

Privacy Policy

Last updated: 9 October 2026

This Policy explains how UmCanto (umcanto.org) processes personal data under Brazil's General Data Protection Law (Law 13.709/2018, LGPD), the Brazilian Internet Framework (Law 12.965/2014, Marco Civil da Internet) and other applicable rules. It covers the website, the application, the public transparency page, the donation page, the messaging bot and the help assistant. Read it together with the [Terms of Service](#).

In this text, "UmCanto", "we", "us" and "our" mean the service and whoever runs it: **Fireho** (CNPJ 15.548.991/0001-19), seated in Monte Santo de Minas/MG, which operates the service and is the controller of the data we control (section 1). "Entity" means the non-profit organisation that subscribes to the platform. "Data subject" means the person a piece of data is about.

The Portuguese version is the original. If the two disagree, the Portuguese version prevails.

1. Start here: who owns the data

UmCanto is the system an entity uses to organise itself: the people it serves, the people who donate, the money coming in and going out, its public partnership agreements, its certificates and its campaigns. **The data about the people it serves, the people who donate and the people who work there belongs to the entity, not to us.**

In the language of the LGPD (art. 5, VI and VII):

- **the entity is the controller:** it decides what to collect about a person served, a guardian or a donor, for what purpose, on what legal basis and for how long. It answers to the data subject and to the regulators;

- **UmCanto is the processor:** we process that data on the entity's behalf, following its instructions, the Terms of Service and this Policy, and **we never use anyone's case file for our own purposes.**

We are **controllers** only of a smaller set of data that our service needs in order to exist:

- the **sign-in account** of whoever uses the platform (name, email, phone, credentials);
- the **entity's own billing** data for the use of the service;
- **technical logs** of access and security;
- **conversations with our support and the help assistant**, and the suggestions and complaints sent through it;
- **usage metrics** for the website.

Are you a person served, a relative, a donor or a volunteer of an entity and want to know what is held about you? Talk to the entity first: it is the one that answers. If it needs our technical help to answer, we help. If you contact us directly, we forward the request to the entity (section 11).

2. What data is processed

2.1 Data the entity enters (the entity is the controller)

People served. What the entity records on the case file: name, date of birth, sex, photo, city and address, documents (CPF, birth certificate, SUS health card, NIS), group or class, date of admission, the free-text history, dated follow-ups (the daily log, the visit, the monthly close) and the answers to questions **the entity itself created**, which may follow the CadÚnico model: household composition, housing, schooling, income, benefits received, referral through the SUAS social assistance network.

This usually includes sensitive personal data (art. 5, II, and art. 11): health, disability, ICD code, medical report, medication, racial or ethnic origin, and **data about children, adolescents and older people**. It is the most delicate data on the platform and gets the strictest protection (sections 9 and 13).

Guardians. Whoever answers for someone who cannot answer for themselves: name, relationship (mother, father, son, tutor, court-appointed guardian), CPF, phone, and whether they may collect the child, sign, or be called first.

Personal documents with a due date. Medical reports, benefits (such as the BPC), school enrolments and identity documents of a person served, with number, issue date and expiry date.

Donors and supporters. Name, email, phone, CPF or CNPJ when given, city, whether they wish to stay anonymous, the campaign that brought them, their donation history, their monthly donation pledges, whether they asked to appear on the donor wall and the Instagram handle they gave.

Team. Who works at the entity and in what role (presidency, treasury, secretariat, volunteering) and, on the government side, the partnership manager.

Finance and partnerships. Termos de fomento, termos de colaboração and cooperation agreements (Law 13.019/2014, MROSC), work plan, disbursement instalments, expenses with suppliers, supplier CNPJ or CPF, invoice number and photo, glosas and replies, the entity's certificates, collection boxes (place, keeper, location) and campaigns.

2.2 Data you give us (we are the controller)

- **Account:** name, email, phone, language, time zone and, if you fill them in, photo, bio, website, gender and location. The password is stored **only as a hash**, never the password itself.
- **Passwordless sign-in:** if you create a **passkey**, we keep only its public key and identifier; the private key never leaves your device. If you sign in with a **magic**

link, we generate a single-use link.

- **Messaging contacts:** the Telegram identifier, WhatsApp number or Discord identifier you link to your account.
- **Entity billing:** plan, invoices, the data needed to issue the service invoice (CNPJ, address, municipal registration) and payment status.
- **Support and assistant:** what you write to support, to the help assistant or to our bots, including files and audio you send, and the ratings you give to answers.

