Modèle de pratiques de protection des renseignements personnels

Dans le contexte du développement
des systèmes d'information
par les organismes publics

PRP

Québec

Modèle de pratiques de protection des renseignements personnels

Dans le contexte du développement
des systèmes d'information
par les organismes publics

Version 1,0

LES PUBLICATIONS DU QUÉBEC
1500 D, rue Jean-Talon Nord, Sainte-Foy (Québec) G1N 2E5

VENTE ET DISTRIBUTION
Téléphone : (418) 643-5150 ou, sans frais, 1 800 463-2100
Télécopie : (418) 643-6177 ou, sans frais, 1 800 561-3479
Internet : www.publicationsduquebec.gouv.qc.ca

Catalogage avant publication
Bibliothèque nationale du Canada

Vedette principale au titre :

Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics, version 1,0

ISBN 2-551-19659-0

1. Droit à la vie privée – Québec (Province). 2. Personnel – Dossiers – Accès – Contrôle – Québec (Province). 3. Gestion de l'information – Québec (Province). 4. Services publics – Québec (Province) – Personnel. I. Roussel, Denyse, 1953- . II. Bistodeau, Denis. III. Lafrance, Marc, 1949- . IV. Marcoux, Linda.

JC596.2.C3M62 2004 323.44'8'09714 C2004-940389-3

Modèle de pratiques de protection des renseignements personnels

Dans le contexte du développement
des systèmes d'information
par les organismes publics

Version 1,0

Québec

Cet ouvrage a été rédigé par

Madame Denyse Roussel
Conseillère en protection des renseignements personnels
Direction du soutien en accès à l'information
et en protection des renseignements personnels
Ministère des Relations avec les citoyens et de l'Immigration

Avec la participation de

Monsieur Denis Bistodeau
Institut Kono

Sous la direction de

Monsieur Marc Lafrance
Directeur du soutien en accès à l'information
et en protection des renseignements personnels
Ministère des Relations avec les citoyens et de l'Immigration

Avec le soutien de

Madame Linda Marcoux
Conseillère en communication
Direction des affaires publiques et des communications
Ministères des Relations avec les citoyens et de l'Immigration

Édition produite par

Les Publications du Québec
1500D, rue Jean-Talon Nord
Sainte-Foy (Québec) G1N 2E5

Graphisme

Groupe Dorcas

Dépôt légal – 2004
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
ISBN 2-551-19659-0

Avis au lecteur

Le *Modèle de pratiques de protection des renseignements personnels (PRP),* ci-après désigné « Modèle », est produit par la Direction du soutien en accès à l'information et en protection des renseignements personnels du ministère des Relations avec les citoyens et de l'Immigration (MRCI).

Ce document est produit à titre de document de référence. Il ne constitue pas une opinion juridique. La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* a préséance dans tous les cas ainsi que les autres dispositions légales de PRP. Le MRCI et Les Publications du Québec n'assument aucune responsabilité quant à l'utilisation qui pourrait être faite de son contenu ou aux résultats obtenus à la suite de son utilisation. Les adresses électroniques et les hyperliens qui sont fournis à titre de référence étaient exacts lors de la publication de ce document.

Le lecteur est invité à consulter la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* sur le site Web des Publications du Québec :
http://www.publicationsduquebec. gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html

Vous pouvez consulter le Modèle ainsi que les mises à jour sur le site Web suivant :
http://www.aiprp.gouv.qc.ca

Vous pouvez obtenir un exemplaire du Modèle en vous adressant aux Publications du Québec :
http://www.publicationsduquebec.gouv.qc.ca/home.php

Dans le présent document, la forme masculine désigne tout aussi bien les femmes que les hommes.

Table des matières

Annexes

Liste des figures

Liste des tableaux

Liste des aide-mémoire

Les auteurs et les collaborateurs

Le *Modèle de pratiques de protection des renseignements personnels* (PRP) a été produit par la Direction du soutien en accès à l'information et en protection des renseignements personnels du ministère des Relations avec les citoyens et de l'Immigration (MRCI), sous la direction de monsieur Marc Lafrance.

Madame Denyse Roussel, conseillère en protection des renseignements personnels, a agi comme chef du projet et rédactrice du document. Elle a réussi à synthétiser ses connaissances et son expérience en PRP pour les mettre à la portée des parties prenantes aux projets de développement des systèmes d'information.

Elle a rédigé ce document avec la participation de monsieur Denis Bistodeau, de l'Institut Kono (www.institutkono.ca). Il a collaboré à toutes les phases du projet et à la rédaction de ce document à titre de conseiller en gestion du projet, en structuration des pratiques de PRP ainsi qu'en utilisation et adaptation du document, dans un contexte de projet de développement et de modification des systèmes d'information.

Ce document a été présenté à une quarantaine de personnes représentant des ministères et des organismes du gouvernement du Québec, travaillant principalement dans le domaine de la protection des renseignements personnels, des technologies de l'information, de la vérification, de la sécurité et de la gestion documentaire.

Leurs nombreux commentaires constructifs ont contribué à améliorer la qualité et l'utilité de ce document. Le MRCI tient à souligner leur contribution importante et les en remercie.

INVITATION À TRANSMETTRE DES COMMENTAIRES

Le *Modèle de pratiques de PRP* est un document appelé à évoluer au fur et à mesure qu'il sera utilisé par les organismes publics. Son évolution se fera, le cas échéant, en fonction des différents défis soulevés par la réalisation du processus de PRP dans les projets de développement des systèmes d'information, des modifications législatives apportées à la Loi sur l'accès, des directives et orientations gouvernementales en matière de PRP et autres.

Le MRCI est très intéressé à recevoir vos commentaires afin d'améliorer ce document ou pour répondre à vos questions. Vous pouvez communiquer vos commentaires ou vos questions à :

Madame Denyse Roussel, conseillère
Ministère des Relations avec les citoyens et de l'Immigration
Direction du soutien en accès à l'information
et en protection des renseignements personnels
1056, rue Louis-Alexandre-Taschereau, 4e étage
Édifice Marie-Guyart
Québec (Québec) G1R 5Z7

Téléphone : (418) 528-1758
Télécopieur : (418) 644-1017
denyse.roussel@mrci.gouv.qc.ca

Guide de lecture de l'ensemble du Modèle

Ce guide de lecture permet au lecteur d'obtenir une compréhension générale du Modèle afin d'être en mesure de le consulter ultérieurement et d'approfondir des éléments de protection des renseignements personnels liés aux projets de développement des systèmes d'information.

PARTIE 1 RÉALISER LA PRP – BUTS ET PRATIQUES SPÉCIFIQUES

PARTIE 2 GÉRER LA PRP – BUTS ET PRATIQUES DE GESTION

Préambule

Le recours accru aux technologies de l'information par les organismes publics facilite grandement la collecte, le traitement et la circulation des renseignements que les citoyens confient aux organismes publics. Les projets de développement ou de modification des systèmes d'information peuvent avoir des répercussions importantes sur leur droit au respect de la vie privée et à la protection des renseignements personnels (PRP).

Dans la foulée du *Plan d'action gouvernemental pour la PRP*, de la modernisation de l'État et du nouveau cadre de gestion de l'Administration gouvernementale axé sur la qualité des services offerts aux citoyens, la PRP constitue un enjeu majeur pour les organismes publics.

Le ministre des Relations avec les citoyens et de l'Immigration (MRCI) est responsable de l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, ci-après désignée « Loi sur l'accès » et de la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Dans l'exercice de ses responsabilités en matière de relations avec les citoyens, le ministre a notamment pour fonctions de favoriser l'accès des citoyens aux documents des organismes publics et d'assurer la protection des renseignements personnels détenus par les organismes publics ou par le secteur privé*.

La Direction du soutien en accès à l'information et en protection des renseignements personnels (DSAIPRP) relève du sous-ministre associé au secteur Identité, Accès et Prestation de services du MRCI.

La DSAIPRP a pour mission, d'une part, de conseiller le ministre et les autorités du Ministère en matière d'accès aux documents et de protection des renseignements personnels et, d'autre part, de soutenir les organismes publics et d'assurer une fonction de veille relativement à l'application de la *Loi sur la protection des renseignements personnels dans le secteur privé* dans le but de mieux connaître les problématiques et enjeux que pourrait poser son application.

La DSAIPRP a élaboré ce Modèle dans le but d'offrir un soutien aux organismes publics et de faciliter la mise en application des principes et des obligations légales de PRP dans les projets de développement, de modification et de déploiement des systèmes d'information, ci-après désignés « projets de développement ».

La prémisse sous-jacente à l'élaboration de ce document est que la mise en application des principes et obligations légales de PRP sera grandement facilitée s'ils sont présentés sous une forme pratique axée sur la description de buts, pratiques et produits de travail à réaliser qui pourront s'intégrer aisément dans les processus habituels d'un projet de développement. Ce document s'avérera utile aux parties prenantes dans un projet, notamment aux gestionnaires, aux responsables de la PRP (RPRP), aux chefs et chargés de projet et aux autres membres d'une équipe de développement.

---

* *Loi sur le ministère des Relations avec les citoyens et de l'Immigration*, art. 11 7°.

Le *Modèle de pratiques de PRP*, est un outil de référence. Ce faisant, l'intention du MRCI n'est pas d'imposer ce Modèle comme le seul outil valable pour réaliser la PRP dans un projet de développement. Chaque organisme public déterminera ce qui constitue pour lui le meilleur ensemble de pratiques de PRP à réaliser et les modalités de réalisation, compte tenu notamment des obligations légales de PRP auxquelles il est assujetti, de sa mission, des défis auxquels il doit faire face, de sa taille, des projets et des ressources dont il dispose.

OBJECTIFS DU MODÈLE

Le *Modèle de pratiques de PRP* est destiné à servir de base de connaissances ou de référence aux organismes publics pour faciliter le respect des principes et obligations légales de PRP lors des projets de développement faisant appel à des renseignements personnels.

LE CONTEXTE

Les citoyens sont de plus en plus renseignés à propos de leur droit au respect de la vie privée et à la protection des renseignements personnels et ils sont très préoccupés par les risques d'atteinte à ces droits qui découlent de l'utilisation accrue des télécommunications par les organismes publics et les entreprises. Ils s'attendent à ce que les organismes publics et les entreprises privées mettent en œuvre les meilleures pratiques pour assurer le respect des principes et des obligations légales de PRP, qu'ils gèrent ces renseignements de manière transparente et qu'ils leur fournissent une assurance à cet effet.

La protection des renseignements personnels et la sécurité sont des dimensions qui influent grandement sur la relation de confiance entre l'Administration publique, ses employés et les citoyens. Elles constituent un enjeu important dans les projets de développement des services ayant recours aux technologies de l'information, particulièrement des services électroniques rendus par l'État à ses clients ou à ses employés.

LE *PLAN D'ACTION GOUVERNEMENTAL POUR LA PRP*

Le 12 mai 1999, le ministre des Relations avec les citoyens et de l'Immigration diffusait le *Plan d'action gouvernemental pour la protection des renseignements personnels* à l'intention des ministères et des organismes gouvernementaux*. Ce plan vise à ce qu'ils prennent les dispositions nécessaires pour assurer la protection des renseignements personnels des citoyens québécois.

Ce plan d'action établit que :

- la protection des renseignements personnels doit être placée au plus haut niveau des préoccupations de tous les ministères et organismes gouvernementaux ;
- tous les ministères et organismes gouvernementaux doivent prendre les dispositions nécessaires pour assurer la protection des renseignements personnels qui leur sont confiés par les citoyens québécois.

* Consultez à ce sujet le site Web du MRCI : http://www.aiprp.gouv.qc.ca/protectionpublic/actions/actions.asp?Sect=1

Le MRCI considère qu'il est important de concevoir des outils pour permettre aux gestionnaires et au personnel travaillant au sein des organismes publics de s'approprier et de mettre en œuvre les principes et les obligations légales de PRP dans les projets liés aux technologies de l'information.

À cet égard, le gouvernement a notamment confié au MRCI une fonction conseil au niveau gouvernemental en matière d'accès et de PRP, et il a invité le ministre du MRCI et le ministre délégué à l'Administration et à la Fonction publique à produire des outils pour faciliter la prise en compte de la PRP*. De plus, plusieurs ministères et organismes ont fait part au MRCI de leur besoin d'outils à cet égard.

LA MODERNISATION DE LA FONCTION PUBLIQUE**

La modernisation de la fonction publique est une vaste entreprise menée par le gouvernement du Québec pour accroître l'efficacité de l'Administration gouvernementale, avec comme objectif ultime l'amélioration de la qualité des services aux citoyens (population et entreprises), et ce, à moindre coût. La modernisation est caractérisée notamment par la mise en place d'un nouveau cadre de gestion pour la fonction publique et par l'utilisation accrue des nouvelles technologies.

Le respect de la vie privée, la protection des renseignements personnels et une plus grande transparence relativement à la gestion des renseignements personnels constituent des éléments fondamentaux qui orientent la façon dont les services sont offerts aux citoyens. De plus, ils font partie des résultats à atteindre lors de la mise en œuvre du nouveau cadre de gestion de l'Administration gouvernementale.

La *Loi sur l'administration publique*, sanctionnée le 30 mai 2000, favorise la modernisation de la gestion gouvernementale et instaure un nouveau cadre de gestion de l'Administration gouvernementale. Selon la réforme proposée, les gestionnaires disposent d'une plus grande liberté d'action dans l'utilisation des moyens et sont davantage imputables de l'atteinte d'objectifs mesurables. L'accent est ainsi mis sur les résultats à atteindre.

Le Modèle de pratiques de PRP est un outil facilitant la mise en œuvre des orientations du Plan d'action gouvernemental pour la PRP dans les projets de développement des systèmes d'information. Il peut être utilisé par tous les organismes publics pour faciliter l'atteinte des résultats en matière de PRP dans les projets de développement des systèmes d'information.

---

* La *Loi sur l'administration publique* confère au Conseil du trésor le pouvoir de déterminer les orientations portant sur les principes ou les pratiques à favoriser en matière de gestion des ressources humaines, budgétaires, matérielles ou informationnelles (art. 72) et d'adopter des règles en matière de PRP et de sécurité (art. 66 1°).

** Consultez à ce sujet le site Web du Conseil du trésor sur la modernisation : www.tresor.gouv.qc.ca/ministre/modernisation/

LE *CADRE DE GESTION DES RESSOURCES INFORMATIONNELLES EN SOUTIEN À LA MODERNISATION DE L'ADMINISTRATION PUBLIQUE*

Le 29 janvier 2002, le Conseil du trésor adoptait, selon la *Loi sur l'administration publique*, le *Cadre de gestion des ressources informationnelles en soutien à la modernisation de l'Administration publique*. Ce cadre de gestion précise les mécanismes de gouverne visant l'utilisation optimale des ressources informationnelles pour soutenir la modernisation de l'Administration et pour mettre en place, par étapes, ce qu'il est convenu d'appeler une « administration électronique »*.

Il énonce sept principes fondamentaux constituant les balises des stratégies et des actions gouvernementales en matière de ressources informationnelles. Un de ces principes porte sur la sécurité et la protection des renseignements personnels :

« *Les ressources informationnelles doivent être utilisées et gérées dans le respect de la sécurité ainsi que de la protection des renseignements personnels et confidentiels. Les exigences à cet égard doivent être prises en compte dès la conception et le développement des nouveaux services d'affaires et des systèmes d'information.* »

Le MRCI et le Secrétariat du Conseil du trésor (SCT) travaillent en étroite collaboration dans leurs activités respectives liées à la production d'outils facilitant la prise en compte de la PRP et de la sécurité dans les projets de développement.

Le Modèle de pratiques de PRP est un outil produit par le MRCI pour faciliter la mise en œuvre de ce principe directeur du cadre de gestion des ressources informationnelles en ce qui concerne la PRP.

LA CLIENTÈLE ET LES RENSEIGNEMENTS VISÉS

LES ORGANISMES VISÉS

Le *Modèle de pratiques de PRP* a été élaboré à l'intention de tous les organismes publics soumis à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels***. Les organismes publics québécois comprennent les ministères et les organismes gouvernementaux, ainsi que les organismes des secteurs municipal, scolaire et de la santé et des services sociaux.

LES RENSEIGNEMENTS VISÉS

Le processus de PRP décrit dans ce document traite des renseignements personnels. La Loi sur l'accès établit que : « Dans un document, sont nominatifs les renseignements qui concernent une personne physique et permettent de l'identifier » (article 54).

Dans le présent document, le terme « renseignements personnels » est utilisé dans le même sens que « renseignement nominatif », tel qu'il est défini dans la Loi sur l'accès.

---

* Extrait du site Web du Secrétariat du Conseil du trésor sur l'autoroute de l'information http://www.autoroute.gouv.qc.ca/dossiers/cadre_de_gestion_ct197638.pdf

** Pour connaître plus en détail les organismes publics soumis à la Loi sur l'accès, consultez le site Web du MRCI : http://www.aiprp.gouv.qc.ca/protectionpublic/intervenants/intervenants.asp

LES INTERVENANTS VISÉS

Ce document peut être utilisé par toutes les parties prenantes à un projet de développement que nous présentons selon deux catégories :

- les autorités supérieures, les conseillers et les intervenants agissant sur un plan horizontal dans un organisme public ;
- les membres de l'équipe d'un projet de développement d'un système d'information.

Les autorités supérieures, les conseillers et les intervenants agissant sur un plan horizontal dans un organisme public

- **La haute direction, le responsable ministériel de la PRP ou de l'organisme et les conseillers**

  La haute direction réfère aux personnes travaillant aux échelons supérieurs de la direction d'un organisme public. Elles comprennent : le sous-ministre, les sous-ministres associés et adjoints, le président-directeur général, les vice-présidents chargés des directions fonctionnelles, les directeurs généraux et les directeurs des différents services.

  La Loi sur l'accès prévoit que « la personne ayant la plus haute autorité au sein d'un organisme public exerce les fonctions que la présente loi confère à la personne responsable de l'accès aux documents ou de la protection des renseignements personnels ». Toutefois, « cette personne peut désigner comme responsable un membre de l'organisme public ou de son conseil d'administration, selon le cas, ou un membre de son personnel de direction et lui déléguer tout ou partie de ses fonctions » (article 8).

  Dans la plupart des cas, la personne désignée responsable de l'accès assume à la fois la responsabilité de traiter les demandes d'accès aux documents et d'assurer la protection des renseignements personnels, leur accès et leur rectification. Le *Plan d'action gouvernemental pour la PRP* prévoit par ailleurs que la personne responsable de la PRP doit relever directement du sous-ministre ou du dirigeant de l'organisme.

  Ainsi, compte tenu que plusieurs des exigences de PRP sont des obligations légales et que des responsabilités légales et administratives sont confiées aux personnes désignées responsables de l'accès et de la PRP, il est très important qu'elles soient associées à la réalisation du processus de PRP, de même que les conseillers juridiques de l'organisme public.

