



# Data Protection and Privacy

*What personal information is collected, why it is used, and how it is protected*

**ADCN (Albanian Diaspora Civic Network)** is a volunteer-led civic network, not a registered organisation or separate legal person. **ADCN** uses its own governance, safeguards and public-facing standards. References to “**ADCN**” in this document describe the network’s agreed rules and working practices.

## SCOPE AND APPLICABLE LAW

ADCN works across Albania and the diaspora. Personal-data obligations therefore depend on the activity, the people involved, where processing takes place and the actual controller. Where applicable, processing should meet the standards of **Albania’s Law No. 124/2024 “On the Protection of Personal Data”**, the **EU GDPR**, the **UK GDPR/Data Protection Act** framework and any other mandatory local rules.

## CORE PRINCIPLES

- Lawfulness, fairness and transparency.
- Specified and legitimate purposes.
- Data minimisation - collect only what is reasonably necessary.
- Accuracy and a route to correct errors.
- Retention only for as long as there is a justified need.
- Security and restricted access proportionate to risk.
- Accountability - be able to show what was decided and why.

## CATEGORIES OF INFORMATION

Depending on the activity, ADCN-related work may involve contact details, membership or volunteer records, areas of expertise, availability, participation records, event or consent records, complaint information, correspondence, media permissions and limited technical/access logs. Projects must not collect identity documents, special-category information or other high-risk data merely because it might be useful later.

## PURPOSE AND LAWFUL BASIS

Before collection, the responsible controller should define the purpose and appropriate lawful basis. Consent is used only where it is genuinely appropriate and freely given; it is not a catch-all legal basis. Other lawful bases may apply depending on the jurisdiction and activity. Special-category or highly sensitive data requires an additional legal condition where the law requires one.

## REFERENDUM AND SIGNATORY DATA

Official referendum signatures and identity information are collected and governed according to the applicable constitutional, electoral and CEC process. ADCN should not create an unofficial parallel database of identity-document details unless there is a clearly defined lawful purpose, controller, security design and retention rule.

Where ADCN supports administrative checking, duplicate prevention or volunteer coordination, use the least intrusive method reasonably available. Signatory or supporter data must not be repurposed for unrelated political campaigns, sold, or added to general marketing lists without a separate lawful basis and appropriate notice.

## ACCESS, STORAGE AND SHARING

- Give access only to people who need it for the stated purpose.
- Use managed accounts, strong authentication and secure storage appropriate to the sensitivity of the data.
- Do not download or copy datasets to personal devices unless necessary and approved.
- Share only the minimum data necessary with partners, service providers or authorities, and identify the legal/operational basis for doing so.
- Use appropriate safeguards for international transfers where required by applicable law.

## RETENTION AND DELETION

Each project should set a retention rule before or at collection. At project closure, data should be reviewed and deleted or anonymised when no longer necessary, unless a legal, audit, complaint, safety or evidential reason justifies continued retention. Backup and archive copies should follow the same principle as far as technically reasonable.

## INDIVIDUAL RIGHTS AND PRIVACY REQUESTS

Where applicable law provides rights of access, correction, deletion, restriction, objection, portability or complaint, the responsible controller should provide a clear route to exercise them. Requests sent to **team@albaniandiasporacivicnetwork.com** should be routed promptly to the actual controller and handled within the time required by the applicable law.

## DATA INCIDENTS AND BREACHES

A suspected loss, unauthorised disclosure, account compromise, malicious access or accidental sharing of personal data should be reported immediately to the privacy contact. Preserve evidence, limit further exposure, assess risk and identify whether the actual controller has a legal duty to notify affected individuals or a supervisory authority within a statutory period.

## PRIVACY BY DESIGN

New forms, databases, mailing lists, platforms and campaigns should be designed to minimise data from the start. High-risk or large-scale processing should be assessed before launch, including who controls the data, access levels, security, retention, sharing, international transfers and how people will be informed.

## CONTACT AND REVIEW

Privacy contact: **team@albaniandiasporacivicnetwork.com**. This policy should be reviewed whenever ADCN begins a materially new data activity or the applicable legal framework changes.

*The workstream names or internal allocation may evolve.*

*Any change must preserve the responsibilities covered by this Charter and be recorded transparently.*

UPDATED 2026