2.3 Data collected automatically

- **Access logs:** IP address, port, date and time, requested page, browser and operating system. Required by art. 15 of the Marco Civil.
- **Application errors and performance**, which may include the address requested and the identifier of the signed-in account.
- **Website usage metrics** through Google Analytics (section 7).
- **Browser notification subscription**, if you allow it (section 8).
- **The app (iOS and Android):** the device's notification identifier and the home screen widget token (section 8).
- **Cookies and local storage** (section 15).

2.4 Data received from third parties

- **Social sign-in**, when offered: Google, Apple or X send us the data described in sections 6 and 8.
- **Messaging platforms:** Telegram delivers your identifier, display name and the content of the messages you send to our bot.
- **Payment institutions:** confirmation that a service invoice was paid.

2.5 What we do not collect

- **We do not receive or hold donation money.** A PIX donation goes from the donor's bank straight into the entity's own account, through a QR code built on the entity's own key. We do not see the payment, the bank or the donor's bank details.
- **A one-off donation through the `/doar` page asks for no registration.** A donor is only recorded for whoever ticks "**Quero aparecer**" ("I want to appear": a name and, optionally, an Instagram handle) and whoever pledges a monthly donation (name and contact details, so the entity knows whom to thank).
- **We do not store full card numbers.** A card, when used to pay for the service, is processed and tokenised by the payment institution.
- **We do not use your device's sensors, camera or location** in the background.

3. What we use data for, and on what legal basis

3.1 When the entity is the controller

We process data entered by the entity **only to provide the service to it**: storing records, calculating balances and reports, assembling accountability filings, generating the donation QR code and receipt, warning about a certificate or medical report about to expire, sending the messages the entity asked for, backing up, keeping things secure and giving support.

The legal basis belongs to the entity, and choosing it is the entity's responsibility. For ordinary data it is usually compliance with a legal or regulatory obligation, performance of a contract or partnership agreement, legitimate interest or consent (art. 7). For sensitive data, the grounds of art. 11, for example specific and prominent consent, compliance with a legal or regulatory obligation, health protection by a health professional or service, or the regular exercise of rights. The platform does not decide that for the entity, and cannot.

3.2 When we are the controller

Data	Purpose	Legal basis (LGPD)	Retention
Account (name, email, phone, credentials)	Create and keep the account, authenticate, recover access	Performance of contract (art. 7, V)	While the account exists; then section 12
Passkey, magic link, social link	Sign in without a password, securely	Performance of contract (art. 7, V)	Until removed or until the account is deleted; the social sign-in identifier follows section 12
Closed account: what section 12 keeps, for as long as the law, the defence of rights or a block requires	Keep the entity's records, meet legal and tax obligations, answer claims, stop a banned person coming back with the same details	Legal obligation, regular exercise of rights and legitimate interest (art. 7, II, VI and IX; art. 16)	Section 12
Access logs	Comply with the Marco Civil, investigate abuse	Legal obligation (art. 7, II)	At least 6 months, as the Marco Civil requires
Error and security logs	Prevent fraud and unauthorised access, fix faults	Legitimate interest (art. 7, IX)	Deleted on request, unless an investigation is ongoing
Entity billing and invoices	Bill, collect, issue NFS-e, meet tax obligations	Contract and legal obligation (art. 7, V and II)	Tax-law period (usually 5 years)
Support, assistant and suggestions	Answer, fix what breaks, improve the service	Legitimate interest (art. 7, IX) and contract	Support messages and suggestions are kept; assistant conversations, until the account is deleted

Data	Purpose	Legal basis (LGPD)	Retention
Sales contact (people who ask to learn about the service)	Reply to those who showed interest	Legitimate interest (art. 7, IX)	Until you ask to be removed, or on request
Usage metrics (Google Analytics)	Understand site usage, in aggregate	Legitimate interest (art. 7, IX)	Per the Google Analytics configuration
Service emails (notices, invoices, alerts)	Run the account and billing	Performance of contract (art. 7, V)	While the account exists
Data in dispute	Defend rights in legal proceedings	Regular exercise of rights (art. 7, VI)	Until the limitation period ends

None of this is sold, rented or handed to advertisers, political parties or list buyers. Ever. We do not use data about people served or donors for advertising, commercial profiling or training artificial intelligence models.