  Dans ce document, la personne qui agit à titre de responsable de l'accès et de la PRP en fonction de la Loi sur l'accès et qui exerce sa fonction pour l'ensemble de l'organisation est désignée « responsable de la PRP de l'organisme public » (RPRP) et la personne assignée à la réalisation du processus de PRP dans un projet est désignée « répondant de la PRP ».

- **Le responsable de la sécurité de l'information numérique (RSIN)**

  Le RSIN est désigné par les sous-ministres ou les dirigeants des ministères et organismes pour assurer la gestion et la coordination de la sécurité et les représenter en cette matière dans l'organisation.

  Dans un projet de développement, il intervient notamment en ce qui concerne les mesures de sécurité à mettre en place pour respecter les principes et les obligations légales de PRP, et ce, tout au long de leur cycle de vie.

Dans les autres organismes publics, par exemple ceux du secteur de la santé et des services sociaux, des secteurs scolaire ou municipal, une personne peut également être désignée responsable de la sécurité et jouer un rôle similaire à celui du RSIN.

- **Le vérificateur interne**

  Il peut intervenir pendant le processus de développement, que ce soit *a priori* ou *a posteriori*, pour assurer notamment l'application des exigences de PRP dans le projet de développement.

  Il peut offrir un soutien, conseiller et accompagner les personnes relativement à la démarche d'intégration de la PRP dans les projets et à la prise en compte des risques qui y sont associés.

- **Le responsable des méthodes de développement et de gestion de projet**

  Il agit comme le « gardien » des méthodes nécessaires à la réalisation des projets. Il peut avoir à adapter ces méthodes pour tenir compte plus explicitement des exigences de PRP.

Les membres de l'équipe d'un projet de développement d'un système d'information

- **Le directeur de projet**
- **Le chef et le chargé de projet**
- **Le pilote de système**
- **Le répondant de la PRP dans le projet**

  Cette personne est désignée spécialement pour coordonner et réaliser le processus de PRP dans un projet. La fonction de répondant de la PRP pourrait également être assumée par le chargé de projet, par le RPRP ou par une personne qu'il désigne, ou par toute autre personne qui détient l'autorité et la compétence requises.

- **D'autres membres**

  Ces membres peuvent être notamment le spécialiste en gestion des risques des projets de développement, le spécialiste de la gestion documentaire, le spécialiste de la gestion de la sécurité, celui-ci pouvant être le responsable de la sécurité de l'information numérique (RSIN) dans les ministères et organismes ou une autre personne désignée à cet effet.

  Se référer au tableau 1 – Légende des rôles des parties prenantes dans un projet de développement *pour une description générale des rôles des parties prenantes dans un projet de développement*.

LES AVANTAGES DÉCOULANT DE L'UTILISATION DU MODÈLE

Le Modèle fournit plus qu'une description de pratiques et de biens livrables. Il propose, selon une approche d'amélioration continue, une route, un chemin à suivre pour intégrer la PRP de plus en plus dans la culture de l'organisation relativement aux projets de développement.

Ainsi, il facilite non seulement la réalisation du processus de PRP dans les projets, mais également la planification, le suivi et le contrôle de ce processus, et ce, tant à l'échelle d'un projet qu'à celle de tous les projets de l'organisation. Il contribue ainsi à la détermination d'objectifs de PRP à atteindre à court, moyen et long terme, et ce, tant pour les petits et moyens organismes publics que pour les grands.

De plus, la description des principes et des obligations légales de PRP sous la forme de buts, pratiques et biens livrables, dans un langage et une approche propres aux membres des équipes de développement, peut faciliter la prise en compte de la PRP dans les projets à toutes les phases des projets.

Ce document peut également contribuer à faciliter le travail des RPRP en leur fournissant un outil pour partager les connaissances relativement aux principes et aux obligations légales de PRP. Il peut favoriser les communications entre les parties prenantes des projets de développement en ce qui concerne les exigences de PRP.

Par ailleurs, la prise en compte de la PRP dès les premières étapes d'un projet de développement d'un système d'information, et pendant sa réalisation, contribue au succès de ce projet. Dans le domaine des technologies, il est reconnu qu'il en coûte beaucoup plus cher d'ajouter une exigence après la conception plutôt qu'à la phase de la conception initiale du système. Ce principe s'applique également dans le domaine de la sécurité.

L'intégration du processus de PRP dans les projets de développement et de modification des systèmes d'information constitue ainsi un avantage pour les organismes publics. Cela peut se traduire par des économies substantielles en évitant d'avoir à remettre en question des aspects importants d'un système d'information et de le modifier, pour y intégrer la PRP, une fois qu'il est complété.

Enfin, la PRP est une dimension de la qualité des services offerts aux citoyens. Elle contribue à accroître la confiance des citoyens envers les organismes publics et peut les inciter à recourir de plus en plus aux services offerts par voie électronique.

L'UTILITÉ DU MODÈLE

Ce Modèle peut être utilisé par toutes les parties prenantes dans un projet de développement pour faciliter l'atteinte d'objectifs communs de PRP et particulièrement par les responsables de la PRP et les personnes désignées « répondants de la PRP » dans le projet. Il peut notamment servir à déterminer le processus de PRP à réaliser dans un projet de développement afin de respecter les principes et les obligations légales de PRP. Il peut également servir à déterminer les améliorations qui peuvent être apportées à ce processus et aux produits qui en découlent.

Introduction

POURQUOI LE MRCI A-T-IL PRODUIT UN *MODÈLE DE PRATIQUES DE PRP* ?

Le développement d'un système d'information constitue toujours un défi important pour une organisation. Comment développer ou modifier un système d'information qui répond aux besoins des clients et des utilisateurs avec une économie d'efforts et de coûts tout en respectant les délais ?

Parmi les exigences d'un projet de développement, le respect des lois, notamment de la Loi sur l'accès, est une exigence incontournable des organismes publics pour respecter la vie privée et assurer la PRP de leurs clients et de leurs employés.

L'intégration de la PRP dans un projet de développement fait appel à divers domaines d'expertise tels que juridique, organisationnel, gestion de projet, gestion des risques, gestion de la sécurité, gestion documentaire, développement technologique et autres. Dans le contexte de la modernisation de la fonction publique, notamment du développement des services électroniques, il apparaît important de créer, en matière de PRP, une synergie entre ces différents domaines et de « démocratiser » en quelque sorte les obligations légales de PRP au bénéfice de l'ensemble des organismes publics et, finalement, des citoyens.

C'est dans cette optique que le MRCI a produit une base commune de connaissances ou de bonnes pratiques en PRP à laquelle les parties prenantes dans un projet de développement pourront se référer lorsqu'ils intègrent la PRP comme faisant partie des exigences prioritaires d'un projet. Ainsi, dans ce document, les principes et les obligations légales de PRP sont présentés dans un langage et une logique propres aux projets tout en gardant à l'esprit que la PRP est avant tout une obligation légale pour les organismes publics.

LES BASES D'ÉLABORATION DU MODÈLE

Le *Modèle de pratiques de PRP* a été élaboré en se basant sur le *Modèle intégré d'évolution des capacités* (intitulé « Modèle de référence CMMI »), en ce qui a trait à la structuration des pratiques, et sur la Loi sur l'accès, d'autres lois québécoises et des principes de PRP reconnus internationalement, en ce qui a trait au contenu même du Modèle.

LE MODÈLE DE RÉFÉRENCE CMMI

Le modèle de référence CMMI, ou *Modèle intégré d'évolution des capacités*, a servi de base de référence pour établir la structure des pratiques du *Modèle de pratiques de PRP*.

Le modèle de référence CMMI a été publié en 2001 par un institut de l'université Carnegie Mellon de Pittsburg, soit le Software Engineering Institute (SEI). Le modèle de référence CMMI est reconnu dans la communauté informatique internationale comme un modèle de référence relativement au développement et à la modification des systèmes informatiques (incluant autant le matériel que le logiciel). Le modèle de référence CMMI est le résultat d'un consensus de milliers d'informaticiens et d'ingénieurs de systèmes informatiques à l'échelle internationale, tant du secteur public que privé.

Le modèle de référence CMMI comprend un compendium des meilleures pratiques ordonnancées de façon à favoriser l'amélioration continue. En effet, la structure du modèle de référence CMMI contient les éléments essentiels de processus efficaces d'une discipline donnée. Ces éléments sont basés sur les concepts d'amélioration de la qualité développés par des spécialistes tels que Crosby, Deming, Juran et Humphrey. Le *Modèle de pratiques de PRP* hérite donc de la structure du modèle de référence CMMI et du concept d'amélioration continue qui y est sous-jacent.

La version du modèle de référence CMMI utilisée comme base dans ce *Modèle de pratiques de PRP* est :

Capability Maturity Model Integration
(CMMI[SM] for Systems Engineering/Software
Engineering/Integrated Product and Process Development)
(CMMI[SM]-SE/SW/IPPD, V1.1), Continuous Representation
(CMU/SEI-2002-TR-003 , ESC-TR-2002-P003), décembre 2001

Cette version du modèle de référence CMMI est conforme à la norme ISO / CÉI 15504 portant sur l'évaluation des processus logiciels tout en demeurant en continuité avec la version antérieure du CMMI, soit le CMM (*Modèle d'évolution des capacités logiciel*), laquelle est en usage dans la communauté informatique internationale depuis plus de dix ans. D'ailleurs, quelques ministères et organismes du gouvernement du Québec ont adopté cette base de référence pour orienter l'évolution de leurs capacités en matière de développement et de modification de systèmes d'information.

Le modèle de référence CMMI, par sa conception ouverte, peut être appliqué à d'autres domaines d'activités ou à des spécialisations du domaine du développement et de modification de systèmes, tels que la sécurité et la protection des renseignements personnels. Il offre une structure réutilisable de systématisation de pratiques. C'est pourquoi le MRCI a utilisé cette structure pour concevoir le *Modèle de pratiques de PRP*.

Ainsi, le *Modèle de pratiques de PRP* qui en résulte peut s'insérer naturellement dans tout environnement informatique faisant appel au CMMI ou au CMM.

Dans un souci de rendre ce Modèle utilisable dans les organismes publics qui n'utilisent pas déjà le CMM ou le CMMI, le Modèle a été conçu de façon à ce qu'il soit un document complet en lui-même et le plus autonome possible. Tout organisme public devrait être en mesure de l'intégrer dans son environnement de développement et de modification de systèmes d'information.

Le Modèle de pratiques de PRP peut donc être utilisé par tout organisme public, peu importe s'il utilise ou non le modèle de référence CMMI.

Le recours à la structure du modèle de référence CMMI a permis de réutiliser certains formalismes de représentation des différents composants du Modèle tels que les pratiques, sous-pratiques et biens livrables.

Ainsi, tous les composants de même type sont décrits de la même façon afin de faciliter leur lecture et de reconnaître rapidement le type de composant. Ce formalisme se retrouve décrit principalement dans les chapitres sur les composants des parties 1 et 2 du Modèle.

LA LOI SUR L'ACCÈS, D'AUTRES LOIS QUÉBÉCOISES ET DES PRINCIPES RECONNUS INTERNATIONALEMENT

La protection de la vie privée des citoyens occupe une place prépondérante dans toute société démocratique. Les lois reflètent les valeurs fondamentales de la société et la majorité des pays démocratiques à travers le monde se sont dotés de lois afin d'assurer aux citoyens le respect de leur vie privée et de permettre l'exercice de leur droit d'accès à l'information.

Outre les obligations légales au Québec, les principes et les bonnes pratiques de PRP reconnus internationalement ainsi que des initiatives en sécurité de l'information fournissent aux organismes publics un cadre de référence qui permet d'enrichir le développement d'outils facilitant la mise en œuvre de la PRP.

La figure 1 qui suit illustre les différentes sources d'information qui ont guidé l'élaboration de ce document.

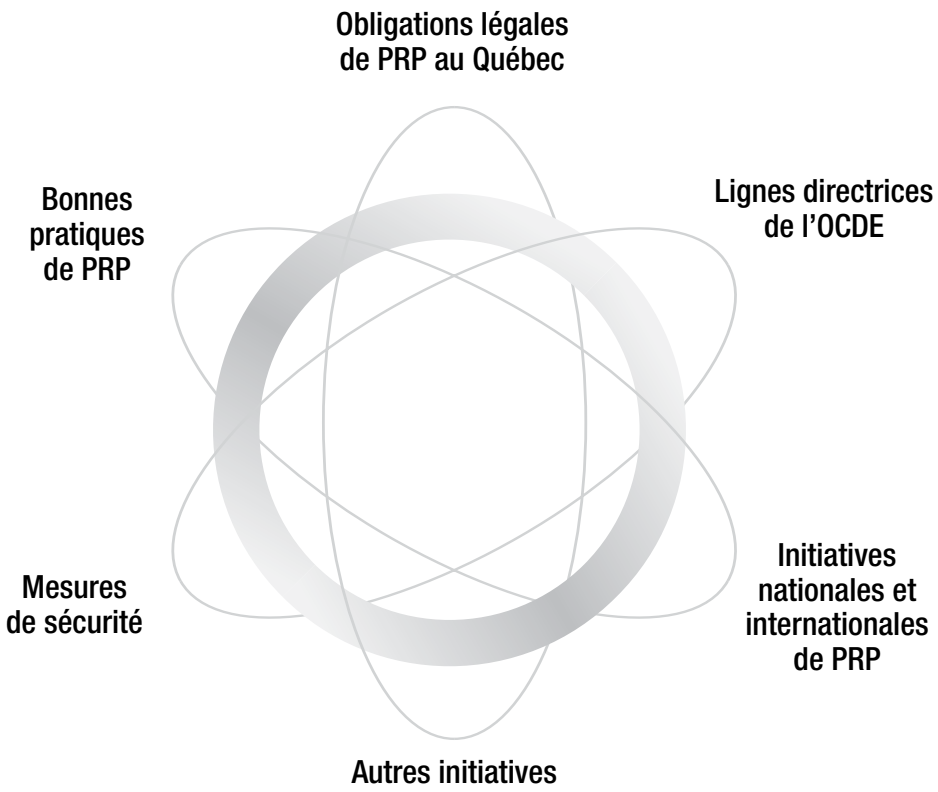


Figure 1 *Sources d'information concernant la PRP*

Pour les organismes publics québécois, la mise en œuvre des bonnes pratiques de PRP repose en premier sur les dispositions de la Loi sur l'accès et des autres dispositions légales de PRP auxquelles ils sont assujettis.

Plus spécifiquement, le *Modèle de pratiques de PRP* a été élaboré sur la base de dispositions légales de PRP du Québec et de principes de PRP découlant des documents suivants.

Les dispositions légales traitées de façon particulière dans le Modèle

- Le chapitre 3 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ;
- les articles 36 et 37 du chapitre 3 du *Code civil du Québec* « Du respect de la réputation et de la vie privée » ;
- les articles 7, 8 et 15 de la *Loi sur les archives*.

Les autres dispositions légales traitées de façon générale dans le Modèle

- La *Loi concernant le cadre juridique des technologies de l'information*

  Cette loi permet d'assurer l'intégrité des documents et d'établir leur valeur juridique durant tout leur cycle de vie. Elle comporte certaines dispositions sur la PRP et la sécurité dont il y a lieu de tenir compte lors de l'intégration du Modèle dans un organisme public.

- Les dispositions légales de PRP auxquelles un organisme public est assujetti

  Outre les lois mentionnées précédemment, les organismes publics peuvent être assujettis à d'autres dispositions légales de PRP. Lorsqu'ils intègrent la PRP dans un projet de développement, ils s'assurent donc que les principes et les obligations de ces lois sont respectés.

Les principes de PRP

Les *Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières des données de caractère personnel* (1980) auxquelles le Canada a adhéré sont devenues la norme nationale en matière de protection des données et le fondement des lois sur la PRP.

Elles énoncent les principes fondamentaux suivants :

- limitation en matière de collecte des renseignements personnels ;
- qualité des données ;
- spécification des finalités ;
- limitation de l'utilisation ;
- garanties de sécurité ;
- transparence ;
- participation individuelle ;
- responsabilité des entités*.

---

* Pour obtenir plus d'information sur les directives internationales sur la vie privée et le cadre légal et administratif québécois à l'égard du respect de la vie privée, de la PRP et de la sécurité de l'information, consultez l'annexe J Cadre légal et administratif de la PRP et de la sécurité et directives nationales et internationales.

Bref rappel de la Loi sur l'accès et des obligations des organismes publics en matière de PRP

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* a été adoptée le 22 juin 1982. Elle est habituellement désignée par : « Loi sur l'accès ».

La Loi sur l'accès met en application deux droits énoncés dans la *Charte des droits et libertés de la personne* du Québec : le droit à l'information (article 44) et le droit au respect de la vie privée (article 5).

Elle comporte deux grands objectifs. Le premier garantit à toute personne un droit d'accès aux documents des organismes publics. Le second prévoit un ensemble de principes et de règles pour assurer la protection des renseignements personnels.

Ce deuxième volet accorde notamment à toute personne le droit d'avoir accès aux renseignements la concernant et d'en demander leur rectification. Il consacre le principe de confidentialité des renseignements personnels et prévoit plusieurs obligations pour les organismes publics visant à assurer la PRP tout au long de leur cycle de vie. Les dispositions légales associées au processus de PRP décrit dans le Modèle réfèrent à ce deuxième volet de la Loi sur l'accès.

La Loi sur l'accès a un statut particulier. En effet, la Loi sur l'accès a préséance sur les autres lois du Québec, à moins que ces lois n'énoncent, expressément, s'appliquer malgré la présente loi*.

Elle s'applique aux documents détenus par les organismes publics dans l'exercice de leurs fonctions, que leur conservation soit assurée par l'organisme public ou un tiers. Elle s'applique quelle que soit la forme du document : écrite, sonore, visuelle, informatisée ou autre (article 1).

En matière de PRP, les organismes publics doivent notamment :

- mettre en place les mesures nécessaires pour permettre aux personnes d'exercer leur droit d'accès aux renseignements et de rectification de ceux-ci ;
- prendre les mesures nécessaires pour que les principes et les dispositions de PRP de la Loi sur l'accès et des autres lois auxquelles ils sont assujettis, soient respectés et mis en œuvre.

Les notions de respect de la vie privée, de protection des renseignements personnels et de sécurité de l'information

Les notions de respect de la vie privée, de PRP et de sécurité de l'information sont distinctes, complémentaires et interreliées. La figure 2, qui suit, illustre ces interrelations en faisant ressortir que la sécurité de l'information est une notion distincte de la PRP et qu'elle est un des moyens d'assurer la PRP. Elle n'est pas garante de la protection des renseignements personnels au sens de la Loi sur l'accès ou d'une autre

* Pour obtenir plus d'information sur cette loi, consultez le site Web du MRCI : www.aiprp.gouv.qc.ca et le site Web de la CAI : www.cai.gouv.qc.ca/fra/cai_fr/cai_fr.htm

loi. Par ailleurs, la sécurité réfère à des dimensions qui ne sont pas régies par la Loi sur l'accès. Ainsi, le processus de PRP décrit dans ce document n'englobe pas toutes les pratiques de sécurité qu'un organisme public met en œuvre dans un projet de développement pour garantir la sécurité de l'information et des systèmes*.

