



FUNDERS FOR LGBTQ ISSUES DATA SECURITY POLICY

August 2026

Table of Contents

1. Introduction and Purpose	2
2. Data Collection and Use	2
3. Data Security Measures	3
4. Data Breach Response	3
5. Policy Review and Updates	3
6. Anonymization and Data Handling	4
7. Retention and Deletion of Grantmaker Data	4
8. Security Training	4
9. Data Sharing with Third Parties	5
10. Compulsory Legal Process	5
11. Feedback and Concerns	5

1. Introduction and Purpose

Funders for LGBTQ Issues ("the Organization") has, for over two decades, reported on foundation funding for LGBTQ communities and issues domestically and globally. Utilizing grant-level data submitted by grantmakers and publicly available data, the Organization produces an annual Resource Tracking Report, analyzing and publishing data to inform strategic philanthropic organizing initiatives and create avenues for transformative changes in LGBTQ grantmaking. Recognizing the paramount importance of data security, this policy outlines the measures the Organization will take to safeguard data submitted by funders and to ensure compliance with current best practices and industry standards.

By adhering to this comprehensive Data Security Policy, the Organization commits to maintaining appropriate standards of data security and privacy, consistent with all applicable laws, to ensure the trust and confidence of our stakeholders in the integrity of our data-handling practices. Although these safeguards are reasonable, given the inherent risk in electronic transmission and storage of information, we cannot guarantee that there will never be an instance of unauthorized access, unauthorized disclosure, or loss of the submitted information.

2. Data Collection and Use

The Organization collects data that is submitted by grantmakers, as well as data from public databases such as Candid, IRS Form 990s, foundation annual reports, and grantee websites. Collected data are utilized to produce the annual Resource Tracking Report and various specialty reports, articles, infographics, blogs, and online tools. Data requests from members and LGBTQIA+ nonprofit organizations are fulfilled based on staff capacity and alignment with the Organization's mission.

3. Data Security Measures

The Organization imposes robust access controls and other protective measures for grantmaker-submitted data (with access restricted to relevant Organization staff and consultants) and conducts regular security audits.

4. Data Breach Response

The Organization has processes for detecting, assessing, containing, and mitigating potential data breaches. In the event of a data breach, affected parties will be notified in accordance with legal and regulatory requirements.

5. Policy Review and Updates

This policy will be reviewed at least annually to align with industry standards and best practices. Interim updates may be made in response to new regulatory requirements, technological advancements, or identified security vulnerabilities. The updated policy will be posted on the Organization's website.

6. Anonymization and Data Handling

Where feasible, the Organization uses data anonymization methods such as data masking, pseudonymization, and aggregation to protect the identity of grantmakers and grantees and their funding relationships.

Grantmakers can request anonymization of their data at the time of submission via the provided submission template or by direct communication with the Organization.

7. Retention and Deletion of Grantmaker Data

Raw data submitted by grantmakers and internal analyses of that data will be retained for seven years. After seven years, this data will be securely deleted using methods that ensure it cannot be recovered (e.g., data shredding, secure wipe) unless otherwise required by law.

8. Security Training

All employees of the Organization participate in cybersecurity awareness training upon hire, followed by periodic refresher training and exercises.

Relevant Organization personnel further participate in training regarding human subjects protections, as well as regulatory and ethics issues related to research conduct.

9. Data Sharing with Third Parties

Data shared with third parties, including but not limited to the Global Philanthropy Project (GPP) and Funders Concerned About AIDS (FCAA), shall be governed by strict confidentiality agreements and shall comply with the same security standards upheld by the Organization. These data, encompassing LGBTQ grant information, geographic and population information, and any other relevant data, shall be utilized exclusively for the purposes of conducting research and analysis pertinent to LGBTQI grantmaking initiatives and resource tracking.

A formal data sharing agreement will be signed by all third parties, specifying the terms and conditions of data use, security, and protection.

10. Compulsory Legal Process

In the event the Organization is subject to a subpoena or other compulsory legal process requiring the production of data from, or communications with, a submitting grantmaker, the Organization will, to the extent legally permitted and reasonably feasible, take steps to notify the affected grantmaker and use reasonable efforts to consult with the grantmaker, including by providing an opportunity for the grantmaker to seek judicial relief with respect to the compulsory process.

11.Feedback and Concerns

We encourage third parties to provide feedback and share concerns or questions regarding this policy to ensure it meets the needs of the philanthropic sector focused on LGBTQ communities and causes. Should your organization have additional concerns not adequately addressed by this policy, we are open to developing an organization-specific policy to enable your full participation in the Resource Tracking Report Project and other research projects. Please share your feedback with us by reaching out via email to research@lgbtfunders.org.