

Data protection briefing

For data protection officers, election agents and branch officers. How Cadrify limits what each person can see, what it records, how it handles requests from electors and what a national party can do when a local branch adopts it.

Last reviewed 07/10/2026

In short

Data protection will not be front of mind for many of the volunteers who handle your campaign data, and Cadrify works on that assumption. Each person gets the least data their job needs. Their access is limited by default and ends when the work does. Cadrify keeps a detailed log of who changed your data and who took it out.

The short version:

- Three levels of access. Activists see only the rounds and tasks they are given. Organisers run their own branch. Admins manage their branch and the branches beneath it.
- Every client in Cadrify is walled off from every other client in the database itself, so no other client can reach your data.
- Changes, exports, sign-ins and data requests are written to an audit log your data protection officer can read and download.
- Subject access and erasure requests are handled in Cadrify, from the day a request arrives to the download or deletion that answers it.

Special category data

Doorstep results record people's political opinions, which makes them special category data under Article 9 of the UK GDPR. The law expects exceptional care with it, so every part of Cadrify puts security first, from what a volunteer's phone keeps offline to who can export a list.

Not every tool needs that data. Leaflet rounds show addresses and never an elector's name, and petitions, events and forms hold only what a supporter chooses to give. You can run that work with lighter controls, such as a QR code that asks volunteers for nothing, and keep the tightest controls for door-knocking.

Who is responsible for what

Your organisation is the data controller for the campaign data you put into Cadrify. Cadrify Ltd is your processor and acts only on your instructions, under a data processing agreement that forms part of every subscription. Cadrify is the controller only for the account data it needs to run the service, such as sign-in details and billing.

Where the data is held

Application servers, database, background workers and cache all run in Frankfurt, inside the European Economic Area, on Render's infrastructure. Data is encrypted in transit with TLS and at rest by the hosting platform. Backups are taken daily.

Who processes it for us	Sub-processors are listed in the data processing agreement, with what each one receives. Optional features that send data to a third party, such as per-address geocoding or AI features, are described in the security policy before you turn them on.
If something goes wrong	The data processing agreement commits Cadrify to tell you without undue delay after becoming aware of a breach affecting your data, in time for you to meet the 72-hour deadline that applies to you as controller.
Certification	Cadrify is not yet ISO 27001 or SOC 2 certified. Certification audits are a cost we have not yet taken on. The controls are set out in full in the security whitepaper, and the data processing agreement gives you the right to audit them.

When a volunteer makes a mistake

Phones get lost and links get forwarded. Training helps, but a system that relies on every volunteer getting it right every time will fail. Whatever a volunteer can see is what they can leak, so Cadrify shows them as little as possible.

A door-knocker sees	A door-knocker never sees
Names, addresses and register numbers in the ward they are assigned to	The rest of the register, or any other ward
The last result recorded at each door, so they do not repeat a conversation	Dates of birth, phone numbers or email addresses
Practical flags such as postal voter, needs a lift or a safety note for the address	Electors who asked not to be called on. They are left off the list entirely
The doorstep screens for their round and nothing else	A search box, a contact list or an export button. None of these exist below organiser

Cadrify's door-knocking view. Branches choose which questions are asked at the door.

What stops one mistake turning into a breach:

- Access to a round comes from an assignment. It ends when the round is complete, when the assignment is withdrawn or on an end date you set, without anyone having to remember to remove it.
- A QR code for an action day covers one task, such as one leaflet round or one teller shift. It expires after 15 minutes, an hour, at the end of the day or on a date you set, can be limited to a number of uses, and can be revoked as a whole or for a single volunteer. A forwarded code reaches one task, not the database.
- Leaflet round codes show addresses only. Nobody delivering leaflets sees an elector's name.
- The copy kept on a phone for working without signal belongs to the volunteer who downloaded it. It is removed when their access ends, after 14 days at most, and when they sign out. Another person picking up the same phone reads nothing.
- Sessions last 24 hours at most, and changing a password signs the account out everywhere.

Paper is the one copy software cannot recall

Printed walk sheets carry names and addresses. Cadrify prints only what the round needs, but once a sheet leaves the office it is in your volunteers' hands. Count sheets out and count them back, and shred them after polling day.

Roles and permissions

Most data incidents in campaigns are accidents. Some are not, such as a volunteer who joins to copy the register or an account taken over with a reused password. The defence is the same principle applied harder. Nobody holds access they do not need, so no single account can take much.

