

Data Protection Policy – African American Equity Impact Scorecard

The African American Alliance of CDFI CEOs (hereafter, “The Alliance”) is a membership-driven intermediary organization that aims to: build the capacity of member organizations; build bridges to economic stability, well-being, and wealth for Black individuals, families, and communities; and build power in Black communities by challenging and influencing financial sectors to operate more equitably.

Community Vision Capital & Consulting (hereafter, “Community Vision”) is a California based CDFI whose mission is to promote economic justice and alleviate poverty by increasing the financial resilience and sustainability of community-based nonprofits and enterprises. Through flexible financial products and sound advice, we create opportunities to make socially responsible investments that revitalize Northern and Central California communities.

Definitions

- **Scorecard** – The African American Equity Impact Scorecard (or The Scorecard) is designed to help CDFIs, grantmakers, banks and other financial institutions guide and assess their impact on wealth-building among Black communities. The Scorecard aims to shift the criteria by which organizations assess every project by quantifying a financial institution’s investment in Black leadership development, power-building, and wealth creation.
- **Personal Data** - refers to any information that identifies or relates to an individual person or applicant, client, or employee of a participating organization. The data includes information such as name, identification number, location, or any other factors specific to the identity of that individual.
- **Project Data** - refers to any information that identifies or relates to a project that is being evaluated using the Scorecard assessment tool. The data includes information such as location, budget, scope, funding decision, scorecard assessment results or any other factors specific to the project.
- **Organizational Data** - refers to any information that identifies or relates to participating organizations, stakeholders, customers, or interested parties. The data includes information such as collective project submissions, assessment results, financial data, or any other factors specific to the organization.

Purpose

The Scorecard Data Protection Policy refers to our commitment to treat information of partners, stakeholders, customers, employees, and other interested parties with care and confidentiality. With this policy, we ensure that we collect, store and process data fairly, transparently and with respect towards individual rights.

Scope

The policy applies to all personal, project, and organizational data processed for the Scorecard and all parties that provide any information to us for the Scorecard.

Data Protection Principles

As part of our organization's work and the goals of the Scorecard, we must collect and process data. Our organization collects this data in a transparent and robust way and only with the full cooperation and knowledge of interested parties. Our organization is committed to processing data responsibly to ensure that data is:

- a. Collected and processed fairly, transparently and for lawful purposes only;
- b. Accurate and, where necessary, kept up-to-date;
- c. Collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- d. Processed to ensure appropriate security of personal data, project data, and organization data;
- e. Aggregated responsibly to remove any personal, project, or organizational identifiers.
- f. Protected against any unauthorized or illegal access by internal or external parties and against accidental loss, destruction, or damage

Data Protection Commitment

To exercise data protection, we're committed to:

- Restrict and monitor access of personal data to authorized users only and prohibit the selling of personal data to any third parties.
- Restrict and monitor access of project and organizational data and prohibit sharing of individual project data or organizational data unless authorized in writing by participating organization.
- Limit the personal data, project data, and organizational data collected to only what is necessary to the purposes for which they are processed
- Share aggregated data only and take reasonable steps to remove any personal, project or organizational identifiers prior to producing and sharing reports, analysis, or insights
- Provide users access to their personal data, project data, and organizational data and respond to requests to access data in a timely manner
- Take reasonable steps to ensure data is accurate and allow requests to modify or correct data contained in our databases
- Keep users informed of which data is collected, how data is processed, and who has access to their information
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks and establish procedures for reporting privacy breaches or data misuse
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization, etc.)

I acknowledge receipt of the Data Protection Policy and agree with the policies and guidelines outlined.

Signature