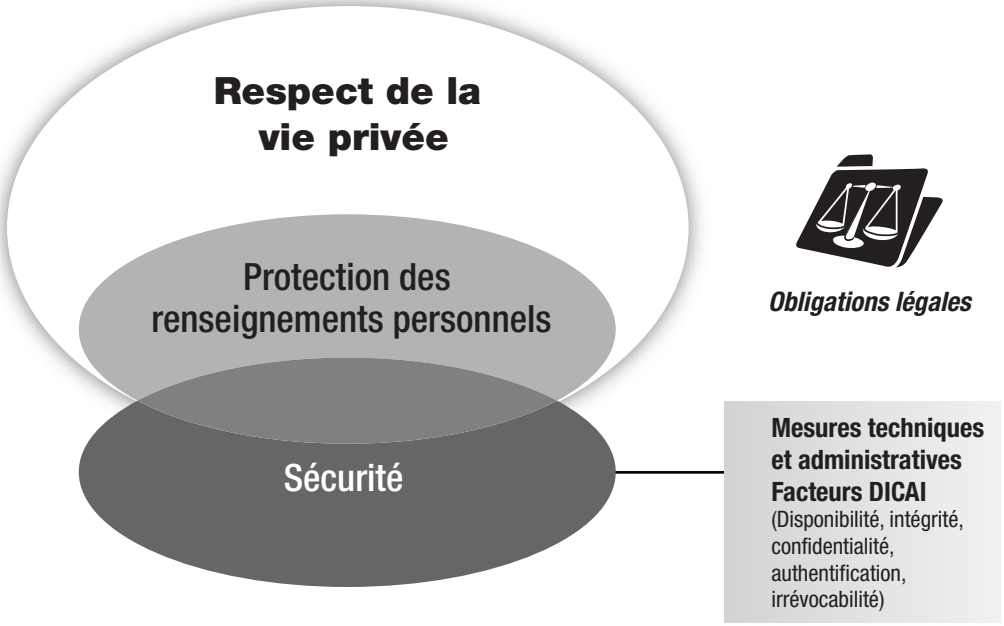


Figure 2 *Interrelations entre les notions de respect de la vie privée, de PRP et de sécurité***

Le cycle de vie de la protection des renseignements personnels

La protection des renseignements personnels constitue une des dimensions du respect de la vie privée. En principe, toute personne a un droit de regard sur les renseignements qui la concernent et qui peuvent être colligés, accessibles, utilisés, communiqués, conservés et détruits par un organisme public. Ces activités constituent les moments clés du cycle de vie des renseignements personnels.

---

* Pour obtenir plus d'information sur les notions de vie privée, de protection des renseignements personnels, de confidentialité et de sécurité, consultez le site Web du MRCI à : http://www.aiprp.gouv.qc.ca/protectionpublic/prpcest/prpcest.asp

** Pour obtenir plus d'information sur la sécurité de l'information, consultez la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale* du Conseil du trésor sur le site Web du Conseil du trésor : www.tresor.gouv.qc.ca/doc/acrobat/dirsec1.pdf

La protection des renseignements personnels se traduit concrètement par le respect des principes et des règles de la Loi sur l'accès relativement à :

- la collecte de renseignements personnels ;
- l'accès aux renseignements personnels et leur rectification par la personne concernée ;
- leur accessibilité par les membres du personnel de l'organisme public ;
- leur utilisation à l'intérieur de l'organisme public ;
- leur communication à des tiers, à l'extérieur de l'organisme public (à des personnes, des organismes publics ou des entreprises privées) ;
- leur conservation ;
- leur destruction ;
- la transparence des pratiques de gestion des renseignements personnels (par exemple par la déclaration des fichiers de renseignements personnels à la Commission d'accès à l'information).

La figure 3 qui suit représente le schéma du cycle de vie de la PRP tel qu'il est décrit dans le *Modèle de pratiques de PRP*.

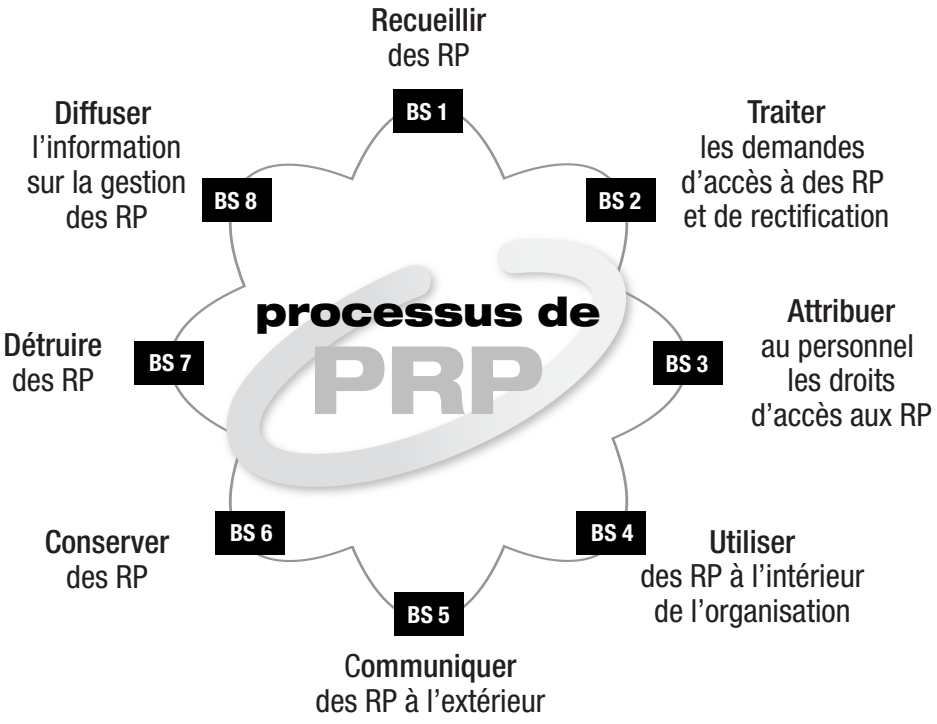


Figure 3 *Schéma du cycle de vie de la PRP*

* RP : renseignements personnels

PORTÉE ET LIMITES DU MODÈLE

Le Modèle présente des pratiques de PRP généralement réalisées pour assurer le respect des principes et obligations légales de PRP dans un projet de développement d'un organisme public.

LA PORTÉE DU MODÈLE

Bien que les principes et les dispositions légales de PRP s'appliquent à l'ensemble des activités de gestion des renseignements personnels d'un organisme public, le processus de PRP décrit dans ce document porte uniquement sur les projets de développement et de modification des systèmes d'information par les organismes publics. Il ne traite pas directement le volet « exploitation » du système, ce dernier étant lié notamment à la performance et la sécurité du système et à la surveillance du réseau, ni le volet « utilisation » du système d'information.

Toutefois, les dimensions relatives à l'exploitation et à l'utilisation des renseignements personnels devant être présentes lors du développement ou de la modification d'un système d'information sont, quant à elles, prises en compte dans les pratiques de PRP lorsque cela est approprié.

Il est important de rappeler qu'un système d'information comprend non seulement une dimension informatique importante, mais également tous les renseignements versés sur d'autres supports et les processus administratifs rattachés à ce système. Ce document englobe donc les volets informatique et administratif d'un système d'information.

Dans ce document, afin de simplifier le texte, le terme « développement » sera utilisé pour désigner à la fois le développement, la modification et le déploiement d'un système d'information, soit trois des phases du cycle de vie d'un système. Il pourra arriver que les termes « modification » ou « déploiement » soient utilisés lorsqu'il sera nécessaire de se référer uniquement à une phase précise du cycle de vie d'un système.

Le *Modèle de pratiques de PRP* est un référentiel ou une base de connaissances en PRP. Il rassemble une partie des connaissances et de l'expérience de spécialistes en PRP et en développement des systèmes d'information, applicables dans les projets de développement des systèmes d'information.

Il comprend un ensemble d'informations relatives aux activités qu'une organisation peut mettre en œuvre pour respecter les principes et les obligations légales de PRP dans ses projets. Les informations rassemblées dans le Modèle sont interreliées et structurées de telle sorte qu'on puisse en extraire des éléments d'information pertinents selon les besoins des différents utilisateurs et des parties prenantes dans des projets de développement.

Le *Modèle de pratiques de PRP* est une description d'un processus de PRP basé sur les principes d'amélioration continue. Il propose un processus de PRP basé sur les principes d'amélioration continue. Il présente les principes et obligations légales de PRP en les décrivant sous forme de buts, pratiques, sous-pratiques et biens livrables, en fonction de tout le cycle de vie de la PRP. Ils sont réalisés collectivement pour atteindre huit buts spécifiques de PRP et constituent le volet spécifique du « processus de PRP ». Ces huit buts spécifiques sont accompagnés de buts et de pratiques de gestion qui proposent un cheminement pour faciliter le travail des organismes publics qui désirent améliorer, selon une approche de « petits pas », la réalisation et la gestion du processus de PRP dans leurs projets et à l'échelle de l'organisation.

Ce document en détermine les principales caractéristiques et fournit des indications afin d'en faciliter la mise en application dans les projets de développement. La structure de présentation s'appuie sur un modèle reconnu internationalement dans le domaine de l'amélioration des capacités de développement des systèmes.

Le *Modèle de pratiques de PRP* est un outil facilitant l'intégration de la PRP dès le début des projets de développement et pendant toute leur durée. Il peut être utilisé à toutes les phases d'un projet de développement d'un système d'information, et ce, dès les études préliminaires d'un projet, pour déterminer, par exemple, les buts de PRP à atteindre dans le projet et les pratiques et biens livrables associés. Il peut être utilisé pendant les autres phases de développement afin de concrétiser dans le système d'information en développement les choix de PRP qui ont été faits en amont du projet.

Il peut également être utilisé afin que les principes et les obligations légales de PRP soient respectés par les membres de l'équipe de développement. Ils utilisent par exemple des renseignements anonymes ou fictifs lorsqu'ils effectuent des essais ou dispensent de la formation.

LES LIMITES DU MODÈLE

Le *Modèle de pratiques de PRP* n'est pas un document normatif. Les organismes publics ont la responsabilité de mettre en œuvre les principes et les dispositions légales de PRP découlant de la Loi sur l'accès et des autres dispositions légales de PRP qui s'appliquent. Ce document n'introduit aucune nouvelle obligation ou responsabilité pour les organismes publics. Il est essentiellement un outil de référence qui décrit ce qui peut être réalisé pour respecter les principes et les dispositions légales de PRP. La Loi sur l'accès et les autres dispositions légales en PRP qui s'appliquent ont toujours préséance.

Le processus de PRP est élaboré de telle sorte que les organismes détermineront la pertinence d'implanter telles ou telles pratiques de PRP proposées dans le Modèle en fonction de leurs objectifs d'affaires et de leurs ressources, tout en respectant les obligations minimales découlant des lois et en maîtrisant les zones à risque.

Le *Modèle de pratiques de PRP* n'est pas un guide. Il fournit une description des pratiques à réaliser pour produire des biens livrables types. Ainsi, les buts et pratiques proposés réfèrent à ce qui peut être fait pour réaliser la PRP (le « quoi »), sans toutefois indiquer la façon de le faire (le « comment »), sauf à certaines occasions où une façon de faire est illustrée par un exemple.

La façon de réaliser la PRP est donc laissée à la discrétion des organismes publics en fonction, notamment de leur contexte particulier d'affaires, de leur environnement de développement spécifique et des particularités des projets à gérer.

Le *Modèle de pratiques de PRP* n'est pas un document juridique. Il décrit des exemples de pratiques et de biens livrables contribuant à l'atteinte des buts de PRP en fonction des principes et dispositions légales de PRP. Plusieurs des pratiques sont associées à des dispositions de la Loi sur l'accès ou d'autres lois, et ces dispositions sont indiquées. Toutefois, le Modèle ne précise pas comment elles doivent être interprétées pour assurer le respect de la loi.

Pour la réalisation de certaines pratiques, il y aura lieu de préciser avec le RPRP et les conseillers juridiques, les critères à respecter en fonction des dispositions légales qui s'appliquent et de la jurisprudence. En ce sens, bien que son utilisation par un organisme public contribue à ce que ses systèmes d'information soient conformes à la Loi sur l'accès, il n'est pas, comme tel, un outil de vérification ou « d'audit » de la conformité à cette loi (contrôle de la PRP *a posteriori*).

Le *Modèle de pratiques de PRP* n'est pas un modèle de pratiques sur la sécurité. La PRP ne peut se réaliser sans la mise en œuvre de mesures de sécurité. Bien que ce Modèle inclut des pratiques de PRP qui sont reliées ou communes à celles de sécurité, il ne traite pas de façon détaillée des pratiques de sécurité à mettre en œuvre dans un projet de développement, tel que cela est illustré à la figure 2. À cet égard, il y a lieu de se référer aux documents portant sur la sécurité et aux normes, directives et orientations du Conseil du trésor et de son secrétariat.

De même, le Modèle ne traite pas de façon détaillée des mesures de protection de l'intégrité des documents ou de la protection des renseignements confidentiels aux termes de la *Loi concernant le cadre juridique des technologies de l'information*.

Le *Modèle de pratiques de PRP* ne traite pas de l'ensemble des renseignements confidentiels. Il traite uniquement des renseignements personnels qui revêtent un caractère confidentiel.

Par exemple, des documents recelant des renseignements confidentiels, tels que des secrets industriels ou des renseignements techniques qu'un fournisseur transmet à un organisme public dans une offre de services, ne sont pas des renseignements personnels et ils ne sont pas traités dans le présent document.

CONVENTIONS ÉDITORIALES

Les conventions éditoriales utilisées visent à faciliter la lecture du Modèle et son utilisation en permettant d'identifier et de trouver rapidement les différents composants du Modèle. L'uniformité dans la présentation de chacun des composants de même type permet d'en simplifier la lecture et sa compréhension. Ainsi, les mêmes termes sont utilisés systématiquement pour désigner une même chose, sans chercher à trouver d'autres synonymes qui pourraient semer le doute dans l'esprit du lecteur.

Les conventions éditoriales utilisées, héritées pour la plupart du modèle de référence CMMI, seront expliquées tout au long du document, au fur et à mesure qu'elles apparaissent.

Une convention spécifique au *Modèle de pratiques de PRP* a été ajoutée et il convient de la souligner dès maintenant. Il s'agit d'une obligation légale associée à une pratique. Cette association est représentée par un pictogramme situé dans la marge de gauche, vis-à-vis de la pratique concernée. Ce pictogramme contient l'image d'une balance représentant la justice, pour indiquer la nécessité d'une interprétation de la pratique selon une disposition légale ; cette image est accompagnée des articles des lois associés à la pratique. À titre d'exemple, on retrouve :

Art. 54
Loi sur l'accès

Il convient cependant de noter que, même si une pratique n'est pas associée à une obligation légale, cela ne veut pas dire que sa réalisation n'est pas importante. Elle peut constituer un préalable à la réalisation d'une pratique associée à une obligation légale. Dans certains cas, sa non-réalisation pourrait placer l'organisation dans une situation de vulnérabilité.

OÙ TROUVER DE L'INFORMATION COMPLÉMENTAIRE ?

Vous pouvez trouver de l'information complémentaire sur la protection des renseignements personnels en consultant le site du ministère des Relations avec les citoyens et de l'Immigration (MRCI) :

http://www.aiprp.gouv.qc.ca/index.asp

Vous pouvez trouver de l'information complémentaire sur le *Modèle intégré d'évolution des capacités* (Capability Maturity Model Integration – CMMI) en consultant le site du Software Engineering Institute (SEI) :

www.sei.cmu.edu/cmmi

Se référer également à l'annexe A – Médiagraphie pour d'autres sources documentaires.

Comment intégrer le Modèle dans l'organisme public ?

Le *Modèle de pratiques de PRP* a été élaboré à l'intention des organismes publics afin de faciliter le respect des principes et des dispositions légales de protection des renseignements personnels dans leurs projets de développement des systèmes d'information faisant appel à des renseignements personnels.

Le fait que ce Modèle s'applique à l'ensemble des organismes publics et qu'il ne soit pas un document normatif ou un guide décrivant une façon de faire à appliquer telle quelle peut impliquer une certaine adaptation. Cette adaptation ou ajustement permet aux organismes publics qui décident d'utiliser le Modèle, de l'intégrer efficacement dans leur environnement particulier. Cela facilite ainsi son appropriation et son utilisation dans les projets de développement. L'utilisation du Modèle et son adaptation demeurent donc un choix de l'organisme public.

Ce chapitre propose des pistes d'adaptation possible afin que ce Modèle soit le plus facilement et rapidement utilisable lors du développement des systèmes d'information, et ce, à moindre coût.

L'adaptation éventuelle se fera donc selon le contexte particulier de l'organisme public et de son environnement méthodologique en place. Les adaptations au Modèle doivent toutefois se faire de telle sorte que les buts de PRP puissent être atteints, tout en gardant à l'esprit que la Loi sur l'accès et les autres dispositions légales de PRP ont toujours préséance lors de l'interprétation des buts et des pratiques spécifiques de PRP.

Les considérations entourant l'intégration du Modèle dans un organisme public sont regroupées dans les quatre sections suivantes :

- adaptation minimale du Modèle :
  portant sur les modifications minimales à apporter au Modèle pour pouvoir l'utiliser rapidement ;
- adaptation du Modèle selon le contexte de l'organisme public :
  portant sur les adaptations pouvant y être apportées pour tenir compte de son contexte particulier ;
- adaptation de l'environnement de développement :
  portant sur les adaptations pouvant être apportées à l'environnement existant de développement des systèmes d'information ;
- répartition des rôles et responsabilités à l'égard de l'intégration :
  portant sur les différentes responsabilités pouvant incomber aux parties prenantes pour réaliser les adaptations qu'un organisme public juge utiles de faire.

ADAPTATION MINIMALE DU MODÈLE

Il est possible de se restreindre à une adaptation minimale qui peut se réaliser rapidement afin de permettre l'utilisation du Modèle dans un organisme public. Les activités suivantes seront réalisées :

- vérifier si l'organisme public concerné est assujetti à d'autres dispositions légales de PRP que celles de la Loi sur l'accès et, si oui, adapter le Modèle en fonction de ces dispositions particulières (tel qu'il est décrit ci-dessous dans « Cadre légal et organisationnel ») ;
- décider d'adopter tels quels les pratiques et les biens livrables proposés (tel qu'il est décrit dans « Préférences de pratiques et de biens livrables types » à la page 16) après en avoir fait la revue ;
- si l'organisme public possède une méthode de développement, y insérer des références aux pratiques du Modèle (tel qu'il est décrit dans « Méthode de développement » à la page 17).

