

Privacy policy

How Cadrify Ltd collects, uses and protects personal data, and the rights you have under the UK GDPR and the Data Protection Act 2018. Cadrify holds two roles: processor for the data a customer organisation uploads, controller for the data it collects to run the platform. This notice describes both.

Last reviewed 06/10/2026

Who we are

Legal entity	Cadrify Ltd
Registration	Registered in England and Wales, company number 17244539
ICO registration reference	ZC158949
Registered address	7 Malvern Road, Hornchurch, Essex, RM11 1BG
Privacy contact	privacy@cadrify.org

Purpose of this notice

This Privacy Policy explains how Cadrify Ltd ("Cadrify", "we", "us", "our") collects, uses and protects personal data in connection with the Cadrify platform and website (cadrify.org and any of its subdomains). It also explains the rights you have under the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018.

We may update this policy from time to time. The current version is always available at cadrify.org/privacy.

Our two distinct roles

Cadrify operates under two different legal roles depending on whose data is being processed.

1. Data processor, on behalf of customer organisations

When a political party, campaign or organisation ("Customer") subscribes to Cadrify and uploads or collects data through the platform, such as electoral register data, door-knock responses, voter contact records and supporter details, the Customer is the data controller. Cadrify processes that data only on the Customer's instructions, under a written Data Processing Agreement. Cadrify has no independent right to use, share or retain that data beyond what is needed to deliver the service.

Cadrify may engage trusted subprocessors to provide infrastructure, email delivery and related services. We maintain written agreements with all subprocessors as required by applicable data protection law. Where we engage a subprocessor to handle Customer data, we remain responsible for ensuring it provides equivalent protections.

If you are an elector, voter or supporter whose data has been entered into Cadrify by a political organisation, please contact that organisation directly to exercise your data rights. You may also contact us at privacy@cadrify.org and we will refer your request to the relevant Customer.

2. Data controller, for platform operations

Cadrify is the data controller for the personal data it collects directly from users and Customers for the purpose of operating the platform. This Privacy Policy primarily describes that processing.

What information we collect, use and why

Website visitors

When you visit cadrify.org we may automatically collect standard server log data, including IP address, browser type, referring URL and page requested. We use this information to maintain the security and performance of the website. Our lawful basis is legitimate interests (securing and operating the website). If you contact us by email, we will use your contact details to respond. Our lawful basis is legitimate interests (responding to enquiries).

Platform user accounts

When you register as a user of the Cadrify platform we collect:

- First name and surname
- Email address
- Password (stored as a one-way script hash, never in plain text)
- Profile picture (optional, uploaded by you)
- Role and branch memberships within your organisation
- Accessibility preferences (font size, button size)

We use this information to operate your account, authenticate you, manage your permissions and communicate with you about the service.

Security and session data

To protect accounts and detect abuse we also collect and store:

- IP address (recorded on login events and active sessions)
- Session tokens (stored in our database with a 24-hour expiry)
- Password reset tokens (short-lived, single-use)
- Login audit trail (timestamp, success or failure, IP address)
- Account lockout state (after repeated failed login attempts)

Customer account and billing information

When an organisation subscribes to Cadrify we collect the name and email address of the account holder for contract and billing purposes. Where card payment is used, card details are handled directly by our payment provider and are never stored by Cadrify.

Technical and usage data

When you use the platform or visit our website we may automatically collect:

- Browser type and version
- Operating system
- Referring URL and pages visited within the platform

Privacy policy

- Date, time and duration of sessions

We use this information to maintain platform security, troubleshoot issues and improve performance. We do not use third-party analytics within the platform. Our public website uses a cookieless, privacy-friendly analytics service that sets no cookies and does not profile visitors.

Lawful bases and data protection rights

Under UK data protection law we must have a "lawful basis" for processing your personal information. Our lawful bases are set out below.

Processing activity	Lawful basis
Website server logs and security monitoring	Legitimate interests
Responding to contact or support enquiries	Legitimate interests
Creating and managing your user account	Contract
Billing and subscription management	Contract
Platform security, fraud prevention, login audit trail	Legitimate interests
Sending service and security notifications	Contract / Legitimate interests
Marketing and promotional communications	Consent

Your rights

Under UK data protection law you have the following rights in relation to the personal data we hold about you as controller:

- Right of access: you can request a copy of the personal data we hold about you.
- Right to rectification: you can ask us to correct inaccurate or incomplete data.
- Right to erasure: you can ask us to delete your data in certain circumstances.
- Right to restrict processing: you can ask us to limit how we use your data.
- Right to data portability: you can request your data in a structured, machine-readable format.
- Right to object: you can object to processing based on legitimate interests.
- Right to withdraw consent: where processing is based on consent, you may withdraw it at any time.