Role	What it can do	What it cannot do
Activist	Work the rounds, polling station shifts and tasks they are given, while the work lasts	Search the register, open elector records, export, or see another ward
Organiser	Run the branch's campaigning and exports for that branch	See other branches, or branches below it
Admin	Manage a branch and every branch beneath it	See sibling branches or anything above it
Data protection officer	Read the audit log, export history and record of processing, answer subject access requests and raise erasure requests across the organisation	Change campaign data or approve an erasure

Door-knocking and telling are work given to an activist, not roles of their own. Organiser, admin and data protection officer roles can be narrowed further to named wards or constituencies. A narrowed role that cannot be resolved grants nothing.

Underneath the roles:

- Every organisation's rows are separated by row-level security in the database. If a mistake in application code ever asked for another organisation's data, the database would still refuse it. A request with no organisation resolves to none.
- The organisation-wide bulk export is reserved for the admin of the top branch. Export API keys need a whole-organisation admin and are rate limited.
- Ethnicity-based and other special-category filters are hidden from customers and kept out of exports.
- Passwords need at least 12 characters and are checked against a list of common and breached choices. Ten failed attempts in 30 minutes lock the account, and sign-in is rate limited by address and by account.
- Passkeys and single sign-on through your own identity provider (OpenID Connect) are available, so accounts can sit behind your party's existing sign-in and its own second factor.
- QR code secrets are stored only as a one-way hash. A copy of the database would not let anyone redeem a code.
- Cadriy staff with operator access are a small, named group, and every request they make is written to a separate staff access log.

What you can prove afterwards

A data protection officer is asked to show their working. Cadriy keeps the evidence as the work happens, so you are not reconstructing it from memory and chat logs after a complaint arrives.

Written to the audit log, with who, what and when:

- Changes to elector and supporter records, assignments and roles
- Register and data imports
- Exports of contacts, filters, segments and round spreadsheets, nomination papers and the export API, with a row count
- Door-knocking sheets, paper assignment sheets, leaflet route sheets and leaflet drop downloads, counted in doors
- Phone bank call lists, petition and open letter signatures, form, quiz and email campaign responses, event RSVPs and ticket orders
- Donation, expense, accountancy and Electoral Commission return downloads
- The bulk export of your organisation's data, one dataset or the whole ZIP
- Subject access requests and downloads, and erasure requests raised, approved and rejected
- QR codes created, claimed, revoked and ended
- Single sign-on logins

The data protection officer and admins read the log on the compliance screen and download it as CSV.

Downloading the log is itself logged. Recent exports have their own view, so the first question after an incident, who took what out and when, has an answer on one screen.

Sign-ins have a page of their own beside the log: successful and failed sign-ins by password, passkey, single sign-on or emailed link, lockouts, and password and passkey changes, with the time and IP address, for every account in your organisation.

Subject access and erasure requests

Electors write in. Some want to know what you hold, and some want it gone. Each request has a one-month clock. Cadrify handles both kinds itself, so answering one does not mean searching spreadsheets.

A subject access request:

1. Log the request on the compliance screen the day it arrives. People who have since left the register are found too. Its due date, one calendar month on, shows until it is answered.
2. Download their record. It brings together the register entry and address, voting history, every door-knocking result and doorstep answer with the question that was asked, changes made to the record, and donation, nomination and other linked records.
3. Send it on. Downloading it from the request marks the request answered, and the download is recorded in the audit log.

An erasure request:

1. An admin or your data protection officer raises the request against the elector or supporter, with the day it arrived. Its due date shows until it is decided.
2. An admin approves or rejects it. The request keeps who raised it, who decided and when, and both steps are in the audit log.
3. On approval Cadrify blanks the person's name and date of birth and deletes what the campaign recorded about them: door-knocking results, doorstep answers, record history, contact details and links to other records. Audit entries about the person keep what was done, by whom and when, with the details removed, so an earlier subject access export is still on record.

If the person is still on the council's register

Erasure removes what your campaign recorded. When a later register upload carries the same person at the same address, or with the council's own reference for them, Cadrify recognises them from a one-way key and keeps the entry blank, even when the register spells the name a little differently, such as Mccarthy for McCarthy or Margret for Margaret: no name, no date of birth, and they are left out of door-knocking. The key cannot be read back as a name. None of their history returns.

