

Security and data protection

Written for the person who has to sign Cadrify off. Who we are, which data we hold and under what role, where that data sits, who else touches it and what happens if something goes wrong.

Last reviewed 06/10/2026

Who you are contracting with

Cadrify is built and run by Cadrify Ltd, a company registered in England and Wales. There is no offshore holding structure, and no other company operates the service on our behalf beyond the sub-processors listed below.

Detail	Value
Legal entity	Cadrify Ltd
Company number	17244539 (England and Wales)
Registered office	7 Malvern Road, Hornchurch, Essex, RM11 1BG
ICO registration	ZC158949
Data protection contact	privacy@cadrify.org
Security disclosures	security@cadrify.org
Procurement and contracts	sales@cadrify.org
Product support	support@cadrify.org

Data protection correspondence is answered by the data protection contact above. Eugene McCarthy, the founder, is accountable for it. Post can be sent to the registered office, marked for the attention of the data protection contact.

Controller and processor roles

Two roles apply here. For the campaign data you put into Cadrify, you are the controller and Cadrify is your processor. For the account, billing and security records Cadrify keeps to run its own business, Cadrify is the controller. The two roles meet on one record type, platform account records, where Cadrify holds the same record in both roles. That case is set out in the table below. No campaign data moves from the first role into the second.

As your processor, Cadrify acts only on your documented instructions. Your instructions are the data processing agreement, the terms of use and the way your own people configure and use the product. Cadrify does not use your campaign data for its own purposes, does not sell it, does not share it with other organisations on the platform and does not use it to train machine learning models.

Data	Controller	Cadrify's role
Electoral register records you import	Your organisation	Processor

Security and data protection

Data	Controller	Cadrify's role
Door-knock records, including voting intention, support score and doorstep notes	Your organisation	Processor
Member, supporter and volunteer records	Your organisation	Processor
Casework, donations, events, email and finance records created in the product	Your organisation	Processor
Platform accounts for your organisers and door-knockers	Your organisation, for the accounts inside it	Processor, and separately controller where the same records are used to administer, secure and bill the service
Billing and payment records for your subscription	Cadrify Ltd	Controller
Support correspondence with Cadrify	Cadrify Ltd	Controller
Security, abuse-prevention and operator access logs kept for our own obligations	Cadrify Ltd	Controller

Section 4 of the data processing agreement, "Independent controller processing", records that Cadrify acts as an independent controller for account administration, support communications, abuse and fraud prevention, records it keeps to meet its own legal obligations and, where billing applies, billing and payment records, and that this processing sits outside that agreement. The dual position on platform accounts exists because the same record is your staff list when you manage it, and our customer record when we administer, secure and bill the service.

Where you connect an external system such as Action Network, NationBuilder, Salesforce or Movement, you do so with your own account and credentials. That provider processes data under your relationship with it, not as Cadrify's sub-processor, and you hold the agreement and the transfer safeguards with them. Only supporter and volunteer contact records are exchanged. Register records and door-knock records are never included in an integration sync.

If an instruction from you looks to us like a breach of data protection law, we will tell you. Beyond that we do not assess the lawfulness of your instructions, and we cannot establish your lawful basis for you. See special category data below.

Where your data is held

All campaign data lives in one managed PostgreSQL database in Frankfurt, Germany, inside the European Economic Area. The application servers that read it run in the same region. The infrastructure is operated by Render on Amazon Web Services.

- Database and application servers: Frankfurt, Germany (EEA).
- Encryption: TLS 1.2 or 1.3 in transit, AES-256 at rest at the storage layer.
- Backups: daily, retained for a minimum of 7 days, with point-in-time recovery inside that window. Backups stay in the same region.
- File storage, for uploaded register files, cached geocoding results and generated PDFs: a persistent disk in the same region.

Security and data protection

Campaign data is held in the EEA. Three flows send data to providers outside that hosting, and what each one carries is different.

- Billing. Stripe processes subscription and payment records in Ireland and the United States under standard contractual clauses. Card details are entered on a Stripe-hosted page and never reach Cadrify's servers. No campaign data goes to Stripe.
- Per-address geocoding, optional and off unless we enable it. Address text goes to the geocoding provider with no name attached to it. No other register field goes with it.
- AI features, where your organisation has them enabled. Two of these carry campaign data. Name origin classification sends forename and surname text. Scanned marked register digitisation sends cropped images of register lines, and those crops contain elector numbers and names. Issue clustering sends keyword lists and message testing sends campaign copy, neither of which carries an elector record. Each feature is set out under sub-processors below.

