Canada Revenue Agency | Agence du revenu du Canada

PRIVACY MANAGEMENT FRAMEWORK

January 2020

Canada

TABLE OF CONTENTS

INTRODUCTION

Your privacy is our priority

The Canada Revenue Agency (CRA) is one of the largest holders of personal information in the Government of Canada. Making sure this personal information is properly managed and protected is one of our top priorities.

We are committed to upholding the trust that Canadians place in our organization. To meet their expectations, we take the necessary measures to protect personal information, enable the appropriate management of data and drive employee responsibility for privacy.[1] Privacy refers to the effective protection and management of personal information. We do this by identifying, assessing, monitoring, and mitigating privacy risks in programs and activities that involve collecting, retaining, using, disclosing, and disposing of personal information.

The CRA has the authority to obtain information from taxpayers to administer and enforce its program legislation, the *Income Tax Act* and *Excise Tax Act*. At the CRA, the appropriate management and protection of Canadians' information is governed through legislation and policies, such as the *Privacy Act* and associated Treasury Board of Canada Secretariat policies and directives, as well as corporate policies like the CRA Privacy Policy. We collect, use and disclose personal information according to these laws and regulations.

Although the overall accountability for our privacy program rests with the CRA's Chief Privacy Officer (CPO), several senior management officials are responsible for the various mechanisms that support privacy.[2] These mechanisms are listed in the "Our privacy commitment" section of this document.

This Privacy Management Framework articulates our vision, our objective and our commitment to privacy, including how we handle and protect personal information to make sure we respect our clients' privacy. The Framework is meant to be a reference document for taxpayers and CRA employees.

We define these key terms as follows:

Privacy management

The combined activities of an organization to:

- collect, use, disclose, and dispose of personal information in a way that follows the law and policy guidance
- safeguard personal information
- manage the risks associated with the handling of that information

Personal information

Personal information is information about an identifiable individual that is recorded in any form.[3]

1 See Annex D for CRA employees' privacy-related accountabilities.
2 See Annex C for a list of all CRA chiefs' and senior management's privacy-related accountabilities.
3 The definition is described more in the Privacy Act.

DRIVING FACTORS FOR OUR APPROACH TO PRIVACY

The privacy landscape is rapidly evolving; the public increasingly expects their personal information to be properly managed and protected.[4]

Although this expectation is driving forward stronger privacy legislation (for example, the European Union's General Data Protection Regulation and the Department of Justice Canada's review of the *Privacy Act*)[5], it is also highlighting the need for strong accountability for privacy and for the handling and protection of personal information. To maintain the trust of individuals, organizations must have sufficient and appropriate practices in place to handle personal information.

We have adopted an accountability framework consisting of various technical and organizational mechanisms to appropriately handle and safeguard personal information. These mechanisms include:

- clear roles and responsibilities that encompass all aspects of our privacy mandate
- governance structures that provide effective oversight, reporting, and decision-making
- transparent internal and external privacy policies, resources, and training

Privacy breaches are on the rise and are top of mind for all organizations.

We recognize that to prevent privacy breaches, privacy must be woven into all organizational activities. To make this possible, all branches and regions must be involved since they share the responsibility to appropriately handle the personal information they collect, retain, use, disclose, and dispose of.

Therefore, we embed Privacy by Design principles into the development and operation of IT systems, networked infrastructure, and business practices so we can mitigate risks, find solutions early on, and support operational excellence.

The CRA is also introducing new privacy professionals and experts to its workforce — who understand how to get value from an ever-increasing quantity of data while maintaining privacy.

Privacy is no longer viewed as a roadblock to innovation and service, but rather as a strategic enabler that drives service delivery by prioritizing the protection of personal information.

We have established a comprehensive and effective privacy governance structure to help foster privacy. This structure has measurable outcomes to show that respecting privacy is a top priority. Privacy permeates our business discussions and decisions because we view it as a proactive measure that creates value in our organization by driving innovation and creative solutions.

Our privacy program has evolved to become a strategic capability rather than solely operational because of the increased demand for privacy advisory support and expertise from the public and across the CRA.