4. The public page and the donation page

Each entity has a **transparency page** (`/orgs/<entity>`) and a **donation page** (`/doar/<entity>`), open to anyone.

- The transparency page shows **the entity's figures**: amounts received, donations this month, campaign progress, number of supporters. **Nothing from a person served's case file appears there.** How many people the entity serves appears only if it switches that on, and never for an entity whose address is confidential: the count of a month already closed, written once and published a month later, rounded and with a floor. Below the floor (10 people; 5 in towns of 20,000 or more, outside health) the page only says "fewer than 10" (or "fewer than 5"). Never a name, a photo, a neighbourhood, an illness or an exact number.

- The **donor wall** (donation page) and the list of monthly supporters (transparency page) show **only whoever ticked "Quero aparecer"** when giving: the name (or nickname), the Instagram handle if given and, on the wall, the amount. **Anyone who did not tick appears as "Anonymous" and is still counted in the total.** A person can leave the wall through the link they get when giving.
- Whoever pledges a monthly donation gives a name and, optionally, email and phone. That data goes to the entity, which is the controller.
- A sharing link may carry the first name of whoever shared it. That name is only shown back on the page; it is not stored.

5. Who we share data with

Only with those needed to run the service, only what is necessary, and under contracts or terms that require confidentiality and security. These are our **sub-processors**:

Category	Who	What they receive
Hosting and database	Servers under our administration, in Brazil	All platform data
File storage	Magalu Cloud (object storage, Brazil region)	Photos, invoices, attachments
Network, DNS and protection	Cloudflare	Access traffic (IP, requested address)
Transactional email	Amazon Web Services (SES, São Paulo region)	Recipient and email content
Support email	Google Workspace	Messages exchanged with support
Artificial intelligence	No one outside: the models run on our own server	n/a (section 7)
Metrics	Google Analytics	Browsing data (section 7)
Messaging	Telegram	Messages exchanged with the bot
Browser notifications	The browser vendor's push service (Google, Mozilla, Apple, Microsoft)	Subscription address and the notice
App notifications	Apple (APNs) and Google (FCM)	The device identifier and the notice
SMS, when used	SMS provider	Phone number and confirmation code
Social sign-in	Google, Apple, X	Authentication request
The entity's Instagram, when connected	Meta (Instagram)	The entity's authorisation, its posts and its comments
Service payments	Sicoob (boleto and Pix billing), Asaas (card)	Entity billing data

Category	Who	What they receive
Invoicing	Municipal or national NFS-e system	Entity tax data
Maps, when shown	Map service (such as OpenFreeMap)	IP and the map area viewed

We may also share data:

- **with the entity itself:** everything entered in it, and the records of who did what, since it is the controller;
- **with public authorities**, when the law, a court order or a lawful request requires it. We ask for the legal ground, hand over only what is necessary and, **where the law allows, warn the entity first**;
- **in a corporate transaction** (merger, acquisition, sale of the service), with whoever takes over UmCanto, who will be bound by this Policy. We will give notice before the change takes effect;
- **to protect rights:** ours, the entity's or third parties', in cases of fraud, abuse or a threat to security.

An entity may give a **government partnership manager** access to a specific partnership. That access is the entity's decision, within what the MROSC requires.

6. Google user data

This section applies whenever you use "**Sign in with Google**" or any integration with Google APIs we may offer.

What we access. Only the `openid`, `email` and `profile` scopes, which give us your **name**, your **email address**, your **profile picture** and your **Google account identifier**. We do not request access to Gmail, Calendar, Drive, Contacts or any other data in your Google account.

How we use it. To create your account or find the existing account with the same email, to authenticate you on later sign-ins, and to show your name and picture inside the platform.

How we store it. The identifier, email, name and picture address are linked to your account in our database in Brazil. We do not receive or keep anything that would let us reach into your Google account after you sign in.

Who we share it with. No one, except the sub-processors needed to host the service (section 5) or where the law requires.

Limited Use. UmCanto's use and transfer of information received from Google APIs to any other app will adhere to the Google API Services User Data Policy, including the Limited Use requirements. In particular, Google user data:

- **is not sold;**
- **is not used for advertising**, including personalised, retargeted or interest-based ads;
- **is not used to train generalised artificial intelligence or machine learning models;**
- **is not read by humans**, except with your explicit consent, where necessary for security (for example, investigating abuse), to comply with the law, or when aggregated and anonymised to run the service.