ADAPTATION DU MODÈLE SELON LE CONTEXTE DE L'ORGANISME PUBLIC

Le *Modèle de pratiques de PRP* peut nécessiter une adaptation au contexte particulier de l'organisme public si, par exemple, cet organisme public est assujetti à des dispositions légales particulières relatives à la PRP ou s'il s'est déjà doté d'un cycle de vie de la PRP qui diffère du cycle de vie retenu pour ce Modèle. Les principales adaptations possibles portent sur les éléments suivants :

- cadre légal et organisationnel ;
- cycle de vie de la protection des renseignements personnels ;
- nature des projets ;
- préférences de pratiques et de biens livrables types.

CADRE LÉGAL ET ORGANISATIONNEL

Tel qu'il est mentionné dans la description des composants du Modèle, plusieurs des pratiques du processus de PRP sont associées à une disposition légale. Les dispositions légales qui sont traitées de façon particulière dans le Modèle sont les suivantes :

- le chapitre 3 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ;
- les articles 36 et 37 du *Code civil du Québec* ;
- les articles 7, 8 et 15 de la *Loi sur les archives*.

De plus, certaines autres lois d'application générale peuvent avoir une incidence sur la PRP. Par exemple, la *Loi concernant le cadre juridique des technologies de l'information* comporte certaines dispositions sur la PRP et la sécurité dont il y a lieu de tenir compte lors de l'intégration du Modèle dans un organisme public.

Par ailleurs, outre ce type de dispositions légales, d'autres lois auxquelles un organisme public est assujetti comportent des dispositions particulières reliées à la protection des renseignements personnels et qui ont été harmonisées avec la Loi sur l'accès.

Par exemple, le ministère du Revenu du Québec est assujetti à la *Loi sur le ministère du Revenu* et à la *Loi facilitant le paiement des pensions alimentaires*, et les établissements du réseau de la santé sont soumis à la *Loi sur les services de santé et les services sociaux*. Dans certains cas, les lois sectorielles comportent des dispositions particulières qui sont plus restrictives que la Loi sur l'accès. Dans d'autres cas, elles peuvent conférer des pouvoirs particuliers à l'égard de la collecte, l'utilisation ou la communication de renseignements personnels à des tiers.

Les parties prenantes dans le projet veilleront à adapter les pratiques et biens livrables du Modèle pour prendre en compte le cadre législatif et réglementaire de l'organisme public. Il y aura lieu de déterminer si des pratiques du Modèle doivent être ajustées ou si de nouvelles pratiques et biens livrables doivent être ajoutés.

Chaque organisation peut avoir défini des orientations et des politiques en matière de PRP et de développement technologique. De plus, dans un organisme public, les noms des parties prenantes peuvent différer de ceux qui apparaissent dans le Modèle et leurs responsabilités peuvent être réparties différemment. Ainsi, un organisme public pourrait adapter les pratiques et les biens livrables en fonction de sa mission et de ses particularités.

Une adaptation peut aussi être faite selon la taille de l'organisme, ses priorités et les ressources dont il dispose. Par exemple, dans un petit organisme, on pourrait cibler un projet particulier dont les enjeux de PRP sont élevés et déterminer les buts, pratiques et biens livrables considérés prioritaires à réaliser et reporter la mise en œuvre de certaines pratiques de PRP.

CYCLE DE VIE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le cycle de vie de la protection des renseignements personnels proposé dans le Modèle pourrait être réorganisé de manière à grouper un ou plusieurs buts ainsi que les pratiques qui y sont associées. Cela est possible dans la mesure où les buts de PRP sont maintenus.

L'organisme peut fonctionner avec un cycle de vie de la PRP qui diffère de celui proposé dans le Modèle.

Voici trois façons d'adapter le cycle de vie de la PRP :

- Une première façon pourrait consister à ce que l'organisme adapte le cycle de vie de la PRP du Modèle afin de faire une correspondance avec celui qu'il utilise. Dans ce cas, il pourrait fusionner ou fragmenter le cycle de vie proposé dans le Modèle ainsi que les pratiques qui y sont associées.
- Une deuxième façon consiste à maintenir les mêmes buts et pratiques du cycle de vie de la PRP proposé dans le Modèle tout en changeant simplement la séquence et la numérotation des buts.
- Une troisième façon consiste à réorganiser la séquence des pratiques associées à un but. Dans le Modèle, la réalisation des pratiques se fait selon une séquence donnée de telle sorte qu'une pratique donnée dispose des intrants nécessaires à sa réalisation. Il peut arriver que ces intrants correspondent à des biens livrables types provenant de pratiques réalisées antérieurement. C'est pourquoi lors de cette réorganisation, il y a aura lieu de s'assurer de la cohérence de la séquence de réalisation des biens livrables types de chacune des pratiques, car certains des biens livrables types d'une pratique doivent être réalisés avant qu'une autre pratique puisse être enclenchée.

Un organisme pourrait ajouter de nouvelles pratiques en fonction d'un contexte particulier d'offre de services aux citoyens. Par exemple, dans le cadre de grappes de services offerts par plusieurs ministères, des objectifs de transparence accrue visant à renforcer la confiance des citoyens à l'égard des organismes qui dispensent les services pourraient amener les organismes publics à ajouter de nouvelles pratiques au but *BS 8 Diffuser l'information sur la gestion des renseignements personnels*.

NATURE DES PROJETS

Il s'agit d'examiner le Modèle afin de l'adapter à la nature des projets de développement. Les principaux points à considérer par rapport à la nature des projets comprennent :

- taille des projets ;
- recours à un progiciel pour le développement des systèmes d'information ;
- type de système d'information ;
- contexte d'utilisation du système d'information projeté.

PRÉFÉRENCES DE PRATIQUES ET DE BIENS LIVRABLES TYPES

Le Modèle propose un ensemble de pratiques et de biens livrables types. L'organisme public aura à décider s'il les adopte tels quels ou s'il les adapte.

ADAPTATION DE L'ENVIRONNEMENT DE DÉVELOPPEMENT

En plus de l'adaptation au contexte de l'organisme public, il peut être indiqué de procéder à des adaptations de l'environnement méthodologique et, éventuellement, des outils supportant cet environnement. Un projet de développement doit tenir compte de plusieurs exigences. La PRP constitue une exigence particulière devant être prise en compte, car elle fait l'objet d'obligations inscrites dans la Loi sur l'accès. De plus, d'autres lois auxquelles un organisme public est assujetti contiennent également des dispositions de PRP.

Si l'organisme dispose d'un environnement méthodologique normalisé, il peut être indiqué de procéder à son adaptation afin d'intégrer le processus de PRP à cet environnement. Cette intégration vise principalement deux objectifs. En premier lieu, elle permet de s'assurer que la PRP n'est pas considérée comme une exigence exogène au projet, mais bien une exigence qui fait corps avec tous les processus pertinents de développement. En deuxième lieu, elle permet de prendre en compte la PRP dans un projet de la façon la plus économique et efficace possible en profitant de l'environnement normalisé de l'organisme public.

L'adaptation reliée à l'environnement de développement porte sur les éléments suivants :

- cadre stratégique de développement ;
- méthode de développement ;
- méthode de gestion de projet ;
- méthode de gestion des risques ;
- processus de gestion des ententes avec les fournisseurs.

CADRE STRATÉGIQUE DE DÉVELOPPEMENT

Lorsque l'organisme public possède des orientations stratégiques en matière de développement des systèmes d'information, il pourrait décider d'intégrer la PRP à ces orientations. Cette intégration permettrait de s'assurer que toutes les parties prenantes concernées par le développement considèrent les exigences de PRP comme une dimension fondamentale de l'organisme.

MÉTHODE DE DÉVELOPPEMENT

Une méthode de développement comprend un ensemble d'activités et de biens livrables regroupés selon des phases allant de la conception initiale d'un projet jusqu'à l'implantation du système d'information en résultant. Le Modèle comprend des buts, pratiques et biens livrables types (ou produits de travail types) de PRP. Le Modèle n'est pas conçu sur la base d'une approche de développement particulière. Il est indépendant des approches de développement qui peuvent être utilisées par un organisme public et il peut donc s'adapter à chacune d'entre elles.

Les pratiques du Modèle s'appliquent à la plupart des phases de développement, particulièrement celles en amont du développement, telles que la conception préliminaire et l'architecture. Quel que soit le type d'adaptation retenu, celui-ci pourra couvrir la plupart des phases de la méthode de développement en usage dans l'organisme public.

Deux stratégies d'adaptation de la méthode de développement sont possibles :

- La première adaptation pourrait consister à modifier de façon minimale la méthode de développement.

  Il s'agirait d'insérer dans la méthode de développement des « pointeurs » au Modèle afin d'indiquer aux membres d'une équipe de développement le moment où ils ont à tenir compte de la PRP en précisant de se référer au Modèle pour réaliser les pratiques de PRP pertinentes à la phase en cours.

- La deuxième adaptation pourrait consister à intégrer complètement le Modèle à la méthode de développement.

  Cela consisterait à intégrer les éléments pertinents du Modèle de sorte que les membres d'une équipe de développement retrouvent toutes les pratiques ou activités et tous les biens livrables et leur explication en un seul document. Cela éviterait aux équipes d'avoir à se « promener » d'un document à un autre.

  De plus, lors de cette intégration, l'organisme pourra constater que la grande majorité des biens livrables types du Modèle peuvent être insérés dans les biens livrables déjà existants d'une méthode de développement.

MÉTHODE DE GESTION DE PROJET

Le *Modèle de pratiques de PRP* décrit des principes et obligations légales de PRP sous la forme de pratiques, lesquelles constituent, pour la plupart des organismes publics, une formalisation de pratiques existantes en matière de PRP. Il est important que ces pratiques soient prises en compte lors de la gestion de projet, que ce soit lors de la planification, du suivi ou du contrôle de projet, afin de s'assurer qu'une attention est accordée aux exigences de PRP et qu'elles font partie des exigences énoncées pour le système d'information en développement.

MÉTHODE DE GESTION DES RISQUES

Une adaptation de la méthode de gestion des risques est indiquée afin de tenir compte du processus de PRP. Il importe de noter que, selon les organismes, la méthode de gestion des risques peut être intégrée à la méthode de gestion de projet. L'adaptation pourrait porter notamment sur les catégories de risques, la liste des risques et les stratégies de mitigation afin de tenir compte explicitement de la PRP.

PROCESSUS DE GESTION DES ENTENTES AVEC LES FOURNISSEURS

Le *Modèle de pratiques de PRP* formalise les pratiques de PRP pouvant être réalisées dans des projets de développement. Il demeure réalisable peu importe qu'il le soit entièrement par une équipe interne, entièrement par un fournisseur ou de façon partagée. Il est possible que le processus de gestion des ententes avec les fournisseurs demande une adaptation afin d'y intégrer des dimensions de PRP, notamment au niveau du choix d'un fournisseur, de l'établissement d'une entente et de sa gestion. Les ententes peuvent comporter par exemple des clauses de confidentialité et de PRP ou prévoir des biens livrables de PRP que doit réaliser le fournisseur.

D'autres processus ou méthodes peuvent être appelés à être adaptés par l'organisme public pour y intégrer le processus de PRP, et ce, selon l'environnement méthodologique en place. Il revient à l'organisme public d'examiner son environnement de développement et de déterminer les parties qui bénéficieraient d'une adaptation.

RÉPARTITION DES RÔLES ET RESPONSABILITÉS À L'ÉGARD DE L'INTÉGRATION

Les documents qui suivent sont proposés pour faciliter la répartition des rôles et responsabilités lors de l'intégration du Modèle dans l'organisme public, ce sont :

- le tableau 1 – *Légende des rôles des parties prenantes dans un projet de développement* qui fournit une description générale des rôles des parties prenantes ;
- le tableau 2 – *Légende des responsabilités des parties prenantes dans un projet de développement* qui fournit une description générale des responsabilités des parties prenantes ;
- le tableau 3 – *Rôles et responsabilités pour l'intégration* qui propose une répartition type des rôles et responsabilités pour réaliser cette intégration.

Il est possible que cette répartition diffère de celle déjà établie ou projetée par un organisme public dans un projet de développement. Il revient donc à chaque organisme d'ajuster cette répartition selon ses particularités.

TABLEAU 1 *Légende des rôles des parties prenantes dans un projet de développement*

DESCRIPTION GÉNÉRALE DES RÔLES DES PARTIES PRENANTES DANS UN PROJET DE DÉVELOPPEMENT	
RÔLE*	**DESCRIPTION GÉNÉRALE**
Haute direction	La haute direction réfère aux personnes travaillant aux échelons supérieurs de la direction d'un organisme public. Elles comprennent : le sous-ministre, les sous-ministres associés et adjoints, le président-directeur général, les vice-présidents chargés des directions fonctionnelles, les directeurs généraux et les directeurs des différents services. La haute direction définit clairement les valeurs organisationnelles et les orientations internes relativement à la PRP dans les projets de développement. Elle les fait partager par l'ensemble de son personnel et les communique à ses partenaires pour s'assurer qu'elles sont respectées. Les orientations données par la haute direction en matière de PRP déterminent en grande partie la perception de l'importance d'assurer le respect des principes et obligations légales de PRP par les autres parties prenantes dans les projets de développement des systèmes d'information d'un organisme public.
Responsable de la PRP (RPRP)	Dans chaque ministère ou organisme, un membre du personnel de direction relevant directement du sous-ministre ou du président de l'organisme est désigné à titre de responsable de la protection des renseignements personnels pour toute l'organisation**. Outre ses responsabilités légales en matière d'accès et de rectification des renseignements personnels, le RPRP agit habituellement comme interlocuteur auprès de la Commission d'accès à l'information et représente l'organisation. Il peut également soutenir et conseiller le personnel d'encadrement et les employés afin que l'ensemble de l'organisation respecte les principes et obligations légales de PRP, et ce, notamment dans les projets de développement des systèmes d'information. Il peut arriver que, dans des organismes publics de grande taille, l'on désigne une personne spécifiquement à titre de représentante de la PRP pour tous les projets de développement. Cette personne aura alors une responsabilité à l'échelle de l'organisation à l'égard de tous les projets de développement qui ont recours à des renseignements personnels.
Le responsable de la sécurité de l'information numérique (RSIN)	Le RSIN est désigné par les sous-ministres ou les dirigeants des ministères et organismes pour assurer la gestion et la coordination de la sécurité et les représenter en cette matière dans l'organisation. Il a notamment la responsabilité de : • soutenir le sous-ministre ou le dirigeant d'organisme dans la détermination des orientations stratégiques et des priorités d'intervention en matière de sécurité ; • s'assurer de la prise en compte des orientations et exigences en matière de sécurité lors de la conception, de la réalisation ou de la modification des processus d'affaires, des systèmes d'information et des infrastructures technologiques et de donner un avis de pertinence aux gestionnaires et aux détenteurs concernés. Dans un projet de développement, il intervient notamment en ce qui concerne les mesures de sécurité à mettre en place pour respecter les principes et les obligations légales de PRP, et ce, tout au long de leur cycle de vie. Dans les autres organismes publics, par exemple ceux du secteur de la santé et des services sociaux, des secteurs scolaire ou municipal, une personne peut également être désignée responsable de la sécurité et jouer un rôle similaire à celui du RSIN.
Conseiller juridique	Le conseiller juridique joue principalement un rôle de soutien et de conseil et il vérifie les aspects légaux. Dans plusieurs organismes publics, le responsable de la PRP est également conseiller juridique.
Vérificateur interne	Le vérificateur interne peut intervenir pendant le processus de développement, que ce soit *a priori* ou *a posteriori*, pour assurer notamment l'application des exigences de PRP dans le projet de développement. Il peut offrir un soutien, conseiller et accompagner les personnes relativement à la démarche d'intégration de la PRP dans les projets et à la prise en compte des risques qui y sont associés. Il procède à un examen et à une évaluation afin de déterminer si les moyens mis en place dans le système d'information fournissent des garanties suffisantes de respect des principes et des obligations légales de PRP. Il pose un diagnostic, détermine les éléments qui doivent être améliorés et propose des pistes d'amélioration et de solution. Il peut également procéder à une vérification plus approfondie ou une vérification de conformité, pour déterminer si telle façon de faire dans le système d'information est conforme aux obligations légales de PRP qui s'appliquent.

* Le rôle réfère à la fonction de la personne.

** *Plan d'action gouvernemental pour la PRP* disponible sur le site Web du MRCI : http://www.aiprp.gouv.qc.ca/protectionpublic/actions/actions.asp?Sect=1

TABLEAU 1 *(Suite)*

DESCRIPTION GÉNÉRALE DES RÔLES DES PARTIES PRENANTES DANS UN PROJET DE DÉVELOPPEMENT	
RÔLE*	**DESCRIPTION GÉNÉRALE**
Responsable des méthodes	Cette personne agit comme le « gardien » des méthodes nécessaires à la réalisation des projets. Ces méthodes peuvent inclure, par exemple, la méthode de gestion de projet, la méthode de développement et la méthode de gestion des risques.
Directeur de projet et comité directeur	Le directeur de projet réfère à un gestionnaire de haut niveau (tel qu'un directeur général), habituellement choisi parmi les clients du projet et qui bénéficie de l'appui d'un comité directeur, qui représente les différents groupes de clients et d'utilisateurs. Il énonce les différentes orientations et exigences en matière notamment de PRP pour le projet et le mode de suivi qu'il entend adopter pour s'assurer que la PRP est prise en compte adéquatement dans le projet.
Chef / chargé de projet	Le chef de projet, qui peut être assisté de chargés de projet pour certains domaines du projet (par exemple chargé de projet pour un des processus d'affaires, chargé de projet pour les aspects administratifs du nouveau système, etc.) a la responsabilité principale de faire en sorte que toutes les activités de développement et de gestion du projet prennent en compte la PRP.
Pilote de projet	Le pilote de projet est une personne qui représente les utilisateurs du futur système d'information. C'est une personne qui connaît bien le processus d'affaires couvert par le système d'information concerné et qui est en mesure de fournir des informations sur les besoins précis des utilisateurs et de valider les biens livrables du processus de PRP du projet.
Répondant de la PRP	À la différence du responsable de la protection des renseignements personnels (RPRP) de l'organisme public ou de la personne qui agit à titre de représentante de la PRP pour tous les projets de développement, les responsabilités et les activités du répondant de la PRP se limitent à un projet de développement particulier. Il est ainsi formellement assigné à la fonction de réalisation du processus de PRP dans un projet. Il a donc le pouvoir de prendre des décisions à cet égard et il répond de cette responsabilité à l'autorité compétente. La fonction de répondant de la PRP pourrait également être assumée par le chargé de projet, par le RPRP ou une personne qu'il désigne, ou toute autre personne qui détient l'autorité et la compétence requises.
Autres membres de l'équipe de développement	Selon la taille et la nature du projet, plusieurs autres personnes contribuent à la réalisation du système d'information. Ces personnes peuvent être des spécialistes de différents domaines. Par exemple : des spécialistes en analyse de processus d'affaires, architecture de système, formation, gestion de projet, gestion des risques, gestion de la sécurité (il peut s'agir du responsable de la sécurité de l'information numérique (RSIN) dans les ministères et organismes ou d'une autre personne désignée à cet effet), gestion documentaire, programmation, documentation et communication, gestion de configuration, en Web et en utilisabilité, gestion du changement, etc. Certains d'entre eux peuvent avoir un rôle important à jouer relativement à la prise en compte de la PRP dans leurs tâches respectives.