4 This is also demonstrated in the Office of the Privacy Commissioner of Canada 2018-2019 survey of Canadians on Privacy.

5 Additional privacy legislative changes include Innovation, Science and Economic Development Canada's review of the *Personal Information Protection and Electronic Documents Act* and the development of the Digital Charter.

PRIVACY GUIDING PRINCIPLES

To foster client trust and confidence in the CRA, we believe in establishing a language about privacy that will help ensure we are working toward the same goals.

The following are our privacy guiding principles:

1. We value and respect the client data in our possession and help our clients clearly understand how and why we are using it.
2. We support our employees in understanding their data handling responsibilities, and we respond to our clients' requests promptly and helpfully to drive a seamless and efficient experience.
3. We put our clients at the heart of all changes and improvements to our service delivery by adopting innovative practices and including Privacy by Design principles into all that we do.
4. We collaborate with our employees and integrate effective and secure client data management across the CRA to foster a holistic approach to building and maintaining client trust.
5. We decide how we handle client data in line with legislative obligations and leading privacy practices and based on ethical standards.

OUR PRIVACY COMMITMENT

Our privacy commitment to you is to appropriately manage and proactively protect your personal information by collaborating across the CRA and adopting the Privacy by Design principles.[6] We believe that privacy management is a responsibility that everyone at the CRA shares. This means our privacy commitment spans all agency branches and regions and is upheld by each of our 46,000+ employees.

To meet our commitment to privacy, we focus on the following measures. Together, these measures provide a set of mechanisms to protect your personal information. Various CRA leaders are responsible for these mechanisms, with the Chief Privacy Officer (CPO) having a line of sight into each capability to execute the CPO's mandate and support the CRA in meeting its privacy commitment.[7]

1. Program design and delivery

We embed our privacy guiding principles and the Privacy by Design principles[8] into the development, operation, and management of all programs, processes, solutions, and technologies involving personal information. Taking into account the need for effective and timely service delivery and privacy considerations to enable the protection of our most sensitive assets.

6 See Annex A for the Privacy by Design principles.
7 See Annex B for the Chief Privacy Officer's mandate and Annex C for a list of all the chiefs' and senior management's privacy-related accountabilities.
8 See Annex A for The Privacy by Design principles.

Key related privacy capabilities include:

- **User-centricity:** We aim to create a positive service experience for Canadians that is user-centric, secure, and transparent from beginning to end. We design our services to be easy-to-use and integrated whenever possible. This will give you a consistent and seamless experience in all your interactions with the CRA, with privacy being a fundamental component.
- **Governance and stewardship[9]:** We have strong governance and stewardship mechanisms to provide oversight and accountability for privacy and to guide whether we are effectively using those privacy requirements in our organization.
- **Privacy notices and privacy communications:** We are responsive and transparent in our communications with you to ensure you know your privacy rights and how we use and manage your personal information (for example, the privacy notices on our forms when collecting personal information). We are also proactive in warning the public about fraudulent communications claiming to be from the CRA.
- **Authentication:** To protect your personal information, we verify the identity of our clients by using:
  - portals or systems
  - over-the-phone or in-person consultations where we request the client's credentials
  - sign-on or two-factor authentication that clients must complete

  We also manage employee credentials to make sure only authorized employees have access to personal information and only for authorized purposes.
- **Identity management:** To protect your personal information, we collect the necessary information to accurately establish our clients' identity when they use our services.

2. Information sharing

The CRA occasionally has to share information, for example, with taxpayers, employees, or other third parties. When sharing information, we include privacy protective measures into those relationships. This facilitates the appropriate handling and protection of personal information.

Key related privacy capabilities include:

- **Intra-agency data sharing:** We work collaboratively to meet our obligations and to deliver a seamless experience to you by sharing client data with relevant branches when appropriate and permitted.
- **Provincial, territorial, and federal information sharing:** As part of the CRA's mandate to administer tax and benefit administration for our provincial and territorial partners, we share clients' personal information with provincial, territorial, and federal governments as needed (and as set out in legislation), while respecting privacy and security, to enable the efficient delivery of government services.
- **Treaties with international jurisdictions:** We take the necessary precautions when sharing information with international jurisdictions by following the Organisation for Economic Co-operation and Development's (OECD) guidelines and including privacy-related clauses into our treaties.
- **Third-party service providers and partners:** We include privacy and security controls and requirements in all interactions with third-party service providers when we procure their services or by conducting reviews and audits of these providers.