To exercise any of these rights please contact us at privacy@cadrify.org. We will respond within one month.

Electoral register data and special-category data

The Cadrify platform is designed to handle electoral register data on behalf of Customer organisations. This data is subject to the Representation of the People Act 1983 (as amended) and is restricted to lawful purposes. Access to the full electoral register is permitted only for the purposes set out in law. Customers are responsible for ensuring they hold the correct lawful basis and permissions before uploading this data.

Door-knock data collected through the platform (including voting intentions, core party affiliation and support levels) may constitute special-category data relating to political opinions under Article 9 of the UK GDPR. Customers, as

Privacy policy

data controllers, are responsible for identifying and documenting their own lawful basis and Article 9 condition for processing this data, including, where applicable, Article 9(2)(d) for political parties, trade unions and certain not-for-profit bodies with a political, philosophical, religious or trade-union aim. Cadrify processes it only under their instructions.

Where a Customer has opted in, Cadrify matches the Electoral Commission's public register of donations (search.electoralcommission.org.uk) to electors on that Customer's register copy by name, and a Customer administrator confirms each match. A confirmed match links a published donation to a named party to an elector record and is special-category data relating to political opinions. The Customer, as data controller, is responsible for its Article 9 condition (in the ordinary case Schedule 1 paragraph 22 of the Data Protection Act 2018, as a registered political party), for telling the elector that the data was obtained from the Commission's register and for honouring an objection. Cadrify holds one copy of the public register as controller of that reference data and processes the Customer's links only under its instructions.

Returning officers must publish the names of the candidates at an election, the people who signed each candidate's nomination paper and the candidates' election agents. Cadrify holds one copy of those published notices as controller of that reference data, taken from the statements of persons nominated that Democracy Club archives (candidates.democracyclub.org.uk) and from the notices of poll and notices of election agents on each council's own website. For a Customer with elector data in the area, Cadrify links a name on a notice to an elector on that Customer's register copy, and only where one elector alone could be the person named. Signing a nomination paper for a named party reveals political allegiance, so the notices and the links are special-category data relating to political opinions. The condition Cadrify relies on is that the person made the data public themselves (Article 9(2)(e) of the UK GDPR), because the returning officer must publish the name of everyone who signs. The Customer, as data controller, is responsible for its own condition for the links, which Cadrify processes only under its instructions. A link can be removed from the elector record, which leaves the published notice unchanged.

Cadrify also holds one record of the candidates and councillors on principal councils, as controller of that reference data: the party each stood or sits for and every change of party since, their terms of office and the email address their council publishes for them. It is drawn from Democracy Club, Open Council Data (opencouncildata.co.uk) and each council's own website. To find a councillor's published email address, Cadrify sends search queries naming the councillor and their council to Brave Search, DuckDuckGo and Bing, and shows names, parties and council web pages to TypeSafe's Jev service, which matches a name to a person and picks the councillor's address from those on a page. Cadrify uses the record to send a supporter's email campaign to their own councillors. For a Customer with elector data in the area, it also links a candidate or councillor to an elector on that Customer's register copy and keeps that elector's stood for council and elected councillor flags current, so the Customer can leave them out of door-knocking rounds and leaflet drops. A party label is special-category data relating to political opinions, which a candidate makes public by standing under it and a councillor by sitting for it (Article 9(2)(e) of the UK GDPR). The Customer, as data controller, is responsible for its own condition for the links and flags, which Cadrify processes only under its instructions.

Where we store your data

The Cadrify platform is hosted by Render. Our primary database is located in Frankfurt, Germany (within the European Economic Area). The EEA is recognised under UK data protection law as providing an adequate level of protection for personal data.

International transfers

Where personal data is transferred outside the UK or EEA, we ensure appropriate safeguards are in place. Depending on the recipient and the nature of the transfer, the safeguard used will be one of:

Privacy policy

- UK adequacy regulations: where the destination country or territory has been assessed by the UK government as providing adequate protection (this covers EEA countries and certain other territories),
- UK-US Data Bridge: for transfers to US organisations certified under the UK Extension to the EU-US Data Privacy Framework, or
- UK International Data Transfer Agreement (IDTA) / Standard Contractual Clauses (SCCs): contractual safeguards approved by the ICO for transfers to countries without an adequacy decision.

Further details about the safeguards in place for any specific transfer can be requested by contacting privacy@cadrify.org.

