves against legal claims. The legal basis is our legitimate interest in maintaining a secure and accountable service, with data minimisation and specific retention periods.

Retention

Waiting list data is removed from ordinary use after 24 months, or earlier if you unsubscribe or the purpose ends. If you do not confirm your address, the sign-up is removed from ordinary use 7 days after the last confirmation email. Contact messages, including privacy requests, and the associated email address are removed from ordinary use after 12 months.

When removed from ordinary use, all these records are blocked. They are moved to an encrypted vault, separate from the active database, restricted to EU data jurisdiction and not visible from the admin panel. From then on, they can only be made available to the courts, the Public Prosecutor's Office, the competent public authorities or the APDA. That disclosure is solely in connection with possible liability arising from the processing. The legal basis for blocking is the legal obligation under Article 30 of the LQPD. As a general rule, we plan to destroy them 36 months after blocking. This is not a universal legal period: a claim, formal action or proceeding can change it. Once every applicable period has expired and no legal obligation requires us to keep them, we remove them from the systems in use. We do not treat destruction as complete while a technical recovery copy could reintroduce them. After a restore, the service stays closed, preserves the block and applies the deletion again. Cloudflare also lets us restore the database to how it was up to 7 days earlier.

To reconcile retries and restores, the vault keeps for 30 days a pseudonymised HMAC receipt. It holds the operation reference, the destruction date, the policy and the key version. It contains no email address or message and cannot reconstruct them on its own. It can then be purged.

This receipt is pseudonymised, not anonymous. Minimised technical audit metadata has its own maximum period of 36 months. The optional notice we receive in our company mailbox (Google) when you write through the form is generic and contains neither your email address nor your message. We do not promise that Gmail deletes it automatically. If the product does not launch, we will block the list and then destroy it in the same way.

Draft in this tab

If, from the form, you open one of the legal pages or change language in the same tab, we temporarily save the email address you typed and the language. We save them in that tab's session storage (sessionStorage). This only restores what you had typed: we do not send this draft to our servers or include it in the URL. We do not save consent. The draft is deleted when restored, once the sign-up is sent successfully or after 30 minutes. If the browser suspends the page, expired drafts are discarded when you return. The 30-minute limit applies only to this stored copy: we do not clear the email field of the form your browser keeps open. If the browser does not retain that form and no valid draft is available, you will need to enter your email address again. A draft may be unavailable because it has expired or storage is blocked. After you sign up, the page keeps your address only in memory for the "Resend the email" and "Change the address" buttons. It does not save it on your device.

Technical tickets and retries

When a sign-up, contact or unsubscribe starts, this site obtains a signed ticket for that action. It also temporarily stores the ticket, its random UUID and a timestamp in this tab's sessionStorage. The ticket identifies Cestly, the action and its validity period; it contains no email address, message or profile. It authorises a new operation for 10 minutes. If the result is uncertain, the same tab may retain it for up to 24 hours solely to reconcile that exact request. It is removed sooner when the result is confirmed, definitively rejected or the tab closes. The server keeps for 24 hours a receipt containing pseudonymised HMAC references to the request and its normalised content. The receipt also holds the action, state and timestamps. It records whether

the first reply said an email was on its way, so that a retry of that exact request gets the same answer. The receipt does not store the ticket, the UUID in clear text, the email address or the message. The daily purge then deletes it. These references are pseudonymised, not anonymous.

If you open the confirmation or unsubscribe link from an email, this site removes it from the address bar. It keeps the link and, when you confirm, the result in that tab's history (history.state). That way you don't lose your place if you reload, go back or change language. That data stays only in that tab, and this site uses it only to pick up where you left off.

Strictly necessary cookie for the waiting list

After a sign-up attempt, we may set our own control cookie. It is strictly necessary. From this browser, it lets you unsubscribe without a link. It also lets you sign up again and update your sign-up (the language, the country and the policy version). Nobody else can do so just by knowing your email address. If you sign up again from this browser and no more emails can be sent to that address for now, this site tells you. Without this cookie, it says nothing. When we give access to a real registration, the cookie's name is dynamic: it starts with __Host-cestly-waitlist-control- and ends with the random UUID of that access. When the response cannot give access to an existing registration, we may set a filler cookie that looks the same as the real one. Its name is random and repeats if you retry the same request. This way the response does not reveal whether the email address is registered. Both cookie types are host-only to cestly.app, Secure, HttpOnly and SameSite=Strict, so JavaScript cannot read them. The token contains a random UUID and its authenticated issued-at (iat) and expiry (exp) timestamps, never the email address or a reversible derivative. The cookie and token last no more than 90 days, and the server validates the signature and expiry before accepting it. They are not used for analytics, advertising or cross-site tracking, and are not shared with anyone except the processors that run this website. This section explains why they are strictly necessary and how they work. You can delete them in your browser. If you delete the

cookie that gives access to your registration, you will no longer be able to unsubscribe or update your sign-up from this browser without a link. You can still always use “Privacy request” or email privacy@cestly.app.