9 See page 6 for more details on privacy governance.

- **Management of privacy complaints and inquiries:** We seek to respond to and resolve clients' complaints and inquiries about their personal information and privacy rights transparently and promptly.
- **Open source data:** To deliver on our mandate, we use publicly available, open source data in keeping with government of Canada laws and policies.
- **De-identification of data:** We take measures to de-identify personal information before sharing statistical information to maintain individual privacy.
- **Information sharing with authorized third parties:** We seek to include the appropriate level of privacy and security safeguards in all information-sharing with authorized third parties such as tax preparers, financial institutions, and authorized representatives.

3. Internal and external controls

The CRA takes the necessary precautions and steps to protect personal information from external and insider threats.

Key related privacy capabilities include:

- **External controls:** We protect your personal information from external threats, such as cyber-attacks and phishing, by using firewalls, encryption, virus detection, and intrusion prevention tools. We also conduct threat intelligence to monitor for and detect breaches, and we validate multiple data points by using multi-factor authentication.
- **Internal controls:** We protect personal information from internal threats by using advanced automated solutions for detecting, identifying, and verifying questionable user transactions on our systems. We also apply information security principles such as minimum system access (employees have only the access they need to do their jobs), need-to-know (information is accessed only by those who need it to do their job) and segregation of duties (separating key job functions to reduce the risk of fraud, error, and misuse).

4. Employee outreach

We support our employees in their understanding of privacy responsibilities and compliance obligations to enhance privacy at the CRA.

Key related privacy capabilities include:

- **Employee Code of Integrity and Professional Conduct**[10]**:** In this code, we explicitly outline the expected standard of conduct including the requirement to protect personal information. CRA employees are asked to review and affirm their obligations under the CRA's Code of Integrity every year.
- **Privacy training, awareness, and testing:** We provide privacy training and outreach for our employees to promote privacy awareness and make sure they understand their privacy obligations.

5. Privacy risk management and compliance

We are committed to managing existing and emerging data risks and to monitoring and responding to privacy compliance issues.

10 See Annex D for CRA employee privacy-related accountabilities.

Key related privacy capabilities include:

- **Data, information, and records management:** We take steps to effectively manage the personal information we possess to maintain its accuracy, make sure we use it only to fulfil our mandate and keep it only for as long as needed.
- **Privacy impact assessments and personal information banks:** We proactively assess the development of all new technologies, services, and initiatives that use personal information to determine the privacy safeguards required. As well, we keep a record of our uses of personal information.
- **Privacy audits, compliance reviews, tools and measurements:** We validate that personal information is handled in compliance with our privacy legislative obligations and policy requirements by conducting audits, self-assessments and ongoing monitoring.
- **Consent:** We follow our legislative obligations and privacy program procedures when collecting, using or disclosing personal information. When required, we will seek your consent at point of collection of your personal information.
- **Privacy policy instruments, processes, protocols, and guidance:** We develop comprehensive privacy policies and related guidance documents that clearly define privacy requirements to make sure personal information is managed securely and respectfully.
- **Analytics:** We embed the necessary data protection and privacy controls in the use of analytics for business intelligence purposes.
- **Ethics for artificial intelligence:** We use artificial intelligence (AI) in an ethical way and have developed a specialized AI executive forum to identify and discuss AI issues and opportunities.

6. Management of privacy breaches

We assess privacy breaches in keeping with Treasury Board of Canada Secretariat policies and procedures to document and evaluate potential risks to the affected individual and mitigate risks.

Key related privacy capabilities include:

- **Response management of privacy breaches:** We designed a comprehensive response plan that we test regularly. If a breach occurs, we act to resolve all outstanding issues and offer support to affected individuals through a dedicated CRA representative. This way, clients have the chance to ask questions and learn more about the implications of the breach. As required, we also inform the Office of the Privacy Commissioner of Canada as well as the Treasury Board of Canada Secretariat.

