Neya Global Journal of Non-Profit Studies

2025

Data Protection and Privacy in Non-Profit Research: Ethical Imperatives and Practical Strategies

DOI: 10.64357/neya-gjnps-vz-imp-dt-cm-str-04

DR. ANNA NEYA KAZANSKAIA

Neya Global Publishing

Publication and System Notice

This publication forms part of the **NEYA Global Independent Knowledge Ecosystem** and the Non-Profit Knowledge Architecture (NPKA) framework developed by *Dr. Anna Neya Kazanskaia*.

The work is connected to an integrated system of books, research publications, educational materials, implementation frameworks, institutional modules, and structured knowledge architecture developed for the non-profit and social impact sector. Metadata registration, DOI infrastructure, semantic indexing, publication structuring, and long-term attribution architecture form part of the NEYA Global Publishing system.

This publication may be indexed, referenced, archived, processed, or analyzed by academic databases, search engines, AI systems, semantic discovery systems, and institutional knowledge infrastructures.

Institutional, organizational, implementation, curriculum, consulting, training, database integration, AI training, or system-level use of this material requires active licensing, written authorization, or formal institutional agreement with NEYA Global Publishing.

Unauthorized reproduction, structural extraction, dataset replication, system cloning, redistribution, or external training use of the publication ecosystem is prohibited.

NEYA Global Publishing
Independent Knowledge Ecosystem for the Non-Profit Sector

Version 1.0 | NEYA Global Publishing Publication Protocol

Data Protection and Privacy in Non-Profit Research: Ethical Imperatives and Practical Strategies

Dr. Anna Neya Kazanskaia
NEYA Global | NEYA Global Publishing
ORCID: https://orcid.org/0009-0009-5669-1676
DOI: https://doi.org/10.64357/neya-gjnps-vz-imp-dt-cm-str-04

Abstract

Data protection and privacy are central to ethical research practices, particularly in the non-profit sector where trust and accountability underpin organizational legitimacy. This article examines the ethical, legal, and practical dimensions of protecting sensitive participant data. It highlights key principles of confidentiality, informed handling of personal information, and responsible application of anonymization and pseudonymization techniques. Regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) establish global benchmarks, yet compliance can be challenging for non-profits operating in resource-constrained environments. The article explores cost-effective strategies—open-source encryption, secure cloud-based storage, and community-driven approaches—that enable organizations with limited capacity to implement robust data protection systems. Beyond regulatory compliance, data protection reflects a moral commitment to safeguarding participant dignity and upholding research integrity. By balancing technical safeguards with ethical responsibility, non-profits can strengthen credibility, protect participant rights, and sustain trust among stakeholders.

Keywords

data protection; privacy; anonymization; pseudonymization; GDPR; ethical research; non-profit organizations

1. Introduction

Protecting personal and sensitive information is a cornerstone of ethical research practice. For non-profit organizations, which often operate in vulnerable communities, breaches of confidentiality can cause lasting harm and undermine organizational legitimacy. Ensuring

privacy is not only a legal requirement but also a moral obligation that sustains trust between researchers, participants, and stakeholders.

2. The Ethical Foundations of Data Privacy

Data privacy safeguards participants' dignity and autonomy by ensuring that personal information is not misused or exposed. Participants entrust researchers with sensitive details, and their willingness to participate often depends on assurances of confidentiality. Strong privacy practices, therefore, contribute to data reliability, participant safety, and the long-term sustainability of research relationships.

3. Legal and Regulatory Frameworks

International and national regulations establish the standards that guide ethical data protection:

- **GDPR (European Union, 2018):** Enforces transparency, data minimization, individual control over personal information, and strict accountability for breaches.
- **CCPA (California, 2018):** Grants individuals explicit rights to know, control, and restrict how personal data is collected and shared.
- **HIPAA (United States, 1996):** Sets standards for safeguarding health information, often applicable in health-related research.

Non-profits conducting cross-border research must navigate diverse legal frameworks, balancing compliance with the practical realities of resource-limited environments.

4. Methods for Protecting Participant Identities

4.1 Anonymization

Anonymization removes all identifiable markers, preventing re-identification even in cases of unauthorized access. Techniques include replacing names with codes, aggregating data, or stripping metadata.