How to revoke and delete. You can remove UmCanto's access to your Google account at any time at myaccount.google.com/permissions. To delete your account here, see section 12. On deletion, the picture is erased; the Google account identifier, name and email are kept (section 12). Revoking at Google does not by itself close your account here; you can still sign in with a password, passkey or link.

7. Artificial intelligence and metrics

Where we use AI. In the **help assistant** (the round button), in the **Telegram bot**, in classifying and summarising suggestions and complaints and, when available, in features that read an uploaded document, such as the photo of an invoice to fill in an expense, always with human review.

Where it runs. Only on **models running on our own server**. The message you wrote, the recent history of that conversation, the receipt photo you sent and excerpts from the public pages of our manual go to that server and to no outside AI provider. It is also where we build the semantic search indexes (embeddings) for the manual and the suggestions. While that server cannot hear audio or read images in a conversation, the bots say this is not available yet.

What does not go. The assistant **does not receive the case files of people served, donor data or the entity's finances** in order to answer. **Do not paste data about a person served (especially health data or data about a child) into a conversation with the assistant or a bot.** If you do, it is recorded in the conversation like any other message.

Training. We do not use your conversations or the entity's data to train our own general-purpose models. No outside AI provider receives that content.

Answers may be wrong. An AI-generated answer is a suggestion, not accounting, legal, medical or social-work guidance. Check before acting, and always at the official source when a deadline or money is involved.

Metrics. In production, the site loads **Google Analytics 4**, which uses cookies to count visits and pages in aggregate. We do not send it names, emails, CPFs or any case-file data. You can block these cookies in your browser or with the Google Analytics opt-out add-on without losing any functionality.

8. Apple, Instagram, notifications and bots

Sign in with Apple, when offered: we receive your Apple account identifier, your email (which may be an Apple relay address if you choose to hide yours) and your name, which Apple only sends the first time. We keep Apple's refresh token only to disconnect the app when you delete your account or disconnect Apple: it is handed back to Apple and erased, and never used for anything else.

Sign in with X, when offered: we receive the account identifier, name, handle and picture and, if X provides it, the email.

The entity's Instagram. The entity can connect its own Instagram account: it authorises posts and comment reading on its own behalf, with its own consent on Meta's screen. Instagram is not a way to sign in.

Browser notifications. Only if you click allow. We store the subscription address the browser generates; the notice goes through the browser vendor's push service. You turn it off in the browser settings. If you say "not now", we remember that choice in the browser itself so we do not ask again.

The UmCanto app (iOS and Android). The app is this same site inside a native shell. On our server, linked to your account, we keep the device's notification identifier (the notice goes through Apple or Google) and the home screen widget token; deleting the account removes the registered devices (section 12). You turn notifications off in the device settings. **Face ID** (or Android biometrics) only locks the app on the device itself: nothing from it leaves here. The app **does not use location or the camera on its own**: only when a page asks (for example, to read a collection box QR or to upload a photo), and the system asks you at that moment. A **PIX donation** does not pass through the app or through us: the code is paid in the donor's own bank app (section 2.5).

Telegram bot. When you write to the UmCanto bot on Telegram, the platform receives your identifier on that network, your display name and the content of the message. If the identifier is not yet linked to an account, we create a minimal record to

keep the conversation going. We keep the conversation to continue it, until the account is deleted (section 12), and use AI to reply (section 7). **The bot never messages people served or guardians on its own**, and does not use a guardian's phone, which exists for the entity to call in an emergency, as a mailing list. Messages you exchange there are also subject to Telegram's privacy policy. **WhatsApp and Discord:** coming soon; when they open, this Policy changes first, with the notice in section 17.

Magic links are single-use and may be sent by email or by message. Do not forward a link to anyone else: it signs into your account.

9. Children, adolescents, older people and people with disabilities

The platform is not directed at anyone under 18. Sign-in accounts are for adults who work at an entity or in government. If we learn that an account belongs to someone under 18, we close the account as in section 12.

