Role of the Chief Privacy Officer (and of Senior Management)

Statute	Requirements for CPO and related statutory obligations
PIPEDA	**Principle 4.1** **4.1 Principle 1 — Accountability** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles. **4.1.1** Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s). **4.1.2** The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.
PIPA Alberta	**s. 5(3)** An organization must designate one or more individuals to be responsible for ensuring that the organization complies with this Act.
PIPA British Columbia	**s. 4(3)** An organization must designate one or more individuals to be responsible for ensuring that the organization complies with this Act.
Quebec Private Sector Privacy Act	**s. 3.1** Any person carrying on an enterprise is responsible for protecting the personal information held by the person. Within the enterprise, the person exercising the highest authority shall see to ensuring that this Act is implemented and complied with. That person shall exercise the function of person in charge of the protection of personal information; he may delegate all or part of that function in writing to any person.

	The title and contact information of the person in charge of the protection of personal information must be published on the enterprise's website or, if the enterprise does not have a website, be made available by any other appropriate means. **s. 3.2** Any person carrying on an enterprise must establish and implement governance policies and practices regarding personal information that ensure the protection of such information. Such policies and practices must, in particular, provide a framework for the keeping and destruction of the information, define the roles and responsibilities of the members of its personnel throughout the life cycle of the information and provide a process for dealing with complaints regarding the protection of the information. The policies and practices must also be proportionate to the nature and scope of the enterprise's activities and be approved by the person in charge of the protection of personal information. Detailed information about those policies and practices, in particular as concerns the content required under the first paragraph, must be published in simple and clear language on the enterprise's website or, if the enterprise does not have a website, made available by any other appropriate means. **s. 3.3** Any person carrying on an enterprise must conduct a privacy impact assessment for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, communication, keeping or destruction of personal information. For the purposes of such an assessment, the person must consult the person in charge of the protection of personal information within the enterprise from the outset of the project. The person must also ensure that the project allows computerized personal information collected from the person concerned to be communicated to him in a structured, commonly used technological format. The conduct of a privacy impact assessment under this Act must be proportionate to the sensitivity of the information concerned, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored. **s. 3.4** The person in charge of the protection of personal information may, at any stage of a project referred to in section 3.3, suggest personal information protection measures applicable to the project, such as **(1)** the appointment of a person to be responsible for implementing the personal information protection measures; **(2)** measures to protect the personal information in any document relating to the project;

	(3) a description of the project participants' responsibilities with regard to the protection of personal information; or **(4)** training activities for project participants on the protection of personal information. **s. 3.5** Any person carrying on an enterprise who has cause to believe that a confidentiality incident involving personal information the person holds has occurred must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature. If the incident presents a risk of serious injury, the person carrying on an enterprise must promptly notify the Commission d'accès à l'information established by *section 103 of the Act respecting Access to documents held by public bodies and the Protection of personal information* (chapter A-2.1). He must also notify any person whose personal information is concerned by the incident, failing which the Commission may order him to do so. He may also notify any person or body that could reduce the risk, by communicating to the person or body only the personal information necessary for that purpose without the consent of the person concerned. In the latter case, the person in charge of the protection of personal information must record the communication of the information. Despite the second paragraph, a person whose personal information is concerned by the incident need not be notified so long as doing so could hamper an investigation conducted by a person or body responsible by law for the prevention, detection or repression of crime or statutory offences. A government regulation may determine the content and terms of the notices provided for in this section. **s. 3.7** In assessing the risk of injury to a person whose personal information is concerned by a confidentiality incident, a person carrying on an enterprise must consider, in particular, the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes. The person must also consult the person in charge of the protection of personal information within the enterprise. **s. 8** … On request, the person concerned is also informed of the personal information collected from him, the categories of persons who have access to the information within the enterprise, the duration of the period of time the information will be kept, and the contact information of the person in charge of the protection of personal information… **s. 18.3 (2)** …A person or body carrying out a mandate or performing a contract of enterprise or for services referred to in the first paragraph must notify the person in charge of the protection of personal information without delay of any violation or attempted violation by any person of any obligation

	concerning the confidentiality of the information communicated, and must also allow the person in charge of the protection of personal information to conduct any verification relating to confidentiality requirements. **s. 28.1** …When granting such a request [for cessation of the dissemination of personal information or de-indexation], the person in charge of the protection of personal information shall attest, in his written reply under section 32, to the cessation of the dissemination of the personal information or to the de-indexation or the re-indexation of the hyperlink. **s. 30** …Such a request [for access or rectification] must be addressed to the person in charge of the protection of personal information. If the request is not sufficiently precise or if a person requires it, the person in charge must assist in identifying the information sought… **s. 32** The person in charge of the protection of personal information must reply in writing to the request for access or rectification promptly and not later than 30 days after the date the request is received. Failure to respond within 30 days of the receipt of a request is deemed to be a refusal to grant the request. **s. 34** The person in charge of the protection of personal information must give the reasons for any refusal to grant a request and indicate the provision of law on which the refusal is based, the remedies available to the applicant under this Act and the time limit for exercising them. If the applicant so requests, the person in charge must also help him understand the refusal. **s. 35** Where the person in charge of the protection of personal information grants a request for rectification, he must, in addition to the obligations prescribed in the second paragraph of article 40 of the Civil Code, issue free of charge to the person who made the request a copy of any personal information modified or added or, as the case may be, an attestation of the deletion of personal information.