

Data processing agreement

The Article 28 agreement between Cadrify Ltd, as processor, and the customer organisation, as controller. It sets out what Cadrify may do with the data you upload, the measures protecting it, the subprocessors and what happens to the data when the contract ends.

Last reviewed 06/10/2026

About this agreement

This Data Processing Agreement ("DPA") forms part of the agreement between Cadrify Ltd and the Customer for the provision of the Cadrify platform (the "Principal Agreement"). It governs the processing of personal data carried out by Cadrify, as processor, on behalf of the Customer, as controller. It sits alongside our Privacy Policy, Terms of use, Cookies policy and Security overview.

Where this DPA conflicts with the Principal Agreement on the subject of data protection, this DPA prevails. Capitalised terms not defined here have the meaning given in the Principal Agreement.

1. Parties

Processor	Cadrify Ltd ("Cadrify", "we", "us", "our"), registered in England and Wales, company number 17244539
Processor registered address	7 Malvern Road, Hornchurch, Essex, RM11 1BG
Processor data protection contact	privacy@cadrify.org
Controller	The organisation that has subscribed to the Cadrify platform under the Principal Agreement (the "Customer", "you", "your"), as identified in that agreement.

2. Definitions

The terms "controller", "processor", "data subject", "personal data", "special category data", "processing" and "personal data breach" have the meanings given in the UK GDPR.

UK GDPR	the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
Data Protection Laws	the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and all other laws relating to the processing of personal data applicable to the parties.
Customer Personal Data	any personal data processed by Cadrify on behalf of the Customer through the platform, as further described in Annex 1.
Subprocessor	any third party engaged by Cadrify to process Customer Personal Data.

3. Roles of the parties

The parties agree that, for Customer Personal Data, the Customer is the controller and Cadrify is the processor. Cadrify processes Customer Personal Data only on the documented instructions of the Customer, including as set out in this DPA, the Principal Agreement and the Customer's use and configuration of the Services in accordance with the Principal Agreement.

The Customer represents, and is responsible for ensuring, that it has a valid lawful basis under Article 6 of the UK GDPR, and where applicable a condition under Article 9, for all Customer Personal Data it uploads to or collects through the platform. Where Customer Personal Data includes electoral register data, the Customer is responsible for ensuring it holds that data and instructs its processing only for purposes permitted under the Representation of the People Act 1983 (as amended) and associated regulations. Where it includes door-knock data revealing political opinions, the Customer is responsible for identifying and documenting its Article 9 condition, including, where applicable, Article 9(2)(d).

Cadrify will inform the Customer if, in its opinion, an instruction infringes Data Protection Laws. Cadrify is not obliged to verify the legality of the Customer's instructions beyond this.

4. Independent controller processing

Separately from its role as processor, Cadrify acts as an independent controller for certain personal data it processes for its own business purposes, including Customer account administration, support communications, abuse and fraud prevention, records kept to meet its own legal and regulatory obligations, and, where billing applies, billing and payment records. This processing is described in the Privacy Policy and is not governed by this DPA.

5. Scope and duration of processing

The subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subject are set out in Annex 1. Processing continues for the duration of the Principal Agreement and any period after termination during which Cadrify retains Customer Personal Data in accordance with section 12.

6. Cadrify's obligations as processor

Cadrify will:

- process Customer Personal Data only on the Customer's documented instructions, unless required to do otherwise by law, in which case Cadrify will inform the Customer before processing unless that law prohibits it,
- ensure that persons authorised to process Customer Personal Data are subject to an appropriate duty of confidentiality,
- implement and maintain the technical and organisational measures set out in Annex 2,
- respect the conditions in section 8 for engaging Subprocessors,
- assist the Customer as set out in sections 9 and 10,
- at the Customer's choice, delete or return Customer Personal Data as set out in section 12, and
- make available to the Customer the information necessary to demonstrate compliance with the obligations in Article 28 of the UK GDPR, as set out in section 11.

7. Confidentiality

Cadrify treats all Customer Personal Data as confidential. Access is limited to personnel who need it to deliver, support or secure the service, each of whom is bound by confidentiality obligations. Cadrify does not sell Customer Personal Data and has no independent right to use, share or retain it beyond what is needed to deliver the service or as instructed by the Customer.