* Le rôle réfère à la fonction de la personne.

TABLEAU 2 *Légende des responsabilités des parties prenantes dans un projet de développement*

DESCRIPTION GÉNÉRALE DES RESPONSABILITÉS	
Responsable (Resp.)	Personne qui est imputable des pratiques, sous-pratiques et biens livrables de PRP et qui a le pouvoir de prendre des décisions à cet égard. Elle peut réaliser les activités ou en déléguer une partie ou toutes.
Réalise	Personne qui exécute ou accomplit des pratiques, sous-pratiques et biens livrables de PRP ou autres activités de PRP.
Offre un soutien et conseille (Soutient)	Personne qui assiste la direction et les autres membres de l'équipe de projet dans le domaine de la PRP sans nécessairement assumer la responsabilité de la décision proposée. Cette personne formule des recommandations et des suggestions concernant les matières relevant de sa compétence. Elle est disponible pour donner suite à toute demande liée à la PRP.
Vérifie	Personne qui effectue un examen pour déterminer si tels pratique, sous-pratique ou produit de travail ou autres activités de PRP ont été réalisés selon les « règles de l'art » et les principes et obligations légales de PRP, en fonction des critères et des orientations établis. Afin d'assurer l'objectivité et l'impartialité, la personne qui vérifie ne peut pas réaliser les activités qu'elle a vérifiées.
Coordonne (Coord.)	Personne qui coordonne diverses actions, fonctions ou services associés à la PRP, qui assure la liaison entre ces actions, ces fonctions et ces services.
Approuve	Personne qui a un niveau d'autorité, qui donne son accord à la suite d'une vérification ou d'une validation positive. L'approbation des biens livrables de PRP peut se faire à différents niveaux selon la structure de gestion du projet.

TABLEAU 3 *Rôles et responsabilités pour l'intégration*

ACTIVITÉS	INTÉGRATION DU *MODÈLE DE PRATIQUES DE PRP*									
	HAUTE DIRECTION					MEMBRES DE L'ÉQUIPE DE DÉVELOPPEMENT				
	Haute direction	RPRP	Conseiller juridique	Vérificateur interne	Responsable des méthodes	Directeur de projet	Chef et chargé de projet	Pilote	Répondant de la PRP	Autres membres
Adaptation du Modèle										
Cadre légal et organisationnel	Approuve	**Resp.** Coord. Réalise	Soutient	Vérifie	Réalise	Soutient	Coord.	Soutient	Réalise Soutient	Réalise Soutient*
Cycle de vie de la PRP	Approuve	**Resp.** Vérifie	Soutient	Vérifie	Réalise	Soutient	Coord.		Réalise Soutient	Réalise Soutient
Nature des projets		Vérifie	Soutient	Vérifie	**Resp.** Réalise	Soutient	Coord.	Soutient	Réalise Soutient	
Préférence de pratiques et de biens livrables types		Vérifie	Soutient	Vérifie	**Resp.** Réalise	Soutient	Coord.	Soutient	Réalise Soutient	
Adaptation de l'environnement de développement										
Cadre stratégique de développement	Approuve	Soutient	Soutient	Soutient Vérifie	**Resp.** Réalise	Soutient	Soutient			
Méthode de développement	Approuve	Vérifie		Soutient Vérifie	**Resp.** Réalise		Soutient		Réalise Soutient	
Méthode de gestion de projet	Approuve	Vérifie		Soutient Vérifie	**Resp.** Réalise		Soutient		Réalise Soutient	
Méthode de gestion des risques	Approuve	Vérifie		Soutient Vérifie	**Resp.** Réalise		Soutient		Réalise Soutient	Réalise Soutient**
Processus de gestion des ententes avec les fournisseurs	Approuve	Vérifie	Soutient	Soutient Vérifie	**Resp.** Réalise	Approuve Soutient	Soutient		Réalise Soutient	Réalise Soutient***

* Spécialiste en gestion documentaire, relativement aux pratiques associées à la conservation des renseignements personnels de façon permanente et à leur destruction ; spécialiste de la gestion de la sécurité relativement aux mesures de sécurité à mettre en place pour tout le cycle de vie des renseignements personnels.

** Spécialiste en gestion des risques

*** Spécialiste en approvisionnement ou en contrats

Partie 1 Réaliser la PRP dans les projets de développement

La Partie 1 propose un ensemble de buts et de pratiques spécifiques qu'un organisme public peut réaliser dans un projet particulier ou dans un ensemble de projets de développement. Les buts et pratiques sont dits spécifiques car ils sont propres au domaine de la PRP et ils découlent des principes et obligations légales de PRP auxquels un organisme public est assujetti.

Après avoir effectué un survol rapide du Modèle à l'aide du *Guide de lecture de l'ensemble du Modèle* (page XVII), le mode de lecture de la Partie 1 décrit ci-après permet :

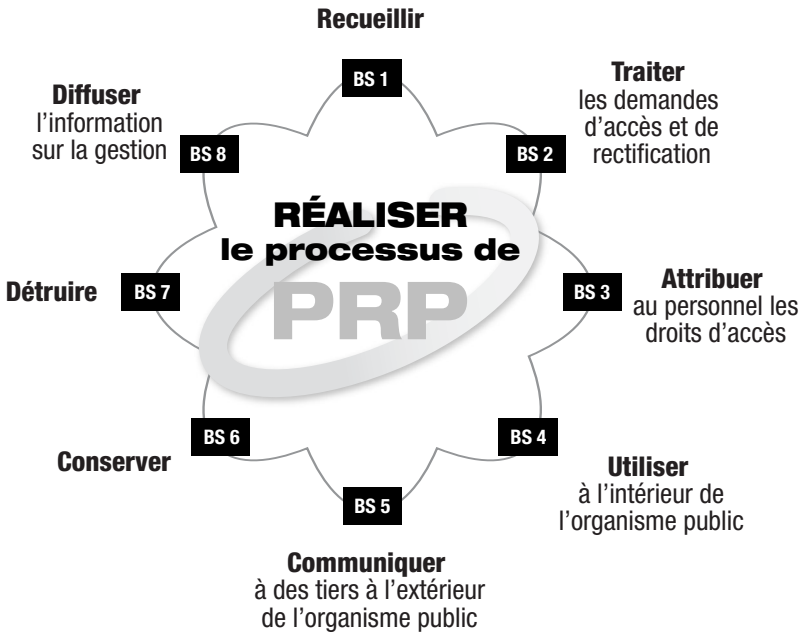
- d'établir la stratégie d'intégration du Modèle dans l'organisme public ou le projet ;
- de prendre connaissance des composants du Modèle qui ont trait à la spécificité même de la PRP ;
- de déterminer les buts et les pratiques spécifiques de PRP à réaliser dans l'organisme ou le projet ;
- de déterminer les rôles et les responsabilités des intervenants ;
- de faire une lecture détaillée des buts et pratiques spécifiques de PRP pour comprendre les pratiques à réaliser et identifier les adaptations à faire selon la stratégie d'intégration retenue.

MODE DE LECTURE SUGGÉRÉ AFIN DE FACILITER LA RÉALISATION DE LA PRP

1. Lire le chapitre : *Comment intégrer le Modèle dans l'organisme public ?* (p. 13 à 22).
2. Lire l'*aide-mémoire n° 1.1 Déterminer les buts spécifiques de PRP à atteindre dans le projet* (p. 195) pour déterminer lesquels doivent être atteints.
3. Consulter le *Schéma de la Partie 1 – Réaliser la PRP dans les projets de développement* (p. 24) pour déterminer les pratiques à examiner en fonction des buts retenus.
4. Lire le chapitre : *Composants du Modèle* – Partie 1 (p. 26 à 31).
5. Lire les pratiques correspondantes et les *aide-mémoire nos 2.1 à 2.8 Déterminer les pratiques spécifiques de PRP à réaliser dans le projet* (p. 31 à 105) : pour déterminer les pratiques à réaliser et, le cas échéant, établir l'adaptation à faire.

SCHÉMA DE LA PARTIE 1

Réaliser la protection des renseignements personnels (PRP) dans les projets de développement



BS 1 Recueillir

PS 1.1 Déterminer tous les renseignements personnels (RP) que l'on projette de gérer dans le système

PS 1.2 Évaluer la nécessité des RP que l'on projette de gérer dans le système

PS 1.3 Déterminer les sources d'obtention des RP

PS 1.4 Informer la Commission d'accès à l'information (CAI) des situations où des RP, déjà colligés par une personne (autre que la personne concernée) ou par une entreprise privée, seront recueillis auprès de celles-ci

PS 1.5 Déterminer les modalités de collecte des RP

PS 1.6 Déterminer les modalités d'information de la personne auprès de qui les RP seront recueillis

BS 2 Traiter les demandes d'accès et de rectification

PS 2.1 Mettre en œuvre les modalités de traitement des demandes d'accès à des RP et de rectification de ceux-ci

BS 3 Attribuer au personnel les droits d'accès

PS 3.1 Déterminer les droits d'accès aux RP

PS 3.2 Concevoir et développer le système de manière à respecter les droits d'accès établis

PS 3.3 Mettre en œuvre des mesures visant à permettre au personnel de l'organisme public l'accès aux RP dans les seuls cas où cela est justifié

PS 3.4 Décrire, dans le formulaire de déclaration de fichiers des RP, les catégories de personnes qui ont accès à des RP

BS 4 Utiliser à l'intérieur de l'organisme public

PS 4.1 Appliquer, dans tous les éléments du système d'information, les règles d'utilisation des RP

PS 4.2 Déterminer et évaluer les utilisations des RP projetées lors de la modification des systèmes existants

PS 4.3 Utiliser, dans la mesure du possible, des renseignements anonymes

PS 4.4 Mettre en œuvre des mesures pour prévenir l'utilisation illicite de RP au sein de l'organisme public

BS 5 Communiquer à des tiers à l'extérieur de l'organisme public

PS 5.1 Déterminer les situations où l'organisme public projette de communiquer des RP à des tiers, à l'extérieur de l'organisme public

PS 5.2 Évaluer les situations où des RP seront communiqués à des tiers, à l'extérieur de l'organisme public

PS 5.3 Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité lorsque des RP sont communiqués à des tiers, à l'extérieur de l'organisme public

PS 5.4 Mettre en œuvre des mesures pour obtenir le consentement des personnes

BS 6 Conserver

PS 6.1 Mettre en œuvre des mesures pour conserver les RP en respectant le calendrier de conservation, et ce, tout au long de leur cycle de vie

PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des RP

BS 7 Détruire

PS 7.1 Mettre en œuvre des mesures de destruction des RP

BS 8 Diffuser l'information sur la gestion

PS 8.1 Constituer et maintenir à jour un inventaire des fichiers de RP créés ou transférés dans le nouveau système ou modifiés dans le système existant et les déclarer à la CAI

PS 8.2 Diffuser l'information sur les modalités de gestion des RP

EXEMPLE DE LECTURE – PARTIE 1

Titre du but spécifique

Énoncé du but spécifique

Références à d'autres pratiques ou d'autres documents

Titre de la pratique spécifique

Obligation légale associée à cette pratique

Explication de la pratique

Résultat concret de la réalisation de la pratique

Parties d'une pratique plus détaillée

Énoncé de la pratique spécifique

Exemple

BS 1 **RECUEILLIR DES RENSEIGNEMENTS PERSONNELS**

Les renseignements personnels sont recueillis en respectant les principes et obligations légales de PRP

Plusieurs principes et dispositions légales de PRP guident un organisme public lorsqu'il recueille des renseignements personnels. Il doit, avant de les recueillir, en évaluer la nécessité (article 64, Loi sur l'accès) ; il tente de les recueillir en premier auprès de la personne concernée et il doit notamment informer la personne des raisons de la collecte et du traitement des informations (article 65, Loi sur l'accès).

Se référer à ce sujet à la pratique spécifique PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système.

PS 1.1 **Déterminer tous les renseignements personnels que l'on projette de gérer dans le système**

Art. 54
Loi sur l'accès

Déterminer, parmi les renseignements que l'on projette de recueillir et consigner dans le système ou produire par celui-ci, ceux qui correspondent à la définition légale de « renseignement personnel ».

Cette pratique est un préalable à la réalisation de l'ensemble des autres pratiques de ce but, BS 1, et de tous les autres buts spécifiques subséquents.

Produit de travail type (bien livrable type)

1. Liste des renseignements personnels que l'organisme public projette de recueillir et consigner dans le système de même que ceux produits par celui-ci (sur support électronique ou autre).

Sous-pratiques

1. Déterminer les renseignements qui sont de nature personnelle.

Pour être identifié comme étant un renseignement de nature personnelle (ou nominatif), c'est-à-dire qui concerne une personne physique et permet de l'identifier (article 54, Loi sur l'accès), un renseignement doit :

- faire connaître quelque chose à quelqu'un ;
- avoir un rapport avec une personne physique ;
- etc.

EXEMPLE

Renseignements personnels :

- l'adresse, le sexe, l'âge, la date de naissance, l'origine ethnique
- le dossier médical, le dossier d'un employé, le dossier fiscal
- etc.

PARTIE 1 RÉALISER LA PRP DANS LES PROJETS DE DÉVELOPPEMENT

COMPOSANTS DU MODÈLE – PARTIE 1

Ce chapitre décrit les définitions et conventions de représentation des différents composants du Modèle. Les composants du *Modèle de pratiques de PRP* de la Partie 1 comprennent des buts spécifiques, des pratiques spécifiques, lesquelles se détaillent par des explications, des produits de travail types (ou biens livrables types) découlant de la réalisation des pratiques, des sous-pratiques qui viennent expliciter une pratique, des définitions et des exemples de pratiques ainsi que des références. Ces composants sont représentés à la figure 4 qui suit :

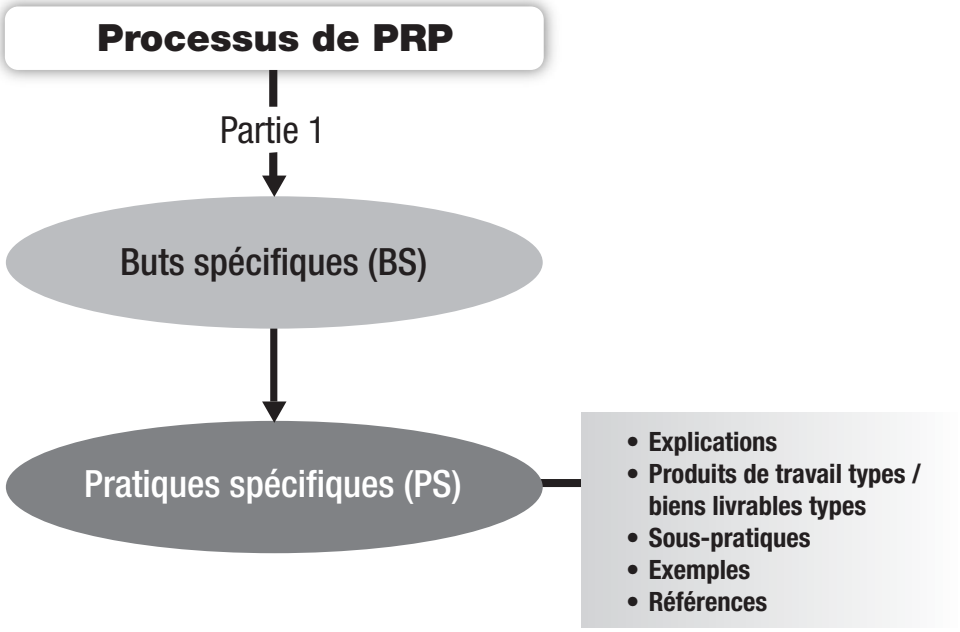


Figure 4 *Composants du processus de PRP – Partie 1 du Modèle*

PROCESSUS DE PRP

Un processus est un ensemble de pratiques regroupées par buts qui, lorsqu'elles sont réalisées, permettent d'atteindre les buts considérés comme étant importants à atteindre pour respecter les principes et obligations légales de PRP.

Dans le contexte de la réalisation de la PRP, le processus de PRP comprend un ensemble de pratiques de PRP regroupées en huit buts correspondant aux huit phases du cycle de vie de la PRP (voir leur illustration au schéma de la Partie 1 apparaissant précédemment). Ces buts et pratiques sont qualifiés de « spécifiques », car dans la Partie 1 du Modèle ils ont trait à la spécificité même de la PRP. Par exemple le but spécifique *BS 1 Recueillir des renseignements personnels* et les pratiques spécifiques qui s'y rattachent portent sur une dimension propre à la PRP et à sa réalisation dans les projets de développement.

BUTS SPÉCIFIQUES

Les buts spécifiques s'appliquent à un seul processus, soit le processus de PRP, et réfèrent aux caractéristiques uniques décrivant ce qui doit être mis en œuvre pour satisfaire aux exigences de celui-ci. La description des buts spécifiques se base sur le cycle de vie de la protection des renseignements personnels tel qu'illustré dans le *Schéma de la Partie 1 – Réaliser la PRP dans les projets de développement* présenté précédemment*.

Dans le contexte du développement des systèmes d'information, les buts et les pratiques qui y sont associées sont proposés aux membres des équipes de développement afin qu'ils tiennent compte de tout le cycle de vie de la PRP qui aura à être supporté dans le futur système d'information.

La façon de décrire les buts spécifiques associés à la PRP peut, à première vue, différer de la façon dont la PRP est prise en compte durant le développement d'un système d'information. En effet, chacun des buts correspond à chacune des phases du cycle de vie de la PRP, alors que pendant le développement d'un système d'information, on se situe juste avant le déclenchement de ce cycle de vie.

Il est apparu essentiel de maintenir la correspondance entre le cycle de vie de la PRP et les buts spécifiques, afin que l'équipe de développement soit en mesure de mieux évaluer tout le travail à réaliser pour que le système à développer respecte les principes et obligations légales de PRP, de même que les pratiques administratives liées à la PRP généralement en place dans les organismes publics.

Afin de faciliter les travaux de l'équipe de développement en matière de PRP, tous les éléments détaillant les buts spécifiques, comme les pratiques et les biens livrables types, tiennent compte que l'on se situe à la phase de développement du système.

Lors d'un projet de développement, les équipes vont réaliser les pratiques pour permettre au système d'information d'atteindre les buts spécifiques de PRP lorsqu'il sera mis en service.