Who we share information with

We do not sell personal data. We share it only with the processors listed below, each of whom is bound by a data processing agreement:

Provider	Purpose	Data location	Transfer basis
Render	Platform hosting and database	Frankfurt, Germany (EEA)	UK adequacy regulations (EEA)
Resend	Transactional email delivery (password resets, invitations, notifications)	Dublin, Ireland (EEA)	UK adequacy regulations (EEA)

We may also disclose personal data if required to do so by law, by a court order or by a regulatory authority, or where necessary to protect the rights, property or safety of Cadrify, its Customers or others.

Optional integrations you can connect

Cadrify offers optional integrations with external CRM and organising systems: Action Network, NationBuilder, Salesforce and Movement. These are off by default. An integration works only if your organisation chooses to enable it and connects it using your organisation's own account and credentials with that provider. Cadrify does not share your data with any of these services unless you set up the integration yourself.

When you enable an integration, Cadrify syncs supporter and volunteer contact records (such as name, email address, postcode, phone number where applicable and tags or subscription status) between Cadrify and the connected system, on your instruction. Electoral register records and door-knock data are never sent to these services. Because you connect the provider with your own account, that provider acts under your own relationship with it, and your use of it is governed by that provider's own terms. Some providers are based outside the UK or EEA. The providers, and links to each one's privacy and data-processing terms, are listed in Annex 4 of our Data Processing Agreement.

Third-party geocoding services

The platform uses external geocoding APIs to convert postcodes and addresses into map coordinates. We minimise the data sent to these services. Where possible, only postcodes are transmitted rather than full addresses or individually named data. The following services may be used in the course of this processing:

- postcodes.io: a free, UK-based open-data service used for postcode lookups.

Privacy policy

- Google Maps Geocoding API (optional, configured per installation): address-level geocoding. Where used, Google's privacy policy applies.
- OpenStreetMap Nominatim (optional, fallback): operated by the OpenStreetMap Foundation. Where used, OSMF's privacy policy applies.

Geocoding results are cached locally. The same data is not re-sent to external services once cached.

How long we keep information

Category	Retention period
Platform user accounts	For the duration of the subscription and 30 days post-termination
Billing and payment records	7 years from the relevant transaction (statutory financial records requirement)
Authentication and account log	No automatic deletion
Organisation audit log	Kept while the account is open. Deleted 30 days after it closes
Operator access log	Life of the platform
Application server logs	30 days
Session tokens	24 hours (or earlier on logout)
Password reset and invite tokens	Deleted on first use or on expiry (hours to days)
Customer-uploaded data (as processor)	As instructed by the Customer, or deleted automatically 30 days after the account is closed
Published donation links (Electoral Commission register matched to an elector, as processor)	Up to 10 years after the last matched donation, as set by the Customer, or 12 months after the elector leaves the register. Unconfirmed matches 180 days. Deleted on erasure
Published nomination notices (as controller) and their links to electors (as processor)	Notices are kept as the public statutory record. Links end 12 months after the elector leaves the register and are deleted on erasure
Councillor and candidate record (as controller) and its links and flags on electors (as processor)	Terms of office and party history are kept as the public record. A councillor's email address is deleted 12 months after Cadrify stops finding it on the council's website, or 12 months after their last term on the council ends. Links end 12 months after the elector leaves the register. Links and flags are deleted on erasure

Cookies

Cadrify uses a small number of strictly necessary cookies to keep you logged in and to maintain your session. We do not use advertising, tracking or third-party analytics cookies. For full details see our Cookies policy.

Security measures

We apply appropriate technical and organisational measures to protect personal data, including:

- Encryption of data in transit (TLS) and at rest
- Passwords stored using script hashing
- Role-based access controls restricting data access to authorised users only
- Login attempt throttling and account lockout after repeated failures
- Session tokens invalidated on logout and after 24 hours
- Access to personal data restricted through authentication and role-based authorisation controls

Intended users

The Cadrify platform is intended for political organisations, campaigns and authorised adult users. We do not knowingly collect personal data directly from children. If you believe a child has provided us with personal data, please contact privacy@cadrify.org and we will delete it promptly.

How to complain

If you have a concern about how we handle your personal data, please contact us first at privacy@cadrify.org so we can try to resolve it.

If you remain unhappy you have the right to complain to the Information Commissioner's Office (ICO):

Address	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Helpline	0303 123 1113
Online	ico.org.uk/make-a-complaint

Security

For information about the technical and organisational security measures Cadrify has in place, see the [Security overview](#) and the [Security whitepaper](#).

Contact us

For any questions about this policy or to exercise your data rights:

Email	privacy@cadrify.org
Post	Cadrify Ltd, 7 Malvern Road, Hornchurch, Essex, RM11 1BG

Privacy policy

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

Generated from app/domain/docs/content/privacy_policy.py. Do not edit an issued copy by hand.