Postcode-level geocoding, boundary lookups and polling station lookups send a postcode or a GSS area code to British services. No name and no register record goes with them.

Sub-processors

A sub-processor is a company Cadrify engages to help deliver the service, which may touch personal data under our contract. The data processing agreement carries the authorised list in Annex 3, and we give you reasonable notice before adding or replacing one.

Sub-processor	Purpose	Where it processes	What it receives
Render	Application hosting and the PostgreSQL database	Frankfurt, Germany (EEA)	All platform data
Resend	Platform email: password resets, invitations, verification and notifications	Dublin, Ireland (EEA)	Recipient name and email address, message content
Stripe	Subscription billing, and donation or ticket payments where you use them	Ireland and the United States, under standard contractual clauses	Billing contact and payment records. No campaign data
postcodes.io	Postcode-level geocoding, the default path	Britain	Postcodes only
mySociety MapIt	Ward, constituency and local authority boundaries by GSS code	Britain	No personal data

This table covers the sub-processors engaged for every customer. The current list is always available from privacy@cadrify.org on request.

Two optional features bring in further providers, and only for organisations we have enabled them for. AI features are set out below. Per-address geocoding sends address text, with no name attached to it, to Google Maps Platform, or to Nominatim (OpenStreetMap Foundation) where no Google key is configured. Neither is covered by the EEA hosting described above. Postcode-level geocoding, the default path, uses neither.

Broadcast email that goes out in your own organisation's name is sent through an email provider you connect yourself: Resend, Amazon SES, Mailgun, Postmark or your own SMTP server. That provider works under your

relationship with it, not as Cadrify's sub-processor, and your recipient list and message content reach it on your instruction. Cadrify's own Resend account carries platform email only.

The public marketing and legal pages load a cookieless analytics script and a demo-booking widget. Neither loads on a signed-in page, so no page address containing a record identifier reaches them.

AI features and what they send

AI-backed features are granted per organisation and are off unless we enable them for you. Where none is enabled, nothing your organisation holds reaches an AI provider. Where one is enabled, the request goes to Anthropic, or to OpenAI where a deployment is configured to use it instead. Both process outside the EEA. This is what leaves the platform.

- Issue clustering sends keyword lists drawn from doorstep issue records. It sends no elector names and no addresses.
- Message testing and copy assistance send the campaign copy being written or tested, and the synthetic personas it is tested against. They send no elector records.
- Name origin classification, an aggregate research tool, sends forename and surname text. A result is stored against the name, never linked to an elector record.
- Scanned marked register digitisation, which is not generally available yet, sends cropped images of register lines. Those crops contain elector numbers and names.

Voting intentions, support scores and door-knock notes are not sent to an AI provider. Two of the features above do send elector data outside the EEA, and they are worth weighing separately. Name origin classification sends forename and surname text and returns an inferred ethnic-origin category. An inference about ethnic origin is special category data under Article 9 of the UK GDPR, and it is created by a provider outside the EEA. Scanned marked register digitisation sends elector numbers and names inside the cropped images. Weigh both against your own Article 9 condition before asking us to turn either on.

Access control

Access is decided in three layers: which organisation a person belongs to, which branch their role sits on and which wards that branch holds.

Organisation	Every record carries an organisation identifier, taken from the signed-in session and never from anything the browser supplies. More than 100 tables additionally carry a PostgreSQL row level security policy, so the database itself withholds rows belonging to another organisation whatever the application asks for.
Branch	Roles are granted on a branch in your organisation's tree and resolved by a recursive query up that tree. An admin of a parent branch is an admin of every branch beneath it. An organiser holds the exact branch they were granted, with no inheritance sideways or upwards.
Ward	A branch's geography is its own ward assignments plus those of the branches beneath it, matched by GSS code rather than by name, because British ward names repeat across local authority districts. A person sees the electors in the wards their role covers and no others.

Security and data protection

Role	Scope	What it reaches
Door-knocker	One active assignment	Only the addresses and electors on that assignment. No register browsing. Access ends when the round ends and can be withdrawn at any time
Organiser	One branch	Data and people in that branch. No inheritance to parent or sibling branches
Admin	A branch and everything beneath it	Full management of that branch and its descendants. No access to another organisation
Data protection officer	The whole organisation, read only	The compliance area: audit log, subject access exports, erasure requests, record of processing activities. No write access to campaign data

A small number of Cadrify staff hold an operator flag that permits cross-organisation access for support and incident response. Every operator request is written to a separate audit log before the request is handled, recording the account, the action, the organisation and the client IP address. Those records are held apart from application data and cannot be edited through the product.

