Canadian Privacy Certification

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

I. Canadian Privacy Fundamentals

A. Legal Basics

a. The Canadian government and legal system
   i. Political structure
   ii. Division of powers
   iii. Role of courts and administrative tribunals
b. Canadian laws and their interpretation
   i. Civil versus common law
   ii. Sources of law
   iii. Scope and application of law
   iv. Relationship to other laws
c. Enforcement, agencies and powers
   i. Privacy commissioners
      a. Office of the Federal Privacy Commissioner
      b. Provincial and territorial privacy commissioners
   ii. Courts and remedies
      a. Federal Court of Canada
      b. Provincial courts

B. Privacy Basics

a. Understand applicable international and regional laws (e.g., GDPR, CCPA, New York Shield Act)
b. Understand that definitions of personal information vary among Canadian jurisdictions and legislation.
c. Types of personal information
   i. Employee and work-related information
   ii. Public records
iii. Publicly available information
   2. Provincial legislation

d. Private/sensitive information

e. Safeguarding personal information (e.g. ISO standards, NIST)

f. General concepts of fair information practices (e.g., notice, types of content, access controls and accountability)

C. Privacy Principles

   i. What the CSA principles are in Canadian privacy law
   ii. How the CSA principles were developed
      a. Organisation for Economic Co-operation and Development (OECD)
      b. American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA)
      c. Generally Accepted Privacy Principles (GAPP)

II. Canadian Privacy Laws and Practices—Private Sector

A. Statutes

a. Understand when to apply The Personal Information Protection and Electronic Documents Act of Canada (PIPEDA)

b. Understand when to apply the private sector privacy legislation in BC, Alberta and Quebec.

c. Understand when to apply Canada’s Anti-Spam Legislation (CASL)

B. Key Concepts and Practices

a. Accountability
   i. Under the Quebec Act
   ii. Other Canadian statutes

b. Openness

c. Collection, use and disclosure
   i. Commercial activity as it relates to PIPEDA
   ii. Business transactions

d. Enhanced and valid consent
   i. Reasonableness
   ii. Opt-out consent mechanisms, their use and limitations
   iii. Consent to new purposes
   iv. Installation of computer programs
   v. Automatic downloads
   vi. Documentation

e. Notice requirements
f. Data breach reporting and investigations
   i. Record keeping
   ii. PIPEDA
   iii. Understand when to apply privacy legislation regarding data breach reporting
        (e.g., Ontario’s Personal Health Information Protection Act (PHIPA), Alberta’s
        Personal Information Protection Act (PIPA), New Brunswick’s Personal Health
        Information Privacy and Access Act (PHIPAA))

| g. Managing privacy protection requirements of third parties (e.g. service providers, cloud solution providers)

h. Access
   i. Rights and obligations
   ii. Compliance trends
      i. Commissioner rulings (e.g., agreements, guidance and published positions,
         appealed decisions, expectations)
      ii. Relevant Canadian court rulings
   j. Compliance issues

III. Canadian Privacy Laws and Practices—Public Sector

A. Statutes
   a. Understand when to apply the Privacy Act of Canada
   b. Understand when to apply the Freedom of Information and Protection of Privacy Acts
      of the different provinces and territories

B. Key Concepts
   a. Consent
      i. Authority to collect
      ii. Consistent use
   b. Disclosure and transfer
   c. Retention, storage and destruction
   d. Openness and access
   e. Privacy implications of service delivery models
      i. E-government initiatives
   f. Sub-contracting and Shared Services
   g. Research and Statistical use of Personal Information
IV. Canadian Privacy Laws and Practices—Health Sector

A. Statutes
   a. Understand when to apply the various Health Information Acts of the provinces and territories

B. Application and scope
   a. Personal health information
      i. Definitions
      ii. Interaction with PIPEDA
      iii. Substantially similar to PIPEDA
   b. The health information custodians and trustees
      i. Custodians working for non-custodians
      ii. When non-custodians receive personal health information from custodians
      iii. Agents

C. Key concepts and issues
   i. Consent and exceptions to consent
   ii. Authorized purposes
      iii. Circumstances requiring disclosures to non-custodians
   iv. Safeguarding data and determining the need for breach notification to the Commissioner and/or affected parties
      1. Agents
      2. Notice of loss
   v. Integrity
   vi. Accountability and openness
   vii. Data access and the right to correct information
   viii. Oversight
   ix. Surveillance