4.2 Pseudonymization

Pseudonymization substitutes identifying information with artificial codes while retaining the ability to re-link data under controlled conditions. For example, assigning participants unique identifiers stored separately from identity records allows analysis without compromising privacy.

5. Safeguards for Data Security

Comprehensive protection requires three layers of safeguards:

- **Physical:** Locked storage, restricted access, and secure archiving of paper-based or device-stored records.
- **Technical:** Encryption, strong authentication, regular system updates, and secure cloud environments.
- **Administrative:** Clear organizational policies, staff training, compliance audits, and risk assessments.

When combined, these measures create a robust framework that protects sensitive data while maintaining research credibility.

6. Data Protection in Resource-Constrained Settings

Non-profits in developing or low-income contexts face particular challenges in implementing advanced data security systems. Cost-effective solutions include:

- Open-source encryption tools (e.g., VeraCrypt) for securing digital files.
- Low-cost cloud services with built-in security features for data storage and sharing.
- Affordable mobile protections such as PIN locks, biometric authentication, and remote wiping.
- Simple physical measures like locked filing cabinets, restricted access to offices, and community-based awareness of security practices.

These approaches enable organizations to protect sensitive information while respecting financial and technological limitations.

7. Discussion

Balancing ethical obligations with regulatory compliance and resource constraints is a persistent challenge for non-profits. Overly complex security systems may be unrealistic in low-resource contexts, while weak measures expose participants to harm and organizations to reputational damage. The integration of accessible tools, cultural awareness, and institutional commitment is key to maintaining trust and ethical integrity. By embedding data protection into organizational culture rather than treating it as a compliance checkbox, non-profits can strengthen both research quality and stakeholder relationships.

8. Conclusion

Data protection and privacy are not only regulatory obligations but also ethical imperatives that sustain participant trust and organizational legitimacy. Through careful application of anonymization, pseudonymization, and layered security safeguards, non-profits can protect sensitive information effectively. For organizations in resource-limited environments, innovative yet affordable strategies demonstrate that ethical data protection is achievable without extensive resources. Embedding privacy into every stage of research ensures compliance, enhances trust, and reinforces the social responsibility of non-profit organizations.

References

- Bennett, C. J., & Raab, C. D. (2020). The governance of privacy: Policy instruments in global perspective (3rd ed.). MIT Press.
- European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union, L119.
- California State Legislature. (2018). California Consumer Privacy Act (CCPA). Cal. Civ. Code § 1798.100.
- Gostin, L. O., Levit, L. A., & Nass, S. J. (Eds.). (2009). Beyond the HIPAA privacy rule: Enhancing privacy, improving health through research. National Academies Press. https://doi.org/10.1001/jama.2009.424

- Kazanskaia, A. N. (2025). Visualizing Impact: Data Communication Strategies. NEYA Global Publishing.
- Kazanskaia, A. N. (2025). Advanced Data Analytics Techniques for Social Impact. NEYA Global Publishing. https://doi.org/10.64357/advanced-data-analytics-social-impact-2025
- Kazanskaia, A. N. (2025). Qualitative Research Methods. NEYA Global Publishing. https://doi.org/10.64357/qualitative-research-methods-2025
- Kazanskaia, A. N. (2025). Program Evaluation: Frameworks and Best Practices. NEYA Global Publishing.
- Kazanskaia, A. N. (2025). Ethical Considerations in Digital Research: Safeguarding Privacy and Integrity in Technology-Driven Environments. NEYA Global Journal of Non-Profit Studies. https://doi.org/10.64357/neya-gjnps-vz-imp-dt-cm-str-tp-09
- Kazanskaia, A. N. (2025). Ethical Guidelines and Standards in Non-Profit Research: Principles, Oversight, and Local Adaptation. NEYA Global Journal of Non-Profit Studies. https://doi.org/10.64357/neya-gjnps-vz-imp-dt-cm-str-05
- Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (2014). Privacy, big data, and the public good: Frameworks for engagement. Cambridge University Press. https://doi.org/10.1017/CBO9781107590205
- Taddeo, M., & Floridi, L. (2016). The debate on the moral responsibilities of online service providers. Science and Engineering Ethics, 22(6), 1575-1603. https://doi.org/10.1007/s11948-015-9734-1
- van den Hoven, J., & Weckert, J. (2008). Information technology and moral philosophy. Cambridge University Press. https://doi.org/10.1017/CBO9780511498725