But many entities serve children and adolescents, and their case files are here. Therefore:

- processing must be done **in the best interest** of the child and adolescent (LGPD, art. 14) and in keeping with the Statute of the Child and Adolescent (Law 8.069/1990, ECA), including the **protection of image and identity** (ECA, art. 17);
- where consent is the legal basis used, for a child it must be **specific and given by at least one parent or the legal guardian** (art. 14, § 1). Obtaining, keeping and proving that consent is **the entity's job**; the platform stores what the entity records;
- **a child's photo and data never appear on the public page** or in campaign material generated by the platform. If the entity decides to use a child's image in a campaign, the decision, the authorisation and the responsibility are the entity's.

The same care applies to **older people**, whose dignity, image and autonomy are protected by the Statute of Older Persons (Law 10.741/2003, art. 10), and to **people with disabilities**, protected by the Brazilian Inclusion Law (Law 13.146/2015). An older person or a person with a disability is, as a rule, able to decide about their own data: recording a guardian or curator does not replace their will except where the law says so.

10. International transfers

Our application and database servers are in **Brazil**, and file storage and email sending use Brazilian regions. Some sub-processors, however, are foreign companies or process data outside the country, for example Cloudflare, Google (Analytics, Workspace, sign-in), Apple, X, Meta and Telegram.

These transfers take place under **art. 33 of the LGPD**: with contractual clauses ensuring a level of protection compatible with Brazilian law (including the standard clauses approved by the ANPD, where applicable), when necessary to perform the contract with you, or with your specific consent, such as when you voluntarily use a bot on a foreign platform.

11. Your rights

The LGPD (art. 18) gives data subjects the right to:

- confirmation that processing takes place;
- access to the data;
- correction of incomplete, inaccurate or outdated data;
- anonymisation, blocking or deletion of unnecessary or excessive data, or data processed unlawfully;
- portability, under the ANPD's regulations;

- deletion of data processed on the basis of consent, subject to art. 16, within the limits of section 12;
- information about whom we share data with;
- information about the possibility of refusing consent and its consequences;
- withdrawal of consent;
- review of decisions taken solely on the basis of automated processing (art. 20);
- objection to processing carried out in breach of the law.

How to exercise them.

- **About case-file, donation or team data of an entity:** ask the **entity**, which is the controller. The platform gives it the tools to correct and delete a case file and to answer the request. If you write to us, we forward it to the entity within 5 business days and let you know.
- **About your sign-in account or other data we control:** write to sac@umcanto.org from the account's email; to delete the account, see section 12. We may ask you to confirm your identity before handing over or deleting anything.

Requests made through Meta. If you used Facebook, Instagram or WhatsApp with UmCanto and ask Meta itself to delete your data, the request reaches us and counts as deleting the account (section 12). You get a confirmation code and a link to follow its progress on this site, at `/meta/deletion/<code>`.

Timing. Confirmation of processing and access in simplified form are answered immediately or, if complete, **within 15 days** (art. 19). Other requests are answered as quickly as possible, within any period the ANPD sets. If we cannot comply, we explain why.

Complaints. If you are not satisfied, you may complain to Brazil's **National Data Protection Authority (ANPD)** at gov.br/anpd, or to consumer protection bodies.

12. Deleting your account

How to ask: on the account page, button *Delete my account* (in the app too), or by email to sac@umcanto.org. A request made through Facebook, Instagram or WhatsApp reaches us and counts the same: you get a code and can follow it at

`umcanto.org/meta/deletion/<code>` .

What happens: the account is closed at once and can no longer sign in.

We erase at once:

- password and passkeys; sign-in keys and tokens stop working at once;
- notification devices and saved cards;
- photo, bio, website, gender, location and notification preferences;
- conversations with the assistant and what it learned about you;
- the link to you on the suggestions you sent, and the page and the device they were sent from (a suggestion keeps the page and the device it came from; the text stays);

We keep:

- name, email, phone, CPF, address and the identifiers of the accounts used to sign in (Google, Apple, Discord, X, Telegram, WhatsApp);
- the date and reason the account was closed;
- messages sent to support and suggestions;
- the care, follow-up and visit records you wrote in the organisation;
- your membership in the organisations' teams;
- invoices and payments, for 5 years;
- the log of your sign-in keys (when each was used, from which IP and with which client), for security;
- access logs, for at least 6 months.

Why: the law requires part of it (LGPD, art. 16, and art. 7, II, VI and IX), we must be able to defend ourselves against claims, and a blocked account must not come back with the same details. None of it is used for anything else. A running subscription ends; what was already owed is still owed. Backup copies are replaced in their normal cycle.

