Canadian Privacy Certification

Outline of the Body of Knowledge for the Certified Information Privacy Professional/Canada (CIPP/C™)

I. Introduction to Privacy in Canada
   A. Canadian Governmental Structure
      a. Understand the basics of the Canadian government and legal system
         i. Know the political structure
         ii. Know the division of powers
         iii. Know the role of courts and administrative tribunals
      b. Understand Canadian laws and their interpretations
         i. Know the difference between civil and common law
         ii. Know the sources of law
         iii. Know the scope and application of law
         iv. Understand the relationships to other bodies of law
      c. Know the purposes and roles of Privacy Commissioners, courts, and remedies
         i. Understand the scope of the Federal, Provincial and Territorial Privacy Commissioners
         ii. Understand the scope of the Federal and Provincial courts
   B. Privacy Basics
      a. Understand that definitions of personal information vary among Canadian jurisdictions and legislation
         i. Know where to find definitions of personal information across jurisdictions and legislation
         ii. Know the different types of personal information (e.g., employee and work-related information, public records, publicly available information)
      b. Understand what constitutes private or sensitive information
      c. Understand how to safeguard personal information
         i. Know that standards or frameworks (e.g., ISO standards, NIST) exist and could be used
ii. Know that there are appropriate methods to follow regarding data (e.g.,
pseudonymization vs anonymization)

iii. Know the categories of controls that should be applied regarding third parties
(e.g., contractual, managerial/administrative, technical)

iv. Understand the basics of cybersecurity issues in privacy field (e.g., data breach
notification laws, state-sponsored attacks)

v. Understand the basics of privacy impacts of technological world (e.g., BYOD, Do
Not Track, AI, biometrics, e-services, surveillance)

d. Understand data events, data incidents and data breaches
   i. Know the high-level processes for dealing with each (e.g., breach notice,
      reporting and investigations)
   ii. Understand the importance of effective record keeping
   iii. Notify privacy commissioner according to applicable legislation

C. Development of Privacy Principles
   a. Understand the general concepts and development of fair information practices
      i. Know when to use applicable practices (e.g., notice, types of content, access
         controls and accountability)
   b. Organisation for Economic Co-operation and Development (OECD) Guidelines on the
      Protection of Privacy
   c. Canadian Standards Association (CSA) Model Code for the Protection of Personal
      Information
   d. Generally Accepted Privacy Principles (GAPP)

D. International Privacy
   a. Understand that international and regional laws impact Canadian organizations
      i. Know where to research relevant laws
      ii. Know when international and regional laws are relevant to particular situations
           (e.g., data transfers across borders, healthcare, education, finance)

II. Canadian Privacy Laws and Practices—Private Sector

A. Know the Privacy Principles that are the foundation of the Personal Information Protection
   and Electronic Documents Act (PIPEDA) and provincial private sector laws
   a. Establish accountability for the personal information, including when using third
      parties
   b. Identify purpose for collecting personal information
   c. Acquire meaningful and valid consent (e.g., reasonableness, opt-out mechanisms,
      consent to new purposes, installation of computer programs, automatic downloads)
   d. Adhere to rules respecting collection, use, disclosure, retention, and deletion of
      personal information
      i. Include fact-finding of qualification as a “commercial activity”
e. Keep information accurate and up to date as necessary for original purpose of collection
f. Safeguard collected personal information
   i. Ensure virtual and physical storage is secure
g. Ensure openness of policies and practices of collecting personal information
   i. Deliver this information at customer point of contact in electronic or print format (e.g., title and address of accountable person, means of gaining access, description of types of information being held)
h. Understand how to respond to individuals seeking access to personal information
   i. Understand what information can be provided or withheld and the timelines for response
   ii. Address inaccuracies immediately
i. Ensure proper policies and procedures are in place to deal with compliance complaints and investigations
   i. Know compliance reporting and record-keeping requirements
   ii. Know the impact of relevant Canadian court rulings (e.g., TELUS, Blood Tribe, ABIKA, Globe 24h)
   iii. Know where to access commissioner rulings (e.g., agreements, guidance, and published positions, appealed decisions, expectations)
   iv. Know the impact of significant commissioner rulings (e.g., SWIFT, TJX, Facebook, Google, Equifax)

B. Know when private-sector privacy legislation is applicable instead of PIPEDA (e.g., Alberta, British Columbia, Quebec)

C. Understand Canada’s Anti-Spam Legislation (CASL)
   a. Follow rules for consent, identification and unsubscribe mechanisms

III. Canadian Privacy Laws and Practices—Public Sector

A. Know the Privacy Principles that are the foundation of the Privacy Act
   a. Understand the expectations of consent governing personal information
      i. Know the circumstances in which the collection, use, or disclosure of personal information is permitted without consent.
   b. Understand the individual’s right of access and correction to their personal information
      i. Comply with requests within the applicable timeframes and in a helpful manner
      ii. Address corrections to personal information
      iii. Know the exceptions where requests to access or to correct personal information may be denied
   c. Follow required storage, retention, and destruction of personal information

B. Privacy Impact Assessments
   a. Understand the processes for how and when to complete
C. Understand the applicability of the Freedom of Information and Protection of Privacy Acts of the different provinces and territories

IV. Canadian Privacy Laws and Practices—Health Sector

A. Understand when to apply the various health privacy acts of the provinces and territories
   a. Know which provincial health laws have been deemed “substantially similar”
      i. Comply with applicable laws
   b. Know what defines Personal Health Information (PHI)
   c. Ensure the purpose of the collection, use and disclosure of PHI is necessary
   d. Ensure access to and right to correct information
   e. Ensure oversight and accountability
      i. Ensure proper use, retention, safeguarding and disposal of PHI, including third parties
   f. Ensure meaningful consent to the collection, use, and disclosure of PHI
      i. Understand when implicit/implied consent is considered appropriate
      ii. Understand what constitutes the circle of care for an individual and who may act as a custodian or trustee for that individual
   g. Ensure safeguarding and breach protocols
      i. Adopt reasonable administrative, technical, and physical safeguards that ensure security of the information
      ii. Understand how to respond to and contain a breach
      iii. Notify the appropriate privacy commissioner when a breach has occurred according to PIPEDA or provincial law as applicable
   h. Openness
      i. Develop comprehensive privacy policies and make them accessible according to PIPEDA or provincial law as applicable