Full Program
Law 25 Compliance

Implementation stages and deliverables	Training Hours (webinars)	Group Q&R Sessions	Documents Included	Description
Step 1: **Introduction to privacy protection, identification of stakeholders, inventories**	2	1	•Communication and work plan •List of duties of the Data Privacy Officer (DPO) •Resolutions for the appointment of the DPO and committee members •Description of roles and responsibilities of the DPO and stakeholders •Inventories of personal information and processes	We offer an introductory course on privacy protection and Law 25. We explain what personal information and sensitive information are, the obligations under Law 25, and the role of the person responsible for privacy protection, the Data Protection Officier (DPO). We provide all the necessary resolutions for the organization to appoint its DPO and to determine whether it needs additional committees. We also begin the inventory of personal information and processes.
Step 2: **Privacy incident**	2	1	•Response and notification procedure in the event of a complaint and/or confidentiality incident •Disaster recovery plan •Register of privacy complaints and incidents •Notification to supervisory authority (provincial) •Notification to supervisory authority (Federal) •Table for calculating risk of harm •Notice to inform individuals of a confidentiality incident	We discuss what a privacy incident is, how to determine whether reporting to the supervisory authorities is necessary, and how to go about reporting. We provide all the necessary documentation for handling privacy complaints and incidents.
Step 3: **Governance framework, privacy policy, consent**	2	1	•Privacy Protection Governance Framework (internal) •Privacy policy (document in English and French for website) •Privacy notice and terms of service to be added to website (English and French documents for website) •Register of privacy notices and requests •Consent and request forms of all types •Clauses to be added to an employment contract	We examine the basic policies to be adopted by the organization. We provide an internal policy (to manage customer and employee data) and the necessary external privacy policies and notices (in particular to inform people who have provided personal information of their rights). We also address the issue of data subject consent.
Step 4: **Disclosure of personal information and service providers**	2	1	•Privacy Impact Assessment (PIA) Methodology •Service Povider Compliance Questionnaire •Data Security Agreement and standard contractual clauses •Transfer Register	We provide all necessary documentation to determine whether sharing data with a third party or outside the province of Quebec is permitted by law. We review the requirements of the law and the questions that need to be asked before data is transferred. We provide model contracts and sample clauses that can be added to any existing contract to protect personal information.
Step 5: **In-house Data Management**	2	1	•Integrated Document Management Policy •Guidelines for mapping processing activities •Classification Plan and Retention Schedule •Data Retention and Destruction policy •Access Rights Control Policy •Access Rights Table and Register	We review all documents relating to access to information, records management and internal practices to ensure that the organization has appropriate measures in place to manage documents, access, file classification, sensitive and non-sensitive data, etc., in order to comply with legal requirements. Retention periods are determined at this stage.
Step 6: **Information Technology and Governance**	2	1	•IT Security Policies (employees and IT services) •Mobile Device and Teleworking Policy •Personal mobile device (PMD) policy •Anonymization, De-identification and Pseudonymization Policy •Policy on the Use of Encryption •Policy on the Use of Video Surveillance •Internal audit procedure outline •Authorization Register - websites, programs, PMD •Employee guide - choosing a password •Guide for the IT department •Guide for Human Resources •Guide for other departments and DPO	We provide information security and information technology documentation. We take into account how employees access and use data within the organization, and develop clear policies on how to handle this data.
Step 7: **Employee Training**	0	0	12 training video clips of approx. 5 minutes each, totaling one hour, with quizzes for employees	Training videos for employees to help them familiarize themselves with their duties regarding confidentiality. Ex: clean desk policy, reporting an incident, not sharing passwords, etc. Quizzes in each module help employees test their knowledge and provide the company with confirmation that the employee has followed the training video and passed. The purpose of the training video is to enable the organization to demonstrate that it has been diligent in training its employees. These videos should be used for all existing employees and for the integration of new employees.
Total	12	6		