8. Subprocessors

The Customer grants Cadrify general authorisation to engage the Subprocessors listed in Annex 3. Cadrify imposes on each Subprocessor, by written contract, data protection obligations equivalent to those in this DPA. Cadrify remains fully liable to the Customer for the performance of each Subprocessor's obligations.

Cadrify will give the Customer reasonable prior notice of any intended addition or replacement of a Subprocessor, giving the Customer the opportunity to object on reasonable data protection grounds. If the Customer objects and the parties cannot agree a resolution, the Customer may terminate the affected part of the service.

Customer-enabled integrations are different from Subprocessors. Where the Customer chooses to connect an external system (for example a CRM) to the platform using the Customer's own account and credentials, that provider processes data under the Customer's own relationship with it, not as Cadrify's Subprocessor. These integrations are off by default and operate only after the Customer enables and configures them. They are described in Annex 4.

9. Assistance with data subject rights

Taking into account the nature of the processing, Cadrify will assist the Customer by appropriate technical and organisational measures, insofar as possible, to respond to requests from data subjects exercising their rights under Chapter III of the UK GDPR (including access, rectification, erasure, restriction, portability and objection).

Where a data subject contacts Cadrify directly about Customer Personal Data, Cadrify will not respond substantively but will, without undue delay, refer the request to the relevant Customer.

10. Assistance with security, breaches and impact assessments

Taking into account the nature of the processing and the information available to Cadrify, Cadrify will assist the Customer in ensuring compliance with its obligations under Articles 32 to 36 of the UK GDPR, including security of processing, personal data breach notification, data protection impact assessments and prior consultation with the ICO.

Breach notification. Cadrify will notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, in time to allow the Customer to meet its own notification obligations under Articles 33 and 34 of the UK GDPR (including the 72-hour deadline that applies to the Customer as controller). The notification will describe, to the extent known, the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences and the measures taken or proposed to address it. Cadrify will cooperate with the Customer and take reasonable steps to mitigate the breach. Cadrify will not notify data subjects or the ICO on the Customer's behalf unless instructed to do so in writing.

Cadrify provides reasonable assistance under this section and section 9 at no additional charge. Where the assistance the Customer requests is materially excessive, in particular extensive or repeated data protection impact assessment, audit or data subject request support, Cadrify may charge for it at reasonable rates, having first notified

the Customer.

11. Audits and information

Cadrify will make available to the Customer all information reasonably necessary to demonstrate compliance with Article 28 of the UK GDPR, including the Security whitepaper and the audit log records described in the Security overview.

Cadrify will allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer, on reasonable prior written notice and no more than once per twelve-month period (unless required by the ICO or following a personal data breach). Audits will be conducted during business hours, will not unreasonably disrupt Cadrify's operations and will respect the confidentiality and security of other customers' data. The Customer bears its own costs in connection with any audit.

12. Return and deletion of data

On termination or expiry of the Principal Agreement, and at the Customer's choice, Cadrify will return Customer Personal Data to the Customer in a structured, commonly used, machine-readable format, or delete it. Unless the Customer requests return or earlier deletion, Cadrify will delete Customer Personal Data from production systems 30 days after the Customer's account is closed, when its organisation is deleted automatically, and encrypted backups are removed on their normal retention cycle. Until then only the Customer's whole-organisation admins can open the account, to export Customer Personal Data or reopen it.

Cadrify may retain Customer Personal Data to the extent, and for as long as, required by law. Where retention is required, Cadrify will continue to protect it under this DPA and will process it only as necessary for the purpose of that legal requirement.

13. International transfers

Customer Personal Data at rest is stored within the European Economic Area (Frankfurt, Germany), which is covered by UK adequacy regulations. Cadrify will not transfer Customer Personal Data outside the UK or EEA except where an appropriate safeguard under Chapter V of the UK GDPR is in place, such as UK adequacy regulations, the UK Extension to the EU-US Data Privacy Framework (UK-US Data Bridge) or the UK International Data Transfer Agreement (IDTA) / Standard Contractual Clauses. The transfer basis for each Subprocessor is set out in Annex 3. Where the Customer enables an integration with an external system located outside the UK or EEA (see Annex 4), the resulting transfer is made on the Customer's instruction and under the Customer's own relationship with that provider, and the Customer is responsible for the transfer safeguards that apply to it.