The other rights, where they live:

Rectification	Admins correct an elector's record directly, and the change is logged.
Objection to contact	Do not knock, the do-not-call list and email unsubscribes each keep a person out of that channel for good. Broadcast emails carry an unsubscribe link.
Consent	Sign-up pages, petitions, event bookings and forms record whether the person opted in, and supporter records keep when and where they gave it.
Record of processing	Cadrify publishes its own record of processing activities, kept beside the code that does the processing and downloadable from the compliance screen, as a starting point for yours.

For national election agents: when a branch adopts Cadrify

When a local branch adopts Cadrify on its own, the national office needs to know where the register now sits, who can see it and what happens when the branch officer who set it up moves on. This section answers those questions.

A branch that signed up on its own

- Its data sits in its own organisation, walled off in the database from every other customer, including other branches of your party.
- Its volunteers work under the same limits as anyone else's. Nobody below organiser can search, browse or export the register.
- Its exports and changes are in its audit log, and it can appoint a data protection officer with read-only access to that log.
- Nothing is shared outward. Cadrify does not pool data between customers, sell it or use it to build a national file.

Cadrify does not check a new sign-up against your party, and it does not tell you when one happens. If you want every branch inside a structure you control, the answer is to set that structure up first and invite branches into it, described below.

Option one: run the party as one organisation

The national or regional office sets up the organisation and creates a branch for each local party underneath it. Branch officers are invited into their own branch.

- National admins see and manage every branch. Each branch admin sees their own branch and the branches below it, and never a neighbour.
- Party ID codes and doorstep questions are set once at the top and inherited by every branch, so the numbers add up when you read across them.

Data protection briefing

- One data protection officer covers the whole organisation without changing campaign data, and can be narrowed to named wards or constituencies if that suits how you work.
- When a branch secretary moves on, a national admin removes their access and the branch carries on with its data intact. The campaign does not leave with the person.

Option two: affiliate separate organisations

Some parties prefer each local party to hold its own subscription and remain its own controller. Affiliation links them to the national organisation without merging them.

1. A national admin issues a join code. Each code works once and expires after 30 days.
2. The local party enters it when it creates its Cadrify organisation. National admins are emailed the request.
3. A national admin approves or declines it. Approval places the local party under the national organisation in the branch tree.

An affiliated organisation keeps its own billing, its own settings and its own records. Affiliation does not give the national office access to the local party's electors, and national settings do not flow down into it. If you need that level of control, choose option one.

A branch that is already using Cadrify on its own cannot yet be moved under you from inside the product. Talk to us about moving it.

Questions to put to a branch that is already using it

1. Who are the admins, and does each of them still need to be one?
2. Has the branch appointed someone to the data protection officer role, and have they looked at the audit log?
3. Who has exported data, and where did the files go? Recent exports are listed on one screen.
4. Are door-knockers given dated assignments and expiring QR codes, rather than standing accounts?
5. How are printed walk sheets counted back in and destroyed?
6. Would the branch move into the national organisation, or affiliate to it? We can help with either.

Data protection FAQ

Can Cadrify staff see our data?	A small number of staff hold operator access for support and incident response. Every request they make is written to a staff access log. Nobody at Cadrify browses customer data for any other reason.
Do you use our data for anything else?	No. We do not sell it and we do not use it to train AI models. If you choose to use features that learn from your data, such as suggested donation amounts, they learn from your data alone, are never pooled with other clients' and work only for you.
What happens when we leave?	Export everything as CSV first. A whole-organisation admin can then delete the organisation, or ask us to, and the data processing agreement sets out how deletion and backups are handled.
Can we limit someone to one ward?	Yes. Organiser, admin and data protection officer roles can each be narrowed to named wards or constituencies.
Do volunteers need an account?	It is up to you, and you choose on each QR code. For less sensitive work such as a leaflet round, a code can let supporters join with no account at all. For a door-knocking round you can require everyone who joins to sign in with a Cadrify account.

Data protection briefing

Is the electoral register safe to upload?

If you are entitled to the full register, yes. Our register handling document covers what happens to it from upload to deletion.

Further reading

- **Data processing agreement** <https://cadrify.org/dpa>
 - **Security policy** <https://cadrify.org/security/policy>
 - **Security whitepaper** <https://cadrify.org/security/whitepaper>
 - **How we handle your register** <https://cadrify.org/how-we-handle-your-register>
 - **Privacy policy** <https://cadrify.org/privacy>
-

Cadrify Ltd, company number 17244539, registered in England and Wales. ICO registration ZC158949. Registered address 7 Malvern Road, Hornchurch, Essex, RM11 1BG.

This briefing explains how Cadrify works. It is not legal advice.