Data Retention Policy

Last Updated: December, 2025

The Scope

This Data Retention Policy (the "**Policy**") outlines how Code for Canada may collect, use, store, retain, and securely destroy your personal, organizational and project data in accordance with the *Ontario Not-for-Profit Corporations Act (ONCA)* and applicable Canadian privacy laws, including the *Personal Information Protection and Electronic Documents Act (PIPEDA)*.

It applies to all data that may be collected from you through our website, partner projects, programs (such as IUR/GRIT), usability testing sessions, and third-party tools used to support our operations, research, and service delivery.

The Purpose

The purpose of this Policy is to ensure that all data we collect from you is:

- Collected for specific, legitimate purposes;
- Retained only as long as necessary to fulfill those purposes;
- Protected against unauthorized access, loss, or misuse; and
- Securely destroyed or anonymized using reasonable efforts once your data is no longer required.

Information We Collect

Depending on your interaction with Code for Canada, we may collect and process the following types of information about you:

- **User Information:** Name, email address, city, province, and phone number.
- **Technical Data:** IP address, browser type, time zone, plug-ins, operating system, and device type.

- **Usage Data:** Website interactions, navigation patterns, and device actions collected through cookies or similar technologies.
- **Demographic Information:** Age, race, gender, preferred language, and employment status (as voluntarily provided by you in surveys or usability studies).
- **Voice or Video Recordings:** Recordings of general meetings, usability or research sessions that you participate in, collected with your consent.
- **P&C and Applicant Information:** Information you provide during hiring or employment processes, including resumes, interview notes, references, and security clearance documentation.
- **Feedback:** Insights or information you share during interviews, workshops, or general discussions to help improve project outcomes.

The types of information described above are not exhaustive and may change over time as our programs, services, or technology evolve. Data is collected and used for purposes consistent with applicable privacy laws. We make reasonable efforts to inform you about the category of personal data we collect.

Retention Periods by Category

We retain data only for as long as necessary to fulfill the purpose for which it was collected or to meet legal, regulatory, or operational requirements. The following table provides a general breakdown of data categories, examples, and corresponding retention periods.

Data Category	Examples	Retention Period	Legal/Operational Justification
IUR/GRIT Participant Data	Name, email, accessibility needs, income, location in Canada, gender, age, and other personal information.	Until participant asks to leave or C4C removes them from	As active members of the community, C4C communicates testing opportunities and updates about community activities.

		the community	Data is retained until removal is requested or initiated. Members who are disrespectful or no longer engage with C4C may have their information removed.
User Contact Information	Names, emails from newsletter signups or contact forms	5 years after last interaction	Operational needs and outreach practices
IUR/ GRIT Usability Research Data	Audio/video recordings, transcripts, survey responses	2 years from the month of project completion.	UX research best practice
Demographic Data from User Research	Race, gender, employment, etc. from survey participation	2 years from the month of project completion or until anonymized	UX research best practice
Technical and Usage Data	IP address, browser, session cookies.	1 year from the year end of project completion	Analytics and performance monitoring
Project Research Data	Audio/video recordings, transcripts, survey responses, interview notes	2 years after the project completion unless mentioned in the Funder Requirement.	Best practice

Secure Storage & Access Control

All personal and sensitive data you provide is stored using reasonable safeguards, including in encrypted, self-hosted systems (e.g., Google Workspace) or through vetted third-party providers, including but not limited to tl;dv, Microsoft Suite, Notion, JotForm, Airtable, Miro Spanning, Rippling, HubSpot, and ActiveCampaign.

Access to your data is restricted to authorized staff and managed through role-based permissions. Access is segmented by department and function, and employee access rights are reviewed regularly to maintain least-privilege access in alignment with organizational security policies.

Sensitive data is encrypted both at rest and in transit. All vendor data centers used by us are expected to meet recognized security standards such as SOC 2 and ISO 27001.

Data Backup

Backups of Google Workspace data are managed through Spanning, which provides encryption, SOC 2 Type II and HIPAA compliance, and secure data handling. We use reasonable efforts to ensure that backup systems protect data integrity, confidentiality, and against unauthorized access or loss.

Third-Party Services

We use third-party service providers to support our programs, research, and digital tools. These providers are evaluated for compliance with Canadian or equivalent data protection laws, with preference given to providers that offer Canadian data hosting. Code for Canada only uses digital products that meet SOC 2 Type II compliance and are ISO 27001 or GDPR compliant.

Destruction Protocols

We use reasonable efforts to securely destroy your data once the retention period has expired or when it is no longer required for its intended purpose. Anonymized data may be retained indefinitely for aggregate reporting or research.

Destruction methods may include:

- **Digital data**: secure deletion using Google Workspace admin console. Google retains delete data for a grace period (20–30 days) before permanent deletion.
- **Physical records**: shredding using cross-cut shredders.
- **Audio/video files**: deletion from both local and cloud storage.
- **Data Anonymization:** removing identifying details from research or program data.

Policy Review

This Policy is reviewed annually to maintain compliance with evolving legal, security, and operational standards.

We may update this Policy from time to time. When updates are made, the revised Policy will be posted publicly on our website. The new version will be effective when we post it. If you continue to use our services after we post any changes to this Policy, you agree to the changes made to this Policy. We will not provide individual notice of changes and encourage you to review this Policy periodically.

Contact Us

If you have any questions about this Policy or how we handle your data, you may contact us at: operations@codefor.ca