EXEMPLE

Le premier but, qui correspond à la première phase du cycle de vie de la PRP, consiste à recueillir des renseignements personnels. Durant le développement du système d'information, on ne recueille aucun renseignement personnel, mais on prépare le système d'information pour qu'il soit apte à recueillir de tels renseignements tout en respectant les exigences de PRP. C'est pourquoi les pratiques associées à ce but sont des pratiques qui préparent la collecte des renseignements personnels, telles que les pratiques consistant à déterminer les renseignements personnels à recueillir et consigner, évaluer leur nécessité et déterminer les modalités de collecte.

Les buts spécifiques sont présentés de la façon suivante. Tous les titres et énoncés des buts du processus apparaissent en caractères gras dans une fiche. Le numéro du but (par exemple : BS 1 pour le but spécifique 1) apparaît dans un onglet à gauche du titre du but. Les buts spécifiques sont numérotés séquentiellement commençant par BS. L'énoncé du but apparaît en italique gras sous le titre du but. Le titre du but (par exemple *BS 1 Recueillir des renseignements personnels*) est une forme abrégée de l'énoncé du but *BS 1* : *Les renseignements personnels sont recueillis en respectant les principes et les obligations légales de PRP*. Il est utilisé pour se référer plus

* Dans le texte qui suit, les termes « projets de développement » incluent également les projets de modification des systèmes.

facilement au but sans avoir recours à l'énoncé du but qui est plus détaillé. Il n'est en aucune façon utilisé pour déterminer si les pratiques associées et réalisées permettent d'atteindre ce but. Seul l'énoncé du but est conçu à cette fin, car il est plus explicite, détaillé et précis.

PRATIQUES SPÉCIFIQUES

Une pratique spécifique est une activité ou un ensemble d'activités importante(s) pour atteindre le but spécifique associé. Les pratiques spécifiques décrivent les activités devant permettre d'atteindre les buts spécifiques d'un processus. Dans le processus de PRP, il y a vingt-quatre **(24) pratiques spécifiques**. Les pratiques constituent une proposition d'activités à réaliser pour atteindre le but associé à ces pratiques. Ce sont les pratiques spécifiques que l'on retrouve normalement dans un organisme public pour satisfaire un but spécifique.

Étant donné que le Modèle n'est pas une norme, les pratiques spécifiques demeurent des propositions de pratiques. L'organisme public peut réaliser une « pratique équivalente », différente de la pratique proposée, mais qui permet d'atteindre tout de même le but associé à la pratique.

Les pratiques spécifiques sont présentées d'une façon similaire aux buts spécifiques. Tous les titres et énoncés des pratiques spécifiques apparaissent en caractères gras dans une fiche et ils sont décalés du texte à partir de la marge de gauche. Le numéro de la pratique (par exemple : PS 1.1 pour la pratique spécifique 1) apparaît dans un onglet à gauche du titre de la pratique. Chaque pratique spécifique commence par PS, suivi d'un numéro ayant la structure « x.y » où « x » correspond au même chiffre que le but auquel il réfère et « y » correspond au numéro séquentiel de la pratique spécifique associée au but spécifique.

L'énoncé de la pratique apparaît en italique gras dans la fiche sous le titre de la pratique. Le titre de la pratique est une forme abrégée de l'énoncé de la pratique et est utilisé à des fins de référence ; c'est l'énoncé de la pratique qui représente le contenu de la pratique.

EXPLICATIONS

Il y a trois types d'explications dans le Modèle.

Le premier type d'explications comprend les explications qui suivent l'énoncé d'un but ou d'une pratique et qui fournissent des détails de façon à mieux comprendre le but ou la pratique. De la même façon, des explications accompagnent d'autres composants comme les produits de travail types ou les sous-pratiques.

Le deuxième type d'explications comprend des informations complémentaires, des commentaires ou des définitions qui peuvent accompagner différents composants. Ces explications apparaissent dans le document dans la marge de gauche vis-à-vis des composants concernés. Ainsi, lorsqu'un nouveau terme est utilisé dans le Modèle, sa définition peut apparaître lorsque cela est approprié pour la compréhension du lecteur.

Enfin, le troisième type d'explications comprend les notes de bas de page. Ces notes fournissent des informations additionnelles sur des composants. Elles peuvent correspondre par exemple à des références à d'autres documents ou à des sites Web.

PRODUITS DE TRAVAIL TYPES (BIENS LIVRABLES TYPES)

Les produits de travail types ou biens livrables types sont des composants du Modèle qui fournissent des exemples de résultats découlant de la réalisation d'une pratique spécifique. Ces exemples sont qualifiés de « types », car ce sont les produits de travail ou les biens livrables que l'on retrouve normalement associés à cette pratique.

Cependant, en étant qualifiés de « types », cela signifie qu'un organisme peut avoir recours à d'autres produits de travail ou biens livrables tout aussi efficaces pour atteindre un même but, mais non répertoriés ni décrits dans ce document. De plus, un organisme peut considérer qu'il y a d'autres produits de travail ou biens livrables à produire pour réaliser complètement la pratique et, ainsi, atteindre le but associé.

L'énumération des produits de travail types ou des biens livrables types ne se veut donc pas nécessairement exhaustive bien qu'une attention particulière ait été apportée pour que la très grande majorité d'entre eux s'y retrouve.

SOUS-PRATIQUES

Les sous-pratiques sont des descriptions détaillées d'activités qui permettent d'orienter la réalisation des pratiques. Les sous-pratiques peuvent être formulées comme si elles étaient normatives, mais elles sont en fait une proposition d'activités à réaliser et sont destinées uniquement à fournir des pistes de travail ou d'interprétation de la pratique à réaliser. Par exemple, la pratique *PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système* comprend des sous-pratiques décrivant des activités détaillées facilitant sa réalisation. Elles réfèrent à la détermination de l'usage des renseignements, à la réalisation du « test de nécessité » et à l'anonymisation des renseignements personnels.

RÉFÉRENCES

Les références sont des composants du Modèle qui dirigent l'utilisateur vers des informations complémentaires ou plus détaillées dans des processus associés auxquels il peut se référer ou dans tout autre document pertinent. Toutes les références sont clairement indiquées en italique dans le Modèle. Toutes les références à des buts ou à des pratiques du Modèle commencent toujours avec le terme « Se référer à » suivi de l'élément référencé, alors que les références à d'autres documents, à une annexe du Modèle ou à un article de loi peuvent commencer avec différents termes tels que « consultez... » ou « se référer à... ».

Dans la Partie 1 du Modèle, les éléments référencés sont :

- Des buts ou pratiques spécifiques ou sous-pratiques autres que le but ou la pratique spécifique ou la sous-pratique où figure la référence, afin d'indiquer certaines interrelations entre les buts et les pratiques spécifiques. À ce moment, le numéro et le nom du but ou de la pratique spécifique ou de la sous-pratique sont mentionnés. Ainsi, dans l'explication de la pratique spécifique *PS 5.1 Déterminer les situations où l'organisme public projette de communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public*, on retrouve :

  Se référer au but spécifique BS 2 Traiter les demandes d'accès à des renseignements personnels et de rectification *et à la pratique* PS 2.1 Mettre en œuvre les modalités de traitement des demandes d'accès à des renseignements personnels et de rectification de ceux-ci, *en ce qui concerne les situations où les renseignements personnels sont communiqués à la personne concernée*.

- Des documents numériques ou papier, inclus ou non dans le Modèle, venant appuyer une pratique, présenter un exemple d'application de la pratique ou fournir des informations additionnelles. Ainsi, dans l'explication de la pratique spécifique *PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels*, on retrouve :

  Pour réaliser cette pratique, se référer, notamment, à la politique et aux directives de sécurité de l'organisme public, à la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale *du Conseil du trésor*, *et aux autres travaux du Conseil du trésor sur la sécurité, à l'adresse suivante : www.inforoute-gouvernementale.qc*

EXEMPLES

Les exemples constituent des illustrations des autres composants du Modèle. Ils apportent une information complémentaire en présentant un cas ou un détail d'un composant. À l'opposé des autres composants du Modèle, qui portent sur le « quoi faire » pour atteindre les buts spécifiques de PRP, les exemples peuvent porter sur le « comment faire » en présentant une façon de faire.

Les exemples, qui peuvent apparaître dans le Modèle, se retrouvent dans une fiche avec l'indication « exemple » dans un onglet.

COMPOSANTS ASSOCIÉS À UNE OBLIGATION LÉGALE

Certaines des pratiques spécifiques, des produits de travail types et des sous-pratiques ainsi que des explications qui les accompagnent, sont associés à des dispositions légales. Cette association est représentée par un pictogramme situé dans la marge de gauche, vis-à-vis de la pratique concernée. Ce pictogramme contient l'image d'une balance représentant la justice ; cette image est accompagnée des articles des lois associés à la pratique. À titre d'exemple, on retrouve :

Art. 54
Loi sur l'accès

Les dispositions légales suivantes sont considérées spécifiquement dans ce document :

- le chapitre 3 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ;
- les articles 36 et 37 du *Code civil du Québec* ;
- les articles 7, 8 et 15 de la *Loi sur les archives*.

La mention des dispositions légales vise, d'une part, à attirer l'attention des membres de l'équipe de développement sur les dispositions légales associées à ces pratiques, sous-pratiques ou biens livrables et, d'autre part, à indiquer que leur réalisation devrait se faire de façon à respecter l'obligation légale correspondante, et ce, en fonction de la jurisprudence établie.

Par ailleurs, certaines pratiques spécifiques décrites dans ce document ne réfèrent pas à une obligation expressément prévue dans la Loi sur l'accès. Toutefois, il peut s'avérer difficile de réaliser une pratique associée à une obligation légale si, avant le déclenchement de cette pratique, on n'a pas réalisé d'autres pratiques.

Par exemple, la pratique *PS 1.1 Déterminer tous les renseignements personnels que l'on projette de gérer dans le système*, n'est pas associée à une obligation légale. Sa réalisation permettra toutefois de déclencher la pratique *PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système*, qui, elle, est associée à l'article 64 de la Loi sur l'accès.

D'autres dispositions légales sont prises en compte de façon générale dans ce document. Elles sont indiquées afin que, lors de l'intégration du Modèle dans un organisme public, les dispositions particulières de PRP auxquelles il est assujetti soient respectées. De plus, la *Loi concernant le cadre juridique des technologies de l'information* comporte des dispositions particulières de PRP et de sécurité dont il y a lieu de tenir compte dans un projet de développement.

PRATIQUES SPÉCIFIQUES (PS) PAR BUT (BS)

Ce chapitre comprend la description des buts et pratiques spécifiques de PRP ainsi que les produits de travail types (ou biens livrables types). Afin de faciliter l'atteinte de chacun des huit buts spécifiques de PRP, des gabarits ou aide-mémoire complètent la description des pratiques.

BS 1 RECUEILLIR DES RENSEIGNEMENTS PERSONNELS

Les renseignements personnels sont recueillis en respectant les principes et obligations légales de PRP.

Plusieurs principes et dispositions légales de PRP guident un organisme public lorsqu'il recueille des renseignements personnels. Il doit, avant de les recueillir, en évaluer la nécessité (article 64, Loi sur l'accès). Il tente de les recueillir en premier auprès de la personne concernée. Il doit notamment informer la personne des raisons de la collecte et du traitement des informations (article 65). Il doit par ailleurs informer la Commission d'accès à l'information lorsqu'il recueille des renseignements personnels auprès d'une personne ou d'un organisme privé qui les a déjà colligés (article 66).

Un organisme public devrait être en mesure de justifier la nécessité de chacun des renseignements qu'il recueille au sujet d'une personne.

EXEMPLE

Le ministère de l'Emploi, de la Solidarité sociale et de la Famille peut être autorisé à demander à un citoyen des renseignements personnels relativement à sa situation financière, afin d'être en mesure de déterminer l'admissibilité de ce citoyen aux prestations de la sécurité du revenu et les montants auxquels il a droit.

Art. 54
Loi sur l'accès

PS 1.1 Déterminer tous les renseignements personnels que l'on projette de gérer dans le système

Déterminer, parmi les renseignements que l'on projette de recueillir et consigner dans le système ou produire par celui-ci, ceux qui correspondent à la définition légale de « renseignement personnel ».

Cette pratique est un préalable à la réalisation de l'ensemble des autres pratiques de ce but, BS 1, et de tous les autres buts spécifiques subséquents. C'est à partir des résultats de cette pratique, à savoir l'identification des renseignements personnels qui sont projetés être recueillis, consignés ou produits par le système d'information, que la pratique subséquente pourra se déclencher, et ainsi de suite pour les autres pratiques.

Produit de travail type (bien livrable type)

1. Liste des renseignements personnels que l'organisme public projette de recueillir et consigner dans le système de même que ceux produits par celui-ci (sur support électronique ou autre).

Sous-pratiques

1. Déterminer les renseignements qui sont de nature personnelle.

   Pour être identifié comme étant un renseignement de nature personnelle (ou nominatif), c'est-à-dire qui concerne une personne physique et permet de l'identifier (article 54, Loi sur l'accès), un renseignement doit :

   - faire connaître quelque chose à quelqu'un ;
   - avoir un rapport avec une personne physique ;
   - permettre de distinguer une personne par rapport à quelqu'un d'autre et de l'identifier*.

EXEMPLE

Renseignements personnels :

- l'adresse, le sexe, l'âge, la date de naissance, l'origine ethnique ;
- le dossier médical, le dossier d'un employé, le dossier fiscal ;
- des numéros d'identification personnels comme le numéro d'assurance sociale, le numéro de permis de conduire, le numéro d'assurance maladie, le code permanent d'un étudiant ;
- le numéro de carte de crédit (si elle est émise à une personne physique).

* Pour obtenir plus d'information sur la notion de renseignements personnels, consultez les deux documents suivants :

Accès à l'information. Loi annotée, jurisprudence, analyse et commentaires. Raymond Doray et François Charrette. p. III/54-4 à III/54-6. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et Loi sur la protection des renseignements personnels dans le secteur privé*. Textes annotés. Me Lina Desbiens et Me Diane Poitras. p. 269 à 271. Afin d'alléger le texte, ces deux documents seront désignés ci-après « *Loi annotée*, R. Doray et F. Charrette » et « *Loi annotée*, L. Desbiens et D. Poitras ».

Les renseignements concernant les personnes morales telles que des entreprises, des organismes publics ou des syndicats ne sont pas des renseignements personnels, bien qu'ils puissent, dans certains cas, être tenus confidentiels.

EXEMPLE

Un organisme public peut être tenu de préserver la confidentialité des devis techniques ou des renseignements de nature financière qu'une firme d'ingénieurs lui a transmis dans une offre de services.

De plus, la Loi sur l'accès confère à certains renseignements personnels un caractère public.

EXEMPLE

Dans le cas d'un employé d'un organisme public, son traitement (salaire) est un renseignement personnel confidentiel. Toutefois, le titre, la fonction, l'adresse et le numéro de téléphone de son lieu de travail ainsi que sa classification, y compris l'échelle de traitement rattachée à cette classification, sont publics.

Par ailleurs, le traitement (salaire), l'adresse et le numéro de téléphone du lieu de travail d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction ainsi que d'un ministre, d'un sous-ministre, de ses adjoints et de son personnel d'encadrement, sont des renseignements à caractère public (article 57 1° et 2° de la Loi sur l'accès).

Il est important de rappeler que la notion de « renseignement personnel » dans ce document est synonyme de « renseignement nominatif » et qu'elle exclut ainsi les renseignements personnels à caractère public. Afin d'obtenir plus d'information, consultez les rubriques « renseignement personnel » et « communication de renseignements personnels à caractère public », sur le site Web du MRCI : http://www.aiprp.gouv.qc.ca/protectionpublic/prpcest/prpcest.asp?Sect=3#renseignements et http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=5#Li1

Par ailleurs, un renseignement peut, *a priori*, ne pas être perçu comme étant à caractère personnel, mais il peut le devenir selon le contexte dans lequel il est recueilli, utilisé ou diffusé.

EXEMPLE

Dans des situations particulières, bien qu'aucun renseignement d'identité ne soit en cause, il est possible de reconnaître de quelle personne il s'agit ou de l'identifier. Dans de petites municipalités de quelques centaines de citoyens, la publication de renseignements statistiques faisant état qu'une personne est atteinte d'une maladie particulière associée à d'autres caractéristiques telles que le sexe, l'origine ethnique ou le groupe d'âge, peut permettre d'identifier la personne, même si son nom ou son adresse ne sont pas mentionnés.

Il est donc important d'évaluer le caractère personnel ou nominatif des renseignements, non seulement en les analysant de façon individuelle, mais également sous l'angle des groupements de renseignements faits dans le système et des types d'utilisation des renseignements personnels dans un contexte particulier (se référer à la pratique *PS 4.3 Utiliser, dans la mesure du possible, des renseignements anonymes*). Une attention particulière sera accordée, dans les cas de groupements de données, lorsqu'ils contiennent très peu de personnes et que celles-ci peuvent être identifiées.

Art. 64
Loi sur l'accès

PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système

Indiquer les critères à respecter pour évaluer la nécessité des renseignements personnels que l'on projette de recueillir et consigner dans le système ou produire par celui-ci, en fonction des principes et des obligations légales de PRP, réaliser le « test de nécessité » et le documenter.

Partant de l'identification des renseignements de nature personnelle, l'organisme public déterminera ceux qu'il doit nécessairement recueillir et consigner dans le système ou produire par celui-ci. Ainsi, la liste finale des renseignements recueillis et consignés dans le système ou produits sera celle établie après avoir fait le « test de nécessité »* et s'être assuré qu'il n'y a pas lieu de se limiter à des renseignements anonymes.

Un organisme public ne recueille que les renseignements personnels dont il est en mesure de démontrer la nécessité, compte tenu de ses attributions et des programmes dont il a la gestion (article 64, Loi sur l'accès).

Il est très important que les critères retenus pour réaliser le « test de nécessité » soient établis en fonction de l'article 64 de la Loi sur l'accès, des dispositions légales qui encadrent les activités de l'organisme public et de la jurisprudence. Les personnes qui effectueront le « test de nécessité » auront été sensibilisées à cet égard, ce qui devrait permettre d'avoir une bonne connaissance et une compréhension commune des obligations de la Loi sur l'accès.

La règle de nécessité contribue à l'atteinte d'objectifs d'efficience et d'efficacité. En effet, l'absence d'évaluation rigoureuse de la nécessité des renseignements personnels au regard des besoins administratifs peut mener un organisme public à recueillir et consigner des renseignements inutiles dans le système, générant ainsi des coûts supplémentaires non justifiés, sans compter les risques inutiles d'atteinte à la vie privée.

EXEMPLE

Le responsable de la PRP détermine, en collaboration avec le répondant de la PRP dans le projet, les critères à respecter pour réaliser le « test de nécessité ». Une session de formation est présentée aux personnes qui participent à ces activités ainsi qu'une grille d'analyse et de documentation de la nécessité des renseignements. Cette grille porte notamment sur les renseignements saisis et tous les rapports qui seront produits à partir de ces renseignements ainsi que sur leur usage projeté.