GOVERNANCE

At the CRA, we believe that privacy cannot be viewed in isolation. Rather, privacy is a topic that intersects activities across all of our branches and within all regions. A strong privacy governance structure fosters cross-branch collaboration and employee awareness for their privacy obligations.

We developed a privacy governance structure that includes:

- **A strategic enterprise-wide privacy committee** that facilitates strategic, horizontal consultation, collaboration, and decision-making on all new or changed initiatives using personal information and provides the strategic direction to establish priorities and manage risk on all matters relating to privacy.

- **Operational committees** that provide updates and facilitate collaboration and information sharing on operational privacy issues and requirements.
- **Initiative-based working groups** that assess the initiative/topic of interest, recommend a go-forward approach for the Agency for consideration by senior management, and work with the appropriate stakeholders to implement the recommendation(s), as required.

This structure lets us include privacy in all our initiatives and services. As well, it opens dialogue amongst all branches and regions, and strengthens oversight on the privacy of all our programs.

We enforce and measure this governance structure through forums, and metrics to report and govern cross-branch engagement, and accountability for privacy.

CONCLUSION

The CRA is committed to protecting the personal information entrusted to us by Canadians and employees. We do this using a thorough approach of privacy management that is based on collaboration across the Agency and the principles of Privacy by Design.

RESOURCES

CRA's Annual Reports to Parliament on the Administration of the *Access to Information Act* and the *Privacy Act*

Personal information banks

Privacy impact assessment summaries

Privacy notice

Employee Code of Integrity and Professional Conduct

Request information from the Canada Revenue Agency

Contact the Access to Information and Privacy Directorate

Follow us:

- Facebook
- Twitter
- YouTube
- LinkedIn

ANNEX A: PRIVACY BY DESIGN PRINCIPLES

1. **Be proactive, not reactive**

Anticipate, identify, and prevent invasive events before they happen. This means taking action before the fact, not after.

2. **Lead with privacy as the default setting**

Ensure personal data is automatically protected in all IT systems or business practices, with no added action required by any individual.

3. **Embed privacy into design**

Privacy measures should not be add-ons but fully integrated components of the system.

4. **Retain full functionality (positive-sum, not zero-sum)**

Privacy by Design employs a "win-win" approach to all legitimate system design goals, which means that both privacy and security are important and no unnecessary trade-offs need to be made to achieve both.

5. **End-to-end security – full lifecycle protection**

Data lifecycle security means all data should be securely retained as needed and destroyed when no longer needed.

6. **Maintain visibility and transparency – keep it open**

Assure stakeholders that business practices and technologies are operating according to objectives and are independently verified.

7. **Respect user privacy – keep it user-centric**

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost. They can do this by offering measures such as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

ANNEX B: CHIEF PRIVACY OFFICER'S MANDATE

The Chief Privacy Officer (CPO) operates as the privacy champion at the CRA. The CPO is appointed by the Commissioner and is responsible for defining, executing on and maintaining the Privacy Commitment of the CRA. The role of the CPO is to ensure that the CRA's respect for privacy is reinforced and strengthened.

The CPO has a broad mandate for privacy oversight at the CRA. The creation of this position reinforces the CRA's commitment to integrity and excellence.

The CPO is responsible for:

- overseeing decisions related to privacy, including assessing the privacy impacts of our programs
- championing personal privacy rights according to legislation and policy, including managing internal privacy breaches
- reporting to CRA senior management on the state of privacy management at the CRA at least twice a year

The CPO oversees the privacy program within the Public Affairs Branch, which serves as the strategic advisor to enable the branches and regions to meet their objectives while maintaining privacy and drives forward the privacy mandate.