Entity data. While the entity is a customer, and for **90 days** after termination so that it can export everything. After that period we delete or anonymise it **on the entity's request, except what the law requires us to keep** (art. 16 of the LGPD).

Note to entities: accountability documents for partnerships with government must be kept **by the organisation** for 10 years from the accountability filing (Law 13.019/2014, art. 68, sole paragraph), and accounting and tax documents have their own periods. **Export and keep those documents before terminating**; the platform does not replace the archive the law requires of the entity.

Records removed by the entity. A case file, donor or collection box that is removed leaves the lists immediately and is marked as removed, with date and author, so that accountability stays consistent. Permanent deletion, at the entity's request, is carried out by us.

Access logs: at least 6 months (Marco Civil, art. 15), or longer under a court order or an authority's request.

Tax and billing data: for the period set by tax law.

13. Security

What we do, in general terms:

- **encrypted traffic** (TLS) between your browser and the platform;
- **encryption at rest of the most sensitive fields:** documents, history, case-file answers and follow-ups of a person served, personal documents, guardians' CPF

and phone, donors' CPF, email and phone, with AES-256-GCM, inside the application;

- passwords stored **only as a hash**, with passkeys as an alternative to passwords;
- **separation by entity and by role**: each person sees only the entities they belong to, and within them only what their role allows;
- regular **backups**, encrypted, kept away from the main server and protected against deletion;
- restricted internal access: people working at UmCanto only touch customer data when support requires it, for as long as needed.

No system is perfect. Security also depends on you: use a strong password or a passkey, do not share accounts, remove access for people who have left the entity.

Incidents. If a security incident may create a relevant risk or harm:

- for **the entity's** data, we notify the entity without undue delay, with what we know, so that it, as controller, can notify the ANPD and the data subjects;
- for **data we control**, we notify the ANPD and the affected data subjects under art. 48 of the LGPD and the ANPD's regulations.

14. Automated decisions

The platform **does not on its own take decisions with legal effects** on anyone.

What it does is **calculate and flag**: a person served who has not been followed up for too long, a donor who stopped giving, an idle collection box, a certificate about to expire, an expense outside the partnership term. What to do about it is decided by a person at the entity.

AI also classifies messages sent to the assistant (question, suggestion, chat). If you believe an automated decision affected your interests, you may ask for a review (art. 20) at sac@umcanto.org.

15. Cookies and local storage

Name or type	What for	Duration
Session cookie	Keep you signed in and protect forms (CSRF)	Until you close the browser or sign out
"Remember me"	Keep you signed in, only if you ask	Per the account configuration
Interface preferences	Remember screen choices (menu open or closed)	Up to 1 year
Google Analytics (<code>_ga</code> , <code>_ga_*</code>)	Aggregate usage metrics, production only	Up to 2 years
Protection network technical cookies	Defend the site against automated traffic	Short
Local storage	Remember whether we already asked about notifications; print preferences	Until you clear the browser

We use no advertising cookies and no social network trackers. Blocking session cookies prevents sign-in; blocking metrics cookies affects nothing.

16. Users in other countries

European Union and United Kingdom (GDPR / UK GDPR). UmCanto is offered to Brazilian entities. If the GDPR applies to you, the legal bases in section 3 correspond to performance of contract, legal obligation and legitimate interests; you have the rights of access, rectification, erasure within the limits of section 12, restriction, portability and objection, and you may complain to the data protection authority in your country. Transfers to Brazil and to sub-processors rely on appropriate contractual safeguards.

California (CCPA/CPRA). We do not sell or "share" personal information for cross-context behavioural advertising, and have not done so in the past 12 months. The categories collected and the purposes are in sections 2 and 3. You may ask to know, correct and delete your data at sac@umcanto.org, within the limits of section 12, without being discriminated against for doing so.

17. Changes to this Policy

We may update this Policy when the service or the law changes. The date at the top always shows the version in force. **A material change is announced on the platform or by email at least 30 days in advance.** Where a change depends on consent, we will ask again.

18. Contact and data protection officer

sac@umcanto.org: channel of Fireho's data protection officer (DPO / encarregado) and any matter concerning this Policy, data subject rights or security.

If you are a person served, a relative or a donor of an entity, remember: **your first contact is the entity.** We help the entity answer.