Le répondant de la PRP coordonne les activités et réalise le « test de nécessité » en collaboration avec d'autres membres de l'équipe de développement. Le responsable de la PRP de l'organisme vérifie le résultat des travaux réalisés et émet son avis sur des problématiques particulières soulevées quant à la nécessité de tels renseignements. Le cas échéant, il informe la direction du projet des situations qui soulèvent des risques particuliers de PRP et qui ont un impact sur le système en développement, ainsi que les solutions alternatives proposées par l'équipe de développement pour réduire ces risques.

* Pour obtenir plus d'information sur les critères à prendre en compte relativement à l'interprétation du terme « nécessaire », consultez *Société de transport de la Ville de Laval c* .X., J. E. 2003-597 (C.Q), disponible sur le site de la Société québécoise d'information juridique http://www.jugements.qc.ca/php/resultat.php?s=lc&recher=3_200302, sous la rubrique Laval (Société de transport de la Ville de) c .X, 2003-02-21.

Produits de travail types (biens livrables types)

1. Liste des renseignements personnels à recueillir et consigner dans le système ou à produire par celui-ci, description de l'usage auquel ils sont destinés et justification de leur nécessité.
2. Liste des renseignements rattachés à des personnes physiques, à recueillir et consigner sous forme anonyme dans le système.
3. Mesures techniques et administratives pour rendre les renseignements anonymes lorsque cela est requis.

Sous-pratiques

1. Déterminer et documenter l'usage projeté des renseignements personnels qui seront gérés dans le système.

   Les finalités ou l'usage projeté de chaque renseignement personnel que l'on projette recueillir et consigner dans le système et produire dans celui-ci sont clairement identifiés. Ils peuvent l'être par processus ou sous-processus d'affaires.

   Il est à noter que les renseignements personnels peuvent provenir d'un système existant qui sera vraisemblablement remplacé par le nouveau système en développement. L'usage projeté de ces renseignements personnels a aussi à être documenté pour le nouveau système. Dans ce cas, les renseignements personnels gérés dans le système devant être remplacé ou mis au rancart pourront être détruits conformément au but spécifique *BS 7 Détruire des renseignements personnels*, dans la mesure où « l'objet pour lequel ils ont été recueillis est accompli, et sous réserve de la *Loi sur les archives* » (article 73, Loi sur l'accès).

   Cette sous-pratique n° 1 est un préalable à l'évaluation de la nécessité de chacun des renseignements personnels.

   Se référer à la sous-pratique n° 2 décrite ci-après.

   L'usage projeté des renseignements personnels est également identifié lorsque l'organisme public projette utiliser ou traiter le renseignement personnel à une fin différente de celle prévue initialement (se référer au but spécifique *BS 4 Utiliser des renseignements personnels à l'intérieur de l'organisme public* et à la pratique *PS 4.2 Déterminer et évaluer les utilisations des renseignements personnels projetées lors de la modification des systèmes existants)*.

2. Déterminer, pour chaque renseignement personnel, s'il est nécessaire à l'exercice des attributions de l'organisme public ou à la mise en œuvre d'un programme dont il a la gestion. Cette activité est désignée comme étant la réalisation du « test de nécessité ».

   Pour ce faire, on référera aux dispositions légales, mandats, fonctions ou attributions de l'organisme public, aux programmes et services qui justifient et autorisent la collecte des renseignements personnels. Dans certains cas, un avis de la personne responsable de la PRP ou un avis légal peut être requis.

   Le « test de nécessité » permet de déterminer les renseignements personnels qui sont nécessaires à l'exercice des attributions de l'organisme public ou à la mise en œuvre d'un programme dont il a la gestion et ceux qui peuvent être recueillis et consignés sous forme anonyme (article 64, Loi sur l'accès).

Une attention particulière sera portée à l'évaluation, le cas échéant, de la nécessité de recueillir et de consigner des renseignements de nature sensible tels que des numéros d'identification personnels, comme le numéro d'assurance sociale, le numéro de permis de conduire ou le numéro d'assurance maladie.

Se référer à la pratique PS 1.1 Déterminer tous les renseignements personnels que l'on projette de gérer dans le système *et sa sous-pratique n° 2*.

Afin de déterminer les critères à considérer et de vous guider lors de l'évaluation de la nécessité des renseignements personnels, consultez la rubrique Les principes et les règles à respecter, sur le site du MRCI :
http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=2

3. Déterminer des mesures techniques et administratives pour recueillir et consigner des renseignements de façon anonyme.

   Cette sous-pratique s'applique pour les renseignements qui concernent des personnes, mais qui n'ont pas à être recueillis de manière à permettre de les reconnaître ou de les identifier.

EXEMPLE

Un chercheur qui contacte des personnes dans le cadre d'un sondage effectué pour un organisme public utilisera un questionnaire comprenant une partie détachable s'assurant ainsi que les renseignements liés au sondage ne soient pas associés à une personne en particulier, mais bien recueillis sous forme anonyme.

PS 1.3 Déterminer les sources d'obtention des renseignements personnels

Déterminer et documenter la provenance des renseignements personnels.

Cette pratique vise à déterminer les différentes sources auprès desquelles les renseignements seront recueillis et ainsi à être en mesure de préciser les principes et obligations légales de PRP qui s'appliquent. L'organisme public privilégie, lorsque cela est réalisable, la collecte des renseignements personnels auprès de la personne concernée.

Produit de travail type (bien livrable type)

1. Liste des sources auprès desquelles des renseignements personnels seront recueillis :
   - la personne concernée ;
   - une entreprise privée ou une personne (autre que la personne concernée) avec indication de la nécessité des renseignements, leur usage projeté et les mesures de sécurité ;
   - un autre organisme public.

Sous-pratiques

1. Déterminer les situations où les renseignements personnels peuvent être recueillis auprès de la personne concernée.

2. Déterminer les situations où des renseignements personnels, déjà colligés par une personne (autre que la personne concernée) ou d'une entreprise privée, seront obtenus auprès de ceux-ci, et déterminer la nécessité des renseignements, leur usage projeté et les mesures de sécurité.

   Il s'agit notamment de la collecte de renseignements personnels qui ont déjà été colligés par une entreprise privée ou une personne autre que la personne concernée. Ces renseignements peuvent concerner une ou plusieurs personnes. Dans certains cas, lorsque l'organisme public recueille des renseignements personnels auprès d'une personne ou d'une entreprise privée, il peut également fournir à celles-ci des renseignements d'identité.

EXEMPLE

Un organisme public recueille des renseignements personnels de crédit auprès d'une agence de crédit ou de recouvrement afin de tenter de recouvrer des sommes dues auprès de la personne concernée. L'organisme public transmettra à l'agence des renseignements d'identité pour lui permettre de retracer la personne dans ses fichiers.

Il y aura donc lieu de préserver le caractère confidentiel des renseignements recueillis et communiqués à l'entreprise privée et à la personne autre que la personne concernée.

Se référer à ce sujet aux pratiques PS 5.3 Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité lorsque des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public *et* PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels.

L'organisme public doit par ailleurs informer la CAI avant de recueillir les renseignements personnels. *Se référer à la pratique* PS 1.4 Informer la Commission d'accès à l'information (CAI) des situations où des renseignements personnels, déjà colligés par une personne (autre que la personne concernée) ou par une entreprise privée, seront recueillis auprès de celles-ci.

Pour déterminer au préalable la nécessité des renseignements personnels recueillis, *se référer à la pratique* PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système.

3. Déterminer les situations où des renseignements personnels seront obtenus auprès d'un autre organisme public.

EXEMPLE

Le ministère de l'Emploi, de la Solidarité sociale et de la Famille recueille, auprès d'autres organismes publics (Régie des rentes, CSST ou autres), le montant de prestations accordé afin de le prendre en compte lorsqu'il établit le montant auquel le prestataire de la sécurité du revenu a droit.

L'organisme public qui recueille des renseignements personnels auprès d'un autre organisme public doit être en mesure de démontrer la nécessité de ces renseignements.

Se référer à ce sujet à la pratique PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système.

Les organismes publics qui s'échangent des renseignements personnels doivent également s'assurer qu'ils respectent les principes et obligations légales de PRP.

Se référer au but spécifique BS 5 Communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public *et à la pratique* PS 5.1 Déterminer les situations où l'organisme public projette de communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public.

PS 1.4 Informer la Commission d'accès à l'information (CAI) des situations où des renseignements personnels, déjà colligés par une personne (autre que la personne concernée) ou par une entreprise privée, seront recueillis auprès de celles-ci

Art. 66 Loi sur l'accès

Déterminer, documenter et mettre en œuvre les mesures nécessaires pour informer la CAI avant de recueillir, auprès d'une personne (autre que la personne concernée) ou d'une entreprise privée, des renseignements personnels qu'elle a déjà recueillis, et informer la CAI.

L'article 66 de la Loi sur l'accès prévoit que l'organisme public doit informer la CAI avant de recueillir des renseignements personnels déjà colligés par une personne (autre que la personne concernée) ou une entreprise privée.

Cette pratique vise à s'assurer que la CAI sera informée, au préalable, de toute cueillette de renseignements personnels provenant de fichiers de renseignements personnels détenus par les entreprises privées ou des personnes. La CAI pourrait notamment évaluer la nécessité pour l'organisme public de recueillir tous les renseignements prévus et recommander de prendre des mesures de sécurité appropriées.

La réalisation de cette pratique peut soulever des questions particulières et, à cet égard, il est important de consulter le responsable de la PRP ou un conseiller juridique.

Produit de travail type (bien livrable type)

1. Document d'information à l'intention de la CAI décrivant les renseignements personnels à recueillir auprès d'une personne (autre que la personne concernée) ou d'une entreprise privée, leur usage, leur nécessité et les mesures de protection et de sécurité.

PS 1.5 Déterminer les modalités de collecte des renseignements personnels

Art. 36, 37 Code civil du Québec

Déterminer, en fonction des principes et des obligations légales de PRP et de respect de la vie privée, les modalités de collecte des renseignements personnels.

Il s'agit de déterminer au préalable de quelle façon les renseignements personnels seront recueillis et d'évaluer, en collaboration avec la personne responsable de la PRP ou les services juridiques, s'il s'agit de moyens autorisés par la loi.

Un organisme public qui recueille des renseignements personnels doit le faire en utilisant des moyens licites et en ne contrevenant pas à la loi, notamment les lois citées précédemment dans les notes d'introduction.

Ainsi, un organisme public qui recueille des renseignements personnels doit, notamment, ne pas porter atteinte à la réputation et à la vie privée d'une personne, sans que celle-ci ou ses héritiers y consentent ou que la loi l'autorise. Voici des types d'actes qui peuvent être considérés, selon l'article 36 du *Code civil du Québec*, comme des atteintes à la vie privée d'une personne :

1° pénétrer chez elle ou y prendre quoi que ce soit ;

2° intercepter ou utiliser volontairement une communication privée ;

3° capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés ;

4° surveiller sa vie privée par quelque moyen que ce soit ;

5° utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public ;

6° utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.

Un organisme public ne peut, de plus, porter atteinte à la réputation et à la vie privée d'une personne dans la constitution et l'utilisation d'un dossier sur une personne (article 37 du *Code civil du Québec*).

Se référer aux pratiques du but spécifique BS 4 Utiliser des renseignements personnels à l'intérieur de l'organisme public.

Produit de travail type (bien livrable type)

1. Description des modalités de collecte des renseignements personnels.

Sous-pratiques

1. Déterminer les documents (sous forme papier, électronique ou autres) à produire pour recueillir les renseignements personnels et les modalités entourant la collecte au moyen de ces documents.

   L'organisme public, pour pouvoir procéder à la collecte de renseignements personnels, détermine les documents que le système d'information produira (sous forme papier, électronique ou autres) et les mesures appropriées, et, lorsque cela est réalisable, il privilégie la collecte des renseignements personnels auprès de la personne concernée.

   Il y aura lieu de s'assurer que les renseignements personnels contenus dans ces documents administratifs ont été pris en compte lors du « test de nécessité » (*se référer à la pratique* PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système) et de la détermination des modalités d'information des personnes (*se référer à la pratique* PS 1.6 Déterminer les modalités d'information de la personne auprès de qui les renseignements personnels seront recueillis).

2. Déterminer si le système permettra de recueillir des renseignements personnels par des moyens électroniques indirects.

   Il y aura lieu de déterminer si les moyens indirects risquent de porter atteinte à la vie privée des personnes concernées et satisfont aux principes et obligations légales de PRP.

EXEMPLE

- La collecte d'un renseignement personnel auprès d'un tiers par des moyens électroniques indirects et à l'insu de la personne concernée (utilisation de « témoins » habituellement appelés « cookies ») ;
- l'utilisation de « témoins » pour suivre et enregistrer les différentes transactions en ligne qu'effectue une personne auprès des ministères et organismes gouvernementaux peut, dans certains cas, constituer une intrusion injustifiée dans sa vie privée.

PS 1.6 Déterminer les modalités d'information de la personne auprès de qui les renseignements personnels seront recueillis

Art. 65 Loi sur l'accès

Déterminer les modalités d'information de la personne auprès de qui les renseignements personnels seront recueillis, en fonction des principes et des obligations légales de PRP.

L'article 65 de la Loi sur l'accès prévoit que les personnes, auprès de qui les renseignements personnels sont recueillis, sont informées, préalablement à leur cueillette, des éléments suivants :

1° le nom et l'adresse de l'organisme public au nom de qui la collecte est faite ;

2° l'usage auquel ces renseignements sont destinés ;

3° les catégories de personnes qui auront accès à ces renseignements ;

4° le caractère obligatoire ou facultatif des renseignements ;

5° les conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande de renseignements ;

6° les droits d'accès et de rectification prévus par la loi.

Il est important de noter que la personne auprès de qui les renseignements personnels sont recueillis peut être la personne concernée ou un tiers.

Produit de travail type associé à une obligation légale :

Lorsqu'un article de la loi est rapporté dans la description d'un produit de travail type, cela indique que ce produit de travail type est prévu dans une disposition légale expresse et que sa réalisation se fera de manière à la respecter.

Produit de travail type (bien livrable type)

1. Document décrivant les modalités d'information des personnes auprès de qui les renseignements personnels seront recueillis, comprenant les éléments suivants (article 65, Loi sur l'accès) :

   1° le nom et l'adresse de l'organisme public au nom de qui la collecte est faite ;

   2° l'usage auquel ce renseignement est destiné ;

   3° les catégories de personnes qui auront accès à ces renseignements ;

   4° le caractère obligatoire ou facultatif des renseignements personnels ;

   5° les conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande de renseignements personnels ;

   6° les droits d'accès et de rectification prévus par la loi.

   Se référer à la pratique PS 2.1 Mettre en œuvre les modalités de traitement des demandes d'accès à des renseignements personnels et de rectification de ceux-ci.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 2.1

DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques spécifiques de PRP qui seront réalisées dans le projet pour atteindre le but spécifique BS 1 (colonne « À faire »)
- déterminer les dispositions légales qui y sont associées (colonne « Article de loi »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts/coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe G – Produits de travail types (biens livrables types) des buts spécifiques
- annexe F – Pratiques spécifiques, sous-pratiques et dispositions légales
- tableau 1 – Légende des rôles des parties prenantes dans un projet de développement
- tableau 2 – Légende des responsabilités des parties prenantes dans un projet de développement

LÉGENDE DES SYMBOLES À UTILISER

ARTICLE DE LOI : insérer le numéro de l'article et le titre de la loi associés à cette pratique

---

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N/A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres		Membres de l'équipe de développement	
Responsable de la PRP de l'organisme	RPRP	Directeur de projet	DP
Conseiller juridique	CJ	Chef et chargé de projet	CP
Vérificateur interne	VI	Pilote de projet	PP
Responsable de la sécurité de l'information	RS	Répondant du processus de PRP dans le projet	RPPP
Responsable des méthodes	RM	Autres membres	A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable	R	Valide	Va
Réalise	Ré	Approuve	A
Offre un soutien et conseille	SC	Coordonne	C
Vérifie	Vé		

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié	P	Réalisé	Ré
En cours de réalisation	ER	Approuvé	A
En suspens	ES		

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 1 – RÉALISER LA PRP	BS 1	RECUEILLIR DES RENSEIGNEMENTS PERSONNELS

AIDE-MÉMOIRE nº 2.1 DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	Nº	Article de loi	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
								Début	Fin	Prévus	Réels
Déterminer tous les renseignements personnels (RP) que l'on projette de gérer dans le système	PS 1.1										
Évaluer la nécessité des RP que l'on projette de gérer dans le système	PS 1.2										
Déterminer les sources d'obtention des RP	PS 1.3										
Informer la Commission d'accès à l'information (CAI) des situations où des RP, déjà colligés par une personne (autre que la personne concernée) ou par une entreprise privée, seront recueillis auprès de celles-ci	PS 1.4										
Déterminer les modalités de collecte des RP	PS 1.5										
Déterminer les modalités d'information de la personne auprès de qui les RP seront recueillis	PS 1.6										

BS 2 TRAITER LES DEMANDES D'ACCÈS À DES RENSEIGNEMENTS PERSONNELS ET DE RECTIFICATION

L'organisme public traite les demandes d'accès à des renseignements personnels consignés dans le système d'information et de rectification de ceux-ci, en respectant les principes et les obligations légales de PRP.

La Loi sur l'accès prévoit que toute personne a le droit d'être informée de l'existence d'un renseignement personnel la concernant. Elle a un droit d'accès aux renseignements personnels que détiennent les organismes publics à son sujet et un droit de rectification de ceux-ci.

Le droit de rectification peut se traduire de deux façons :

1. La personne concernée peut demander de modifier ou d'ajouter un renseignement personnel s'il est « inexact, incomplet ou équivoque ».
2. La personne concernée peut demander la destruction d'un renseignement personnel si « sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi »*.

   Se référer à la pratique PS 7.1 Mettre en œuvre des mesures de destruction des renseignements personnels.

L'article 94 de la Loi sur l'accès prévoit qu'« *[…] une demande de communication ou de rectification ne peut être considérée que si elle est faite par écrit par une personne physique justifiant de son identité à titre de personne concernée, à titre de représentant, d'héritier ou de successeur de cette dernière, d'administrateur de la succession, de bénéficiaire d'assurance vie ou comme titulaire de l'autorité parentale. Elle est adressée au responsable de la protection des renseignements personnels au sein de l'organisme public […]* ».

L'organisme public doit notamment aider les personnes à préciser leurs demandes, répondre dans les délais prescrits par la loi et justifier tout refus d'accès à l'ensemble ou à une partie des renseignements personnels demandés ainsi que tout refus d'une demande de rectification (articles 96 à 98 et 100, Loi sur l'accès). Il doit rendre sa décision par écrit et informer les personnes de leur droit de recours auprès de la CAI et des délais qui s'appliquent (article 101, Loi sur l'accès).