The privacy program is responsible for:

- developing tools, guidelines and resources that enable all branches to embed Privacy by Design
- reviewing and updating existing privacy policies and procedures
- developing new policies and procedures as needed to ensure they embody and reflect the CRA's privacy vision, mandate and objectives
- developing the Annual Privacy Strategy and conducting annual operational effectiveness reviews
- educating and advising the branches and regions on their roles and responsibilities to protect personal information and providing advice as needed
- responding to and managing privacy breaches, inquiries, and complaints
- processing, advising on, and evaluating initiatives, processes, technology, and new uses of data through privacy impact assessments and privacy protocol assessments
- conducting third-party risk management activities
- communicating with internal and external stakeholders about privacy at the CRA
- acting as a point of contact between the Agency and the Office of the Privacy Commissioner of Canada and other regulatory bodies, as appropriate, with respect to matters related to the protection of personal information
- developing and maintaining training materials for employees and providing general and targeted training for the branches and regions
- driving awareness, commitment, buy-in, and adoption from the branches, regions, and key stakeholders

ANNEX C: AGENCY CHIEFS' AND SENIOR MANAGEMENT'S PRIVACY-RELATED ACCOUNTABILITIES

Chief Information Officer

The Chief Information Officer (CIO) oversees IT infrastructure, networks and applications for the CRA's tax systems. In relation to privacy, the CIO ensures personal information is protected by securing the CRA's systems and through sound threat management.

Chief Data Officer

The Chief Data Officer (CDO) maximizes the CRA's ability to use data for the benefit of Canadians as well as the CRA. This includes ensuring personal information is appropriately managed in all datasets. The CDO ensures the sound handling of data that could identify an individual, and ensures the Agency Data Strategy lines up with our agency's privacy principles and policies.

Chief Service Officer

The Chief Service Officer (CSO) enables service excellence at the CRA. The CSO embeds privacy into the design of all the CRA's services to ensure the client is at the heart of the solution. This includes the appropriate protection of client personal information.

Agency Security Officer

The Agency Security Officer (ASO) provides department-wide strategic leadership, coordination, and oversight for all security management activities and security controls, including those related to the protection of information. As part of these responsibilities, the ASO oversees establishing department-wide policies, processes, and practices to ensure an integrated approach to security management in collaboration with partners and other stakeholders.

Chief Financial Officer

The Chief Financial Officer oversees the financial management and financial administration for the CRA, including funds to support the privacy function.

Information Management Senior Officer

The Information Management Senior Officer coordinates and implements information management policy, sound record management and external information-sharing arrangements involving personal information.

Legal counsel

Legal counsel offers legal advice on interpreting and applying legislation and supporting requirements the Agency must follow. They also give advice on developing privacy policy and appropriately interpreting privacy legislative requirements.

Chief Human Resources Officer

The Chief Human Resources Officer oversees all of the CRA's human resources needs. This includes ensuring the proper controls for protecting employee personal information are in place as well as maintaining records of employee privacy training.

Chief Audit Executive

The Chief Audit Executive performs audits to assess the effectiveness and efficiency of policies, practices and controls, in order to advise the branches, Commissioner and Chief Executive Officer and Board. This includes the auditing of privacy related activities to strengthen controls and the protection of personal information.

Assistant Commissioner of the Public Affairs Branch

The Assistant Commissioner of the Public Affairs Branch develops, maintains and publishes privacy communications and awareness materials for the CRA and the Public, in order to ensure we clearly communicate our privacy practices and to increase transparency in how we handle personal information.

Assistant Commissioner of the Assessment, Benefit, and Service Branch

The Assistant Commissioner of the Assessment, Benefit and Service Branch administers key services for the CRA to ensure interfaces and applications allow clients to access their data.

All program areas and regional assistant commissioners

Assistant commissioners from all program areas and regions are accountable for managing personal information within their branch and region and for ensuring they apply appropriate privacy safeguards. This includes the secure and appropriate sharing of personal information internally throughout the CRA and externally with authorized third parties.

ANNEX D: CRA EMPLOYEES' PRIVACY-RELATED ACCOUNTABILITIES

All employees within the branches and regions

Employees from all branches and regions play a vital role in helping the CRA meet its commitment to safeguarding our clients' personal information. Employees must understand their obligations to properly handle and safeguard personal information. Employees are responsible for ensuring they handle, manage, and protect the personal information they collect, use, or disclose while doing their duties in accordance with the CRA's privacy policies, procedures, processes, and protocols.