Recipients

Cloudflare (Cloudflare, Inc., USA) processes data on our behalf to host the website, run it and receive the forms, through Workers, D1 and Queues. Through Email Routing it also receives the copy of the direct email that we use to prepare the acknowledgement. Workers may run in any Cloudflare data centre in the world, usually the one closest to your connection. The D1 database is currently in Western Europe (WEUR), but it is not restricted to EU data jurisdiction. Queues (on its free plan) receives a notification UUID, generated separately for this purpose. It arrives inside a technical envelope that is the same for every message (the format version and the event type), with no email address, message or request type. Queues keeps it for up to 24 hours. Cloudflare publishes its data processing agreement (DPA) (https://www.cloudflare.com/cloudflare-customer-dpa/) and its list of subprocessors (https://www.cloudflare.com/gdpr/subprocessors/cloudflare-services/). Transfers to the US rely on the EU standard contractual clauses in that DPA; you can ask us for a copy at privacy@cestly.app. To timestamp the audit log, we send the public OpenTimestamps calendars a cryptographic digest with no personal data.

The optional notice for each new message from the contact form uses **Google Workspace and Google Apps Script**. We only turn it on after accepting Google’s Cloud Data Processing Addendum (CDPA) (https://knowledge.workspace.google.com/admin/compliance/privacy-compliance-and-records-for-google-workspace-and-cloud-identity) for the account. We also turn it on only after documenting the contracting entity, the subprocessors (https://workspace.google.com/terms/subprocessors/) and the international transfer safeguards. That notification email is generic: it does not include your email address, your message, the UUID or the date. We do not rely solely on the EU-US Data Privacy Framework to protect people in Andorra. You can ask through our privacy channel for a reference to the applicable safeguards or a copy of them.

Technical details of the optional notice: to generate it, this website sends Google only that notification UUID (event_id), the website name and the request type. The technical envelope of that transmission adds the version, the key identifier, a timestamp, a single-use random number and the HMAC signature. Apps Script schedules deletion of the UUID hash after 70 hours. The time and request type of the notice may be indirectly linked to the message stored in D1. This applies during the 12 months for which the message is kept, and until the next daily purge (less than 24 hours later, while the scheduled task runs normally).

Through **Google Workspace** (Google Cloud EMEA Limited, Ireland), the provider of our company email, which is subject to the same CDPA, we send these emails from support@cestly.app:

- the sign-up confirmation (also when you select “Resend the email”);
- the “You’re already on the Cestly waiting list” notice, when someone enters an already confirmed address again;
- the unsubscribe confirmation link;
- the contact form acknowledgement, which only carries a reference that reveals nothing and no content from your message;
- and the acknowledgement of the emails you write to support@ or privacy@.

Those emails are prepared by this website. **Supabase** (Supabase Pte. Ltd., Singapore), the server provider for our apps, hands them to Google mainly from its EU region (Frankfurt), without keeping them. Supabase publishes its DPA (https://supabase.com/legal/dpa) and its list of subprocessors (https://supabase.com/legal/subprocessors). Transfers to Singapore rely on the EU standard contractual clauses in that DPA; you can ask us for a copy at privacy@cestly.app. Google receives your address, the language, the signed links, the confirmation code and, in the acknowledgement of a direct email, the subject of your email. We keep no copy of those emails in any of our mailboxes, and Google keeps technical delivery logs under its CDPA. We do not sell your data or share it for commercial purposes.

Direct email to support@ and privacy@

If you choose to write directly to privacy@cestly.app or support@cestly.app instead of using the form, your email service sends **Google Workspace** your address. It also sends everything you include: subject, body, signature and attachments. We use that content only to receive, handle, document and answer the request. The legal basis is compliance with our legal obligations when you exercise a right and our legitimate interest when you make a general enquiry. That content is not used for marketing. We delete each direct message, together with our reply, at the first monthly review after it is 365 days old. Before that we keep an encrypted copy, outside the mailbox, blocked like the rest of this data. It can only be made available to the courts, the Public Prosecutor's Office, the competent public authorities or the APDA. As a general rule, we destroy it after 36 months. Only a documented legal or tax obligation to keep it can postpone that deletion, and those exceptions are checked at that same monthly review. Once the deletion is irreversible, the CDPA (https://cloud.google.com/terms/data-processing-addendum) allows Google to complete deletion from its systems as soon as reasonably practicable. The maximum period it allows is 180 days, unless law requires retention. Do not include special-category data or attachments unless strictly necessary; the form is the option that collects the least data.