Encryption and passwords

In transit	TLS 1.2 or 1.3 on every connection. Plain HTTP is redirected at the infrastructure layer, and cookies carry the Secure flag in production.
At rest	AES-256 at the storage layer, covering the database volume, its backups and the persistent disk.
Passwords	Hashed with bcrypt, a memory-hard function chosen to stay expensive to attack if a database copy were ever taken. Minimum 12 characters. Passwords are never stored or logged as readable text and cannot be recovered, only reset.
Sign-in protection	An account locks for 30 minutes after 10 failed attempts inside a 30-minute window. Sign-in is rate limited, and the error message does not reveal whether an email address is registered.
Sessions	A random token equivalent to 256 bits of entropy, held in a Secure HttpOnly cookie, expiring after 24 hours and cleared on sign-out and on password change.
Integration credentials	Encrypted at the application layer with Fernet before they are written to the database, and decrypted only when an outbound request is built.
Single sign-on	OIDC single sign-on is available for organisations that authenticate people through their own identity provider. SAML is not built.

Multi-factor authentication is on the roadmap and is not available yet. We would rather say so here than have you find out in month two. The full roadmap, including planned external penetration testing, is in the security whitepaper.

Audit logging

Security and data protection

Two logs matter to a data protection officer.

The authentication log	Sign-in attempts, successful or failed, by password, passkey, single sign-on or sign-in link, with the account where there is one, the outcome, the client IP address and the timestamp. It also records lockouts, password changes and resets, accounts created, activated, deactivated or deleted, roles added, changed or removed and invitations issued, redeemed, regenerated or cancelled.
The organisation audit log	Data-changing actions inside your organisation, including record edits, exports and erasures, with the actor, the entity acted on, a summary and the client IP address.

Your data protection officer and your admins read the organisation audit log in the compliance area and export it as CSV. Exporting the log is itself recorded in the log.

They also see sign-in and credential events on the Sign-ins page in the same area: password, passkey, single sign-on and sign-in link sign-ins, failed attempts, lockouts, password resets and changes, with the time, the account, the action and the IP address. The page covers accounts that hold a role in your organisation, and sign-in attempts through your organisation's own single sign-on connection. A failed sign-in against an email address that has no account is not linked to any organisation, so it does not appear there. Someone who belongs to two organisations signs in once for both, so their sign-ins appear on both organisations' pages.

Neither log can be edited through the product. Two things change entries. When an erasure request is approved, the organisation audit log entries about that elector or activist keep who did what and when, and lose the summary and details that describe the person. When an organisation is deleted, its organisation audit log and export records are deleted with it. Authentication log entries are not deleted. When an account is deleted, its entries stay without the link to the account.

Log	Retention	Who can read it
Authentication and account log	No automatic deletion	Your admins and data protection officer, for sign-in and credential events. The rest from Cadrify on request
Organisation audit log	Kept while your account is open. Deleted 30 days after it closes, except as set out above	Your admins and data protection officer
Operator access log	Life of the platform	Cadrify, and your organisation on request
Application server logs	30 days	Cadrify

Retention, export and deletion

You decide how long your campaign data lives. While your subscription runs, Cadrify holds what you put in and deletes what you delete.

- Export at any time. Dataset exports as CSV or JSON in the product and through the export API, the audit log as CSV, a subject access export for a single elector as JSON and your record of processing activities as Markdown. Downloads of your organisation's personal data are logged with who downloaded what, when and how many rows: register and contact lists, door-knocking and leaflet sheets, call lists, signatures, form and event responses, finance files and the bulk export. Your admins and data protection officer see them on the compliance overview and on the exports page of the data hub. A subject access export and an export of the

audit log are recorded in the audit log.

- **Erasure.** An erasure request is raised against the elector and tracked in the compliance area. On approval the name and date of birth are erased from the record, and the elector's door-knock logs, change history, published donation links and objections are deleted, and the audit log entries about the elector keep only who did what and when. The stripped record stays in place, so ward and round counts do not change. A copy can persist in an encrypted backup until that backup ages out of its retention window.
- **On account closure.** At your choice we return your data in a structured, machine-readable format or delete it. An admin of the whole organisation closes the account in the product, or we close it on request. For 30 days after closure only those admins can open it, to export what they need or reopen it. Then it is deleted automatically, with its audit log and export records. Encrypted backups fall out on their normal cycle, set out in the security whitepaper.