14. Liability

Each party's liability arising out of or in connection with this DPA is subject to the limitations and exclusions of liability set out in the Principal Agreement. Nothing in this DPA limits either party's liability where it cannot lawfully be limited.

15. Changes to this DPA

Cadrify may update this DPA from time to time to reflect changes in law, regulatory guidance or its processing operations. The current version is always available at cadrify.org/dpa, with the date of the latest revision shown at the top. Where a change materially reduces the protections that apply to Customer Personal Data, Cadrify will give

the Customer reasonable prior notice. Continued use of the platform after a change takes effect constitutes acceptance of the updated DPA.

16. Term and governing law

This DPA takes effect on the start date of the Principal Agreement and remains in force for as long as Cadrify processes Customer Personal Data. It is governed by the laws of England and Wales, and the parties submit to the exclusive jurisdiction of the courts of England and Wales.

Annex 1: Details of processing

Subject matter	Provision of the Cadrify electoral campaign management platform to the Customer.
Duration	For the term of the Principal Agreement, plus the retention period in section 12.
Nature and purpose	Storage, organisation, retrieval and processing of voter and supporter data to support lawful political campaigning, including managing the electoral register, door-knocking rounds, get-out-the-vote activity, activist coordination, nominations and leaflet drops.
Categories of data subject	Electors and members on the register. Supporters and contacts recorded by the Customer. The Customer's own staff, organisers and activists who hold platform accounts.
Types of personal data	Names, postal addresses, electoral register entries (including GSS-coded geography), contact details, door-knock responses and voting intentions, support levels, activity and assignment records and platform account data (names, email addresses, roles, branch memberships).
Special category data	Door-knock data may reveal political opinions (Article 9 UK GDPR). The Customer is responsible for its Article 9 condition. No other special category data is intended to be processed.

Annex 2: Technical and organisational measures

Cadrify maintains the following measures. Further detail is in the Security overview and Security whitepaper.

- Encryption in transit: all connections use TLS (HTTPS). Unencrypted HTTP is not permitted.
- Encryption at rest: the database is encrypted at rest by the underlying storage infrastructure.
- Passwords: stored using a modern, memory-hard password hashing algorithm, never stored in plain text and subject to minimum complexity requirements.
- Access control: a tiered, role-based permission model. Data access is restricted to authorised users and scoped to the relevant branch or ward.
- Separation between organisations: every record is bound to a single organisation and queries are scoped so one organisation cannot read or modify another's data.
- Login protection: automatic account lockout after repeated failed attempts, server-level rate limiting and generic error messages.
- Sessions: time-limited authenticated sessions using cryptographically random tokens stored as secure, HttpOnly cookies, with secure invalidation on logout and on password change.

- Audit logging: logs of security-relevant events (sign-ins, password changes, user and role changes, invite tokens, support access) and of data changes and exports, which platform users cannot edit. When an erasure request is approved, audit entries about that person keep who did what and when and lose the details that describe them, and an organisation's audit and export entries are deleted when the organisation is deleted.
- Time-limited activist access: activists see only doors and electors assigned to a specific round. Access expires when the round expires and can be revoked at any time.
- Backups and resilience: managed, encrypted backups via the hosting infrastructure.
- Breach response: documented incident response with notification to affected Customers without undue delay.

Annex 3: Authorised subprocessors

Engaged for every Customer:

Provider	Purpose	Data location	Transfer basis
Render	Application hosting and the PostgreSQL database	Frankfurt, Germany (EEA)	UK adequacy regulations (EEA)
Resend	Platform email: password resets, invitations, verification and notifications	Dublin, Ireland (eu-west-1, EEA)	UK adequacy regulations (EEA)
Stripe	Subscription billing, and donation or ticket payments where the Customer uses them. Card details are entered on a Stripe-hosted page and are never processed or stored by Cadrify	Ireland and the United States	Standard Contractual Clauses
postcodes.io	Postcode-level geocoding. Receives postcodes only	Britain	None needed, processing is in Britain
mySociety MapIt	Ward, constituency and local authority boundaries by GSS code. Receives no personal data	Britain	None needed, processing is in Britain

Render hosts the application and the database, so it processes all Customer Personal Data, including electoral register data and door-knock records, in Frankfurt. Resend receives platform email only: the recipient's name and email address and the message content. Stripe processes billing and payment data only, and never receives electoral register data or door-knock records.