When your email arrives at either address, we send you an automatic acknowledgement so you know it reached us. To prepare it, a copy passes through **Cloudflare** (Email Routing and one of our Workers). It reads the copy only to check that it is not automated mail or a forged sender, to see which language you wrote in and to take its subject. That way the acknowledgement reaches you in the same thread. It then discards the copy, and its text is not kept anywhere. Every new email gets its acknowledgement (replies within the same conversation do not), up to 10 per person per hour. Two traces remain. First, pseudonymised counters that stop loops between machines, deleted within 2 days. Second, the Email Routing activity log. For each copy, Cloudflare records there the date and time, the sender, the recipient, the subject and the message identifier. It also records the result of its authenticity and spam checks. It keeps the log for 31 days. We only consult it from our Cloudflare account, to check that the acknowledgement

works or to investigate abuse. The legal basis for this processing is our legitimate interest. This interest is in confirming that your email has arrived, without letting anyone use the acknowledgement to write to third parties.

Website language

Each language has its own address: cestly.app is the Spanish version, and /en, /ca, /fr and /pt are the others. The address sets the language and you change it with the selector. Only when an address does not specify a language (for example, a page that does not exist) does the site use the first supported language of your browser. That choice is made **on your device**. We do not store the language permanently on your device (only in the draft in this tab, described above) or use geolocation.

Bot protection

To stop bots from submitting the sign-up, contact and unsubscribe forms, we use our **own proof of work**. Your browser solves a small calculation tied to that submission and our server checks it. It uses no cookies, does not analyse your browser and sends no data to third parties. To limit abuse of the sign-up and contact forms, we keep a pseudonymised HMAC reference to the IP address in D1, never the IP address in clear text. We also keep, with the same mechanism, a pseudonymised HMAC reference to the email address. It is for sign-up emails, the unsubscribe page and the contact form acknowledgement. We keep it whether or not the address is on the list, and never the address in clear text. With it we limit what we send to each address. Every 24 hours, at most 3 sign-up confirmation emails (counting the first) and 1 “You’re already on the Cestly waiting list” email. Every 10 minutes, 3 unsubscribe links (and 5 every 24 hours). Every hour, 3 acknowledgement emails (and 6 every 24 hours). For the acknowledgement email and the confirmation code, we also keep, with the same mechanism, a reference that combines the email address and the IP address. This way, the website tells you only what was done with that email address from your IP address. That is at most 3 acknowledgement emails every hour and 5 attempts at entering the code every 24 hours. It never tells you what was done with that email address from other IP addresses. Across all IP addresses, we allow at most

10 attempts at entering the code for each email address every 24 hours. Each reference becomes due for deletion after 24 hours. The daily purge deletes it on its next run, less than 24 hours later, while the scheduled task runs normally. The proof of work, rate limits and automated guards only decide whether a particular submission is technically accepted. They do not profile you, decide anything about the future service or produce legal or similarly significant effects. If there is a false positive, retry or write to privacy@cestly.app.

Your rights

You can **unsubscribe**, exercise your rights (access, rectification, erasure, objection, restriction and portability), and withdraw consent by writing to privacy@cestly.app or through our unsubscribe and contact page (cestly.app/unsubscribe). You can ask through the same channel for a copy of our record of processing activities. You may also lodge a complaint with the Andorran Data Protection Agency (APDA) (https://www.apda.ad/) and, where applicable, the supervisory authority where you habitually reside. The service is not directed at children under 16: they must not use the waiting list or the contact form without authorisation from their legal representative. If we detect a submission from a child, we will limit processing to proportionately verifying that authorisation or deleting the submission; the child and their representative retain their rights.

You can unsubscribe from any device. The sign-up confirmation email and the “You’re already on the Cestly waiting list” email include your signed unsubscribe link. On the unsubscribe page, if you enter your email address, we send you a link to confirm that you want to unsubscribe. Unsubscribe links keep working even after their validity period ends (730 days for current links), and so does your email app’s unsubscribe button. If you open the page from one of these links, we show which address will leave the list, partly hidden. If this browser still holds the technical sign-up credential, the unsubscribe runs without a link. In both cases, the page’s response is generic: it does not reveal whether the address was registered, and only the

link or the credential can execute the unsubscribe. For any other right, or if the link does not arrive, choose “Privacy request” on the same page. We will verify your identity proportionately and handle the request.

Informational document for a waiting list. Not legal advice.