Customer-managed retention, where an admin sets an automatic deletion period for register and door-knock data, is on the roadmap and is not built yet. Until it lands, deletion is on request or carried out by your own admins in the product.

Personal data breaches

If personal data we process for you is breached, you have 72 hours to decide whether to tell the ICO. Our job is to get you the facts inside that window.

1. Contain the incident and preserve the evidence.
2. Establish what data was involved and whose.
3. Notify you without undue delay after becoming aware, in time for you to meet your own obligations under Articles 33 and 34 of the UK GDPR.
4. Cooperate with any notification you make to the ICO or to the people affected.
5. Provide a post-incident report on request.

The notification tells you, as far as it is known at the time: what happened, which categories and roughly how many data subjects and records are affected, the likely consequences and what we have done or propose to do about it. We do not notify the ICO or data subjects on your behalf unless you instruct us in writing.

Special category data and political opinions

This is the section most procurement reviews stop on, so it is worth being exact.

A voting intention is a political opinion. Under Article 9 of the UK GDPR, personal data revealing political opinions is special category data, and processing it needs both a lawful basis under Article 6 and a separate condition under Article 9. Support scores, party preference and doorstep notes that record how someone intends to vote all sit in that category. So does anything you choose to record about a person's ethnic origin, religion or health.

You establish the lawful basis, not Cadrify

You are the controller. Establishing the Article 6 basis and the Article 9 condition is your responsibility, not ours, and Cadrify cannot do it for you. As your processor we act on your instruction and we do not assess whether your basis holds, though we will tell you if an instruction looks to us like a breach.

British campaigns generally rely on one of a small set of positions, and which one fits depends on what kind of organisation you are.

Security and data protection

- Article 9(2)(d), for a not-for-profit body with a political aim processing data about its members and people in regular contact with it.
- The substantial public interest conditions in Schedule 1 to the Data Protection Act 2018, including the condition for registered political parties and the democratic engagement provisions that cover campaigning contact with electors.
- Article 9(2)(e), where the person has deliberately made the opinion public. This is narrower than it sounds and rarely covers doorstep responses.

Take your own advice on which condition applies to you, and record the decision. Your record of processing activities in the compliance area is a reasonable place to keep it.

The register is a separate question. Electoral register data is governed by the Representation of the People Act 1983 and its regulations, which set out who may hold a copy and what they may use it for. Cadrify does not supply register data. You import the copy you are entitled to hold, and you remain responsible for keeping its use inside those limits.

What Cadrify does with special category data:

- Records it as structured fields, so it can be found, exported and erased rather than left buried in free text.
- Keeps it under the same access control as everything else, so a door-knocker sees it only for the electors on their current assignment.
- Logs the actions that change or export it in the audit trail.
- Never includes it in a sync to an external CRM.
- Never sends voting intentions, support scores or doorstep notes to an AI provider. Name origin classification is the one place special category data meets an AI provider, in the other direction: it sends names, and the ethnic-origin category it returns is itself special category data. It is described under AI features and what they send.
- Never sells it, never shares it between organisations and never uses it for our own purposes.

Raising a request or a security disclosure

What you need	Where to write
A data protection request: access, rectification, erasure, restriction, portability or objection	privacy@cadrify.org
A suspected vulnerability or a security concern	security@cadrify.org
A procurement pack, a supplier questionnaire or a signed data processing agreement	sales@cadrify.org
A question about the product itself	support@cadrify.org

We assist with data subject requests and with data protection impact assessments at no charge for reasonable volumes. If an elector or a member writes to Cadrify directly about data you control, we do not answer for you. We pass the request to you without undue delay.

For a security disclosure, include what you found, how to reproduce it and which pages or endpoints are affected. We acknowledge within 2 business days and give an initial assessment within 5 business days. We ask for reasonable time to fix an issue before public disclosure, and we take no legal action against researchers acting in

good faith.

The data processing agreement gives you an audit right once in any 12-month period, and more often following a personal data breach or where the ICO requires it.

Related documents:

- [Data processing agreement](#)
- [Security whitepaper](#)
- [Privacy policy](#)
- [Terms of use](#)
- [Cookies policy](#)

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

This document describes how the platform works. It is not legal advice. As controller you are responsible for your own lawful basis and, for anything revealing political opinions, your own Article 9 condition.