Engaged only where Cadrify has enabled the feature for the Customer:

Provider	Purpose	Data location	Transfer basis
Anthropic	AI features. What each feature sends is set out in the Security overview	Outside the UK and EEA	On request from privacy@cadrify.org

Data processing agreement

Provider	Purpose	Data location	Transfer basis
OpenAI	AI features, where a deployment is configured to use it instead of Anthropic	Outside the UK and EEA	On request from privacy@cadrify.org
Google Maps Platform	Per-address geocoding. Receives address text with no name attached	The provider's own infrastructure, not Cadrify's EEA hosting	On request from privacy@cadrify.org
Nominatim (OpenStreetMap Foundation)	Per-address geocoding where no Google key is configured. Receives address text with no name attached	The provider's own infrastructure, not Cadrify's EEA hosting	On request from privacy@cadrify.org

AI features are off unless Cadrify enables them for the Customer. Where none is enabled, no Customer Personal Data reaches an AI provider. Per-address geocoding is likewise enabled per Customer. Postcode-level geocoding, the default path, uses neither Google Maps Platform nor Nominatim.

Annex 4: Customer-enabled integrations

The platform offers optional integrations with external CRM and organising systems. These are off by default. An integration operates only where the Customer chooses to enable and configure it, using the Customer's own account and credentials with that provider. For these integrations the provider processes data under the Customer's own relationship with it: the provider is the Customer's processor or independent controller, not Cadrify's Subprocessor, and the Customer is responsible for its own agreement (including any data processing agreement) and lawful basis with that provider.

When the Customer enables an integration, Cadrify, on the Customer's instruction, exchanges supporter and volunteer contact records (such as name, email address, postcode, phone number where applicable and tags or subscription status) with the connected system. Electoral register records and door-knock data are never included in any integration.

Integration	Operator	Data location	Provider terms
Action Network	Action Squared, Inc.	United States	Privacy · Data Processing Terms · Terms
NationBuilder	3dna Corp.	United States (EU-US Data Privacy Framework, UK Extension)	Privacy · DPA · Subprocessors · Terms
Salesforce	Salesforce, Inc.	The Customer's own Salesforce instance	Privacy · Agreements (MSA / DPA) · Trust and compliance
Movement	Movement Industries Ltd (England and Wales)	EEA (Frankfurt, Germany)	Privacy · Trust Vault. DPA and terms provided by Movement on request

The provider terms named in the table above:

- Action Network, privacy <https://actionnetwork.org/privacy/>
- Action Network, data processing terms <https://actionnetwork.org/data/>

Data processing agreement

- Action Network, terms <https://actionnetwork.org/terms/>
- NationBuilder, privacy <https://nationbuilder.com/privacy>
- NationBuilder, DPA <https://nationbuilder.com/dpa>
- NationBuilder, subprocessors <https://nationbuilder.com/subprocessors>
- NationBuilder, terms <https://nationbuilder.com/tos>
- Salesforce, privacy <https://www.salesforce.com/company/legal/privacy/>
- Salesforce, agreements (MSA / DPA) <https://www.salesforce.com/company/legal/customer-agreements/>
- Salesforce, trust and compliance <https://compliance.salesforce.com/>
- Movement, privacy <https://www.yourmovement.org/privacy-policy>
- Movement, trust vault <https://trust.yourmovement.org/>

Because some of these providers are located outside the UK and EEA (for example in the United States), enabling an integration may involve a transfer of contact data outside the UK or EEA. That transfer is made on the Customer's instruction and under the Customer's own relationship with the provider, and the Customer is responsible for the transfer safeguards that apply to it. The links above are provided so the Customer can review each provider's terms before enabling an integration.

Broadcast email sent in the Customer's own name goes through an email provider the Customer connects itself: Resend, Amazon SES, Mailgun, Postmark or the Customer's own SMTP server. That provider works under the Customer's own relationship with it, not as Cadrify's Subprocessor, and the recipient list and message content reach it on the Customer's instruction. Cadrify's own Resend account carries platform email only.

Contact

For questions about this DPA or to exercise rights under it:

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

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/data_processing_agreement.py`. Do not edit an issued copy by hand.