FUNDERS FOR LGBTQ ISSUES DATA SECURITY POLICY

August 2024

Table of Contents

FUNDERS FOR LGBTQ ISSUES

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.

2. Definitions

Confidential Information: All non-public data pertaining to the operations, systems, services, personnel, financial affairs, strategies, and other proprietary information of the Organization or its stakeholders.

Data Security: Measures employed to protect data from unauthorized access, disclosure, alteration, and destruction.

Anonymized Data: Data that has been processed to remove or obscure personal identifiers and funding relationships between grantmakers and grantees, making it virtually impossible to identify individual funding relationships from the data set.

3. Data Collection and Use

- Data Sources: The Organization collects data that is submitted by grantmakers, as well as public databases such as Candid, IRS 990 forms, foundation annual reports, and grantee websites.
- Data Utilization: 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.

4. Data Security Measures

The Organization is transitioning from Dropbox to Google Drive and OneDrive for file storage, with access restricted to relevant Funders staff and related consultants. While these platforms do not encrypt folders by default, they offer robust access controls. Multi-factor authentication (MFA) is required for accessing sensitive data. Regular security audits are conducted by CMIT, an outsourced tech provider, to identify and address vulnerabilities, and our data security policy is reviewed annually or as needed to ensure compliance with current best practices and industry standards.

5. Data Breach Response Plan

1. Incident Reporting: All data breaches must be reported immediately to the Director of Research, who will coordinate the response with relevant staff at the Organization.
2. Mitigation Steps: Upon detection of a data breach, immediate steps will be taken to assess, contain, and mitigate the impact of the breach.
3. Notification: Affected parties will be notified of the breach in accordance with legal and regulatory requirements.
4. Documentation: All breaches and the corresponding response actions will be documented for review and future prevention.

6. Policy Review and Update Procedures

This policy will be reviewed annually every July by key members of the Organization's leadership and Board of Directors as part of the debriefing process from developing the last Resource Tracking Report and in preparation for the next one. Interim updates may be made in response to new regulatory requirements, technological advancements, or identified security vulnerabilities. All reviews and updates will be documented, with changes communicated to all relevant stakeholders. Feedback from Funders staff and the Board will be solicited during these reviews, and the updated policy will be posted on the Organization’s website.

FUNDERS FOR LGBTQ ISSUES

7. Anonymization and Data Handling

- Anonymization Techniques: Data anonymization methods such as data masking, pseudonymization, and aggregation will be employed to protect the identity of grantmakers and grantees and their funding relationships.
- Data Submission: Grantmakers can request anonymization of their data at the time of submission via the provided submission template or by direct communication with the Research Team.

8. Data Retention Policy

Data will be retained indefinitely to allow for ongoing trend analysis over time. After seven years, data no longer required for analysis will be securely deleted using methods that ensure it cannot be recovered (e.g., data shredding, secure wipe) unless otherwise required by law.

9. Security Training

Effective August 15th, all employees of the Organization will be required to participate in a Security Awareness Training program delivered remotely via a provided link. This program consists of educational videos, each lasting between 3-5 minutes, followed by brief assessments comprising 4-6 questions to test subject knowledge. Initially, employees must complete six foundational videos, with subsequent monthly releases of one new video. Before commencement, each user will receive a CMIT Welcome Email. The training will begin with an Introductory Video, followed by access to all active videos available at the time of onboarding, totaling up to nine videos. Additionally, every three months, starting on the eighth day after the initial video launch, employees will participate in a phishing simulation/test. The program includes ongoing monitoring and alerts for any new exposures identified on the Dark Web. This comprehensive training initiative is designed to enhance and maintain cybersecurity awareness and practices of all staff members.

Staff on the Research Team are required to complete the Social-Behavioral-Education (SBE) Foundations Course through the CITI

Program, which provides foundational training covering the major topical areas in human subjects protections, as well as regulatory and ethics issues related to research conduct. Key research consultants are also required to complete this training.

10. 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 Funders for LGBTQ Issues. 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.

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

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.

12. Conclusion

By adhering to this comprehensive Research Data Security Policy, Funders for LGBTQ Issues commits to maintaining the highest standards of data security and privacy to ensure the trust and confidence of our stakeholders in the integrity of our data handling practices.

FUNDERS FOR LGBTQ ISSUES