Pour obtenir plus d'information sur le traitement des demandes ainsi que sur les obligations légales imposées aux organismes publics à cet égard, cliquez sur la rubrique « Demandes d'accès et de rectification » sur le site Web du MRCI :
http://www.aiprp.gouv.qc.ca/protectionpublic/demande/demande.asp

La pratique qui suit s'appuie sur des processus existants à l'intérieur de l'organisme public pour recevoir les demandes d'accès aux renseignements personnels et de rectification de ceux-ci. Elle réfère ainsi à des politiques ou des directives déjà établies et à des responsabilités qui incombent légalement à la personne responsable de la PRP.

Cette pratique est présentée dans ce document afin notamment que les principales règles de la Loi sur l'accès à cet égard, ainsi que les processus administratifs déjà établis et qui ont une incidence sur le système d'information en développement, soient pris en compte et respectés.

---

* *Loi annotée*, L. Desbiens et D. Poitras, p. 342.

Il y aura donc lieu de déterminer, en collaboration avec le responsable de la PRP de l'organisme public, à quelle étendue et de quelle façon les obligations légales ou autres reliées au traitement des demandes d'accès et de rectification seront intégrées dans le nouveau système d'information.

De plus, il y aura lieu de déterminer si le processus déjà en place au sein de l'organisme public pour traiter les demandes d'accès et de rectification doit être adapté pour qu'il soit prêt à recevoir et traiter de telles demandes relatives aux renseignements personnels consignés dans ce nouveau système.

Dans le cas de demandes d'accès faites par une personne autre que la personne concernée ou que celles décrites précédemment selon l'article 94 de la Loi sur l'accès, se référer au but spécifique *BS 5 Communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public*.

PS 2.1 Mettre en œuvre les modalités de traitement des demandes d'accès à des renseignements personnels et de rectification de ceux-ci

Art. 53, 83 à 102.1 Loi sur l'accès

Élaborer, documenter et mettre en œuvre des mesures pour permettre, à la personne concernée, l'exercice de son droit de consulter et d'obtenir une copie des renseignements qui la concernent ainsi que de demander à ce qu'ils soient rectifiés, en respectant les principes et les obligations légales de PRP.

Les obligations de la Loi sur l'accès relativement au traitement des demandes d'accès à des renseignements personnels s'appliquent, peu importe la personne qui fait une telle demande (personne concernée ou autre).

Cette pratique met toutefois l'accent sur le traitement des demandes d'accès et de rectification faites par la personne concernée. Il s'agit notamment de préparer le système d'information en développement pour supporter ce type de demande, et ce, en fonction des orientations de l'organisme public à cet égard et des obligations légales.

Produit de travail type (bien livrable type)

1. Liste des mécanismes mis en place pour :

   - traiter les demandes d'accès à des renseignements personnels et de rectification de ceux-ci en respectant les obligations légales de PRP, notamment les délais prescrits par la loi ainsi que ceux énoncés dans la « Déclaration de services aux citoyens » à cet égard ;
   - vérifier l'identité de la personne concernée avant de lui communiquer les renseignements demandés ;
   - préserver le caractère confidentiel des renseignements communiqués.

     Se référer à ce sujet aux pratiques PS 5.3 Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité, lorsque des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public *et* PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels.

Sous-pratiques

1. **Déterminer les différentes modalités par lesquelles la personne concernée peut exercer son droit d'accès et de rectification auprès de l'organisme public.**

   La personne concernée a le droit de prendre connaissance des renseignements la concernant pendant les heures habituelles de travail ou à distance et d'en obtenir une copie, sous réserve des restrictions qui s'appliquent. Les renseignements personnels informatisés doivent lui être communiqués sous la forme d'une transcription écrite et intelligible (article 84, Loi sur l'accès).

EXEMPLE

La personne pourrait transmettre sa demande écrite à l'organisme public par courrier ou courriel. Elle pourrait aussi utiliser un formulaire produit par l'organisme ; toutefois, cela ne pourrait être obligatoire.

2. **Déterminer les mesures à prendre pour répondre aux demandes d'accès et de rectification en respectant les obligations légales de PRP.**

   Cette sous-pratique peut s'appliquer pour le traitement des demandes d'accès à des renseignements personnels effectuées par la personne concernée ou par un tiers. Toutefois, elle ne s'applique qu'à la personne concernée relativement à la rectification des renseignements personnels (article 94, Loi sur l'accès).

   La Loi sur l'accès permet à un organisme public d'invoquer certaines restrictions à l'accès (articles 86 à 88.1) et à la rectification (89.1). Elle prévoit un délai de vingt (20) jours pour répondre aux demandes d'accès et de rectification avec une possibilité de prolongation de dix (10) jours supplémentaires si cela est justifié. Il s'agit de délais maximums ; un organisme public pourrait décider de traiter certains types de demandes plus rapidement.

EXEMPLE

Un organisme public pourrait permettre à la personne concernée d'avoir un accès en ligne à certains de ses renseignements personnels.

L'organisme public peut informer sa clientèle des délais prévus dans sa « Déclaration de services aux citoyens » ou sur son site Web ou celui du système concerné. *Se référer à cet effet à la pratique spécifique* PS 8.2 Diffuser l'information sur les modalités de gestion des renseignements personnels.

   L'organisme public met en place un mécanisme de suivi afin de respecter les délais établis ainsi que les autres dispositions légales relatives au traitement des demandes, notamment l'accusé de réception, l'avis de prolongation du délai si cela est requis, la lettre de réponse et l'information sur les droits de recours de la personne concernée. Une personne peut consulter gratuitement les renseignements personnels qu'un organisme détient à son sujet. Toutefois, des frais n'excédant pas le coût de la transcription, de la reproduction et de la transmission du renseignement personnel peuvent être exigés du requérant.

Ces frais ainsi que les modalités de paiement sont prescrits par le *Règlement sur les frais exigibles pour la transcription, la reproduction et la transmission de documents et de renseignements nominatifs*. Il est à noter qu'un organisme a la discrétion d'exiger des frais. S'il décide d'en exiger, ces frais ne pourront excéder ceux prévus à ce règlement (article 85). Consultez à ce sujet la rubrique Demande d'accès, frais exigibles, sur le site Web du MRCI :
http://www.aiprp.gouv.qc.ca/protectionpublic/demande/demande.asp?Sect=4

3. **Déterminer les mesures à prendre pour s'assurer de l'identité de la personne qui adresse une demande d'accès ou de rectification (article 94, Loi sur l'accès).**

   Les mesures de contrôle de l'identité différeront en fonction de la manière dont les demandes sont adressées à l'organisme public.

EXEMPLE

Une personne se présente sur place pour consulter son dossier et l'organisme exige qu'elle présente une pièce d'identité lui permettant de constater « *de visu* » son identité. Toutefois, il ne consignera pas les renseignements inscrits sur la pièce d'identité.

4. **Déterminer, en ce qui concerne la rectification des renseignements, le processus à mettre en place pour que le système permette de consigner qu'il y a contestation de la teneur des renseignements par la personne concernée et, lorsque la personne le demande, pour enregistrer la demande de rectification (article 91, Loi sur l'accès).**

   Cette sous-pratique s'applique uniquement dans le cas où l'organisme public refuserait, en partie ou totalement, d'accéder à une demande de rectification.

EXEMPLE

À la suite d'un incident survenu en cours d'emploi, un organisme public fait enquête sur la situation et produit un rapport qu'il verse au dossier d'employé de la personne concernée. Celle-ci conteste l'opinion de l'organisme public et lui demande de la corriger de même que la conclusion inscrite au dossier. L'organisme rejette la demande de rectification et la CAI confirme qu'il est en droit de le faire. L'organisme versera au dossier de la personne, une copie des commentaires qu'elle lui a transmis et de sa version des faits.

5. **Déterminer la modalité de livraison, sans frais, à la personne concernée, d'une copie de tout renseignement personnel modifié ou ajouté ou, selon le cas, une attestation du retrait d'un renseignement personnel (article 92, Loi sur l'accès).**

   Cette sous-pratique s'applique lorsque la demande de rectification est acceptée tout en respectant les règles de sécurité associées à toute communication de renseignements personnels. *Se référer à la pratique spécifique* PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels.

6. **Déterminer la modalité pour faire suivre, à la demande de la personne concernée, une copie du renseignement rectifié ou de l'annotation au dossier à l'organisme de qui il a obtenu le renseignement ou à tout organisme à qui le renseignement a pu être communiqué, dans le cadre d'une entente conclue suivant la Loi sur l'accès (article 93, Loi sur l'accès).**

   Cette sous-pratique s'applique lorsque la demande de rectification est acceptée.

7. **Déterminer les modalités pour communiquer des renseignements personnels de manière sécuritaire afin, notamment, d'en préserver l'intégrité et la confidentialité.**

   L'article 53 consacre le caractère confidentiel des renseignements personnels.

   Se référer à la pratique spécifique PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels.

EXEMPLE

L'organisme public transmet des renseignements personnels par courrier recommandé. S'ils sont transmis par voie électronique, des technologies de cryptage seront prévues.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 2.2

DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques spécifiques de PRP qui seront réalisées dans le projet pour atteindre le but spécifique BS 2 (colonne « À faire »)
- déterminer les dispositions légales qui y sont associées (colonne « Article de loi »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts/coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe G – Produits de travail types (biens livrables types) des buts spécifiques
- annexe F – Pratiques spécifiques, sous-pratiques et dispositions légales
- tableau 1 – Légende des rôles des parties prenantes dans un projet de développement
- tableau 2 – Légende des responsabilités des parties prenantes dans un projet de développement

LÉGENDE DES SYMBOLES À UTILISER

ARTICLE DE LOI : insérer le numéro de l'article et le titre de la loi associés à cette pratique

---

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N/A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable de la sécurité de l'information . . . . . .RS
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Pilote de projet . . . . . .PP
Répondant du processus de PRP dans le projet . . . .RPPP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié . . . . . .P
En cours de réalisation . . . . . .ER
En suspens . . . . . .ES
Réalisé . . . . . .Ré
Approuvé . . . . . .A

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 1 – RÉALISER LA PRP	BS 2	TRAITER LES DEMANDES D'ACCÈS À DES RENSEIGNEMENTS PERSONNELS ET DE RECTIFICATION

AIDE-MÉMOIRE nº 2.2 DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	Nº	Article de loi	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
								Début	Fin	Prévus	Réels
Mettre en œuvre les modalités de traitement des demandes d'accès à des renseignements personnels et de rectification de ceux-ci	PS 2.1										

BS 3 ATTRIBUER AU PERSONNEL, LES DROITS D'ACCÈS AUX RENSEIGNEMENTS PERSONNELS

La protection des renseignements personnels est réalisée, en respectant les principes et les obligations légales de PRP, lorsque les droits d'accès aux renseignements personnels sont accordés au personnel de l'organisme public.

Une fois qu'un organisme public a recueilli des renseignements personnels, le principe fondamental de confidentialité l'oblige à limiter la circulation de ces renseignements et à en restreindre l'accès. Les pratiques qui suivent ne visent que l'accès aux renseignements personnels par les membres du personnel d'un organisme public.

Ce principe s'applique toutefois à toute personne ayant accès aux renseignements personnels détenus par celui-ci. *Se référer à ce sujet aux pratiques du but* BS 5 Communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public.

L'appréciation de la nécessité pour une personne qui œuvre au sein d'un organisme public de prendre connaissance d'un renseignement personnel s'effectue en considérant les fonctions et les tâches de cette personne, le contexte propre à chaque situation, l'utilisation qui sera faite du renseignement et les buts visés.

EXEMPLE

Dans le cadre de la gestion des dossiers du personnel, des agents de la paie auront accès en mode consultation, modification et impression aux renseignements concernant la rémunération, incluant le numéro de compte de l'institution financière, afin de produire la paie et faire le dépôt direct au compte de la personne.

Seules les personnes qui ont réellement besoin des renseignements personnels, dans le cadre de leurs fonctions, tâches et activités quotidiennes, devraient y avoir accès, et ce, lorsqu'elles en ont besoin seulement.

Avant de permettre l'accès au personnel à des renseignements personnels, un organisme public aura à évaluer si les conditions suivantes sont satisfaites (article 62, Loi sur l'accès) :

- les personnes qui ont accès à des renseignements personnels sans le consentement des personnes concernées « ont qualité » (ou sont « autorisées, qualifiées ou habilitées »*) pour en prendre connaissance, et les renseignements personnels auxquels elles ont accès sont « nécessaires à l'exercice de leurs fonctions » ou à la réalisation de leurs mandats respectifs ;
- les personnes désignées pour avoir accès aux renseignements personnels appartiennent à l'une des « catégories de personnes » inscrites à la déclaration de fichiers de l'organisme, déclaration produite à la pratique *PS 8.1 Constituer et maintenir à jour un inventaire des fichiers de renseignements personnels créés ou transférés dans le nouveau système ou modifiés dans le système existant et les déclarer à la Commission d'accès à l'information (CAI)*.

* Le Petit Robert définit l'expression « avoir qualité » : « être habilité, être autorisé, qualifié ». *Loi annotée*, R. Doray et F. Charrette, p. III/62-4

Pour obtenir plus d'information concernant les principes et les règles à respecter en matière d'accès aux renseignements personnels par le personnel, consultez le site Web du MRCI :
http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=3

Consultez également : *Loi annotée*, R. Doray et F. Charrette. p. III/62-1 à III/62-6 et *Loi annotée*, L. Desbiens et D. Poitras, p. 290 à 293.

PS 3.1 Déterminer les droits d'accès aux renseignements personnels

Indiquer, documenter et appliquer les critères permettant de déterminer les personnes, parmi le personnel de l'organisme public, qui ont qualité (ou sont « autorisées, qualifiées ou habilitées ») à prendre connaissance des renseignements personnels et les renseignements personnels qui sont nécessaires à la réalisation de leurs tâches, et ce, en fonction des principes et des obligations légales de PRP.

Art. 62 Loi sur l'accès

Droit d'accès du personnel :

Autorisation du personnel de l'organisme à prendre connaissance des renseignements personnels en fonction des obligations légales de PRP. Dans un contexte informatique, on réfère souvent aux droits et aux privilèges d'accès de l'utilisateur.

Profil d'accès :

Description des catégories de personnes qui ont accès aux renseignements personnels, aux programmes de traitement, à la configuration de production et aux rapports produits par le système, sous forme électronique ou autres, de leurs privilèges d'accès (lecture, modification, copie, destruction, impression ou autres). Cette description est faite en fonction des processus d'affaires et des unités administratives concernées.

Il est très important que les critères retenus pour déterminer les droits d'accès soient indiqués et documentés en fonction de l'article 62 de la Loi sur l'accès, des dispositions légales qui encadrent les activités de l'organisme public et de la jurisprudence.

Les personnes qui détermineront les droits d'accès auront été sensibilisées à cet égard, ce qui devrait permettre d'avoir une bonne connaissance et une compréhension commune des obligations de la Loi sur l'accès à cet effet. Le responsable de la PRP de l'organisme public et le répondant de la PRP dans le projet seront associés à ces activités afin, notamment, de conseiller les membres de l'équipe de projet et de valider les critères établis.

L'évaluation portera sur chacun des renseignements personnels, et non de façon globale pour l'ensemble d'un système, d'un sous-système, d'un rapport ou autres. Il importe donc que l'attribution des droits d'accès soit effectuée en considérant les fonctions de chaque personne, ses responsabilités et ses tâches.

Les résultats de cette évaluation pourront être utilisés afin que l'architecture du système puisse en tenir compte. C'est pourquoi la pratique spécifique *PS 3.2 Concevoir et développer le système de manière à respecter les droits d'accès établis* est intimement liée à cette pratique.

Le *Guide d'évaluation des profils d'accès aux fichiers de renseignements personnels dans les organismes publics*, produit par le MRCI, bien que conçu en fonction des systèmes d'information qui sont déjà en place au sein d'un organisme public, est un outil de référence*. Il décrit les critères à considérer et propose une démarche d'évaluation des profils d'accès.

* Pour en obtenir une copie, s'adresser à : webmestre.aiprp@mrci.gouv.qc.ca

Produits de travail types (biens livrables types)

1. Liste des critères à respecter pour établir les droits d'accès.
2. Description des catégories de personnes qui ont accès aux renseignements personnels, aux programmes de traitement, à la configuration de production et aux rapports produits par le système, sous forme électronique ou autres, ainsi que de leurs privilèges d'accès (lecture, modification, copie, destruction, impression ou autres). Cette description est faite en fonction des processus d'affaires et des unités administratives (profils d'accès).

Sous-pratiques

1. Indiquer et documenter les critères à respecter pour déterminer quelles sont les personnes qui « ont qualité » (« sont autorisées, qualifiées ou habilitées ») pour prendre connaissance des renseignements personnels et les renseignements personnels nécessaires à la réalisation de leurs tâches.
2. Déterminer les droits d'accès aux renseignements personnels, aux programmes de traitement, à la configuration de production et aux rapports produits par le système (sous forme électronique ou autres), en fonction des éléments suivants :
   - les processus d'affaires et les unités administratives concernées ;
   - les catégories de personnes et les profils de tâches et de responsabilités des personnes qui auront accès aux renseignements personnels consignés dans le système ;
   - la nécessité d'avoir accès aux renseignements personnels, aux programmes de traitements et aux rapports en fonction des critères établis ;
   - les privilèges d'accès : lecture, modification, copie, destruction, impression ou autres, pour chaque renseignement personnel.

   Cette activité sert à établir les profils d'accès et elle est réalisée de manière à couvrir tous les renseignements personnels accessibles au personnel de l'organisme public, notamment les gestionnaires, le personnel professionnel, technique et de soutien, de développement informatique, les administrateurs du système et autres.

EXEMPLE

La CAI énonce, dans le cas des dossiers médicaux que : « *Le personnel de développement informatique ne doit pas avoir accès aux données sociosanitaires nominatives réelles et aux systèmes de production. En fait, le personnel de développement informatique ne doit avoir accès aux données sociosanitaires réelles que si elles sont anonymisées. Quant au personnel de support informatique, il a accès aux systèmes de production si c'est nécessaire (en cas de panne, par exemple)* ». Elle recommande également que : [...] « *l'équipe de projet utilise des données fictives ou anonymisées lorsque les personnes font des présentations ou donnent de la formation ou pour faire des tests* ». Consultez à ce sujet les *Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la Santé et des Services sociaux*, disponibles sur le site Web de la CAI : www.cai.gouv.qc.ca/fra/docu/exigence.pdf

Bien que la CAI ne fasse référence qu'au personnel de développement, nous comprenons qu'elle inclut également le personnel dédié à la modification du système. La PRP sera assurée tant en ce qui concerne la partie administrative, telle que la manipulation des formulaires papier, que la partie informatique d'un système d'information.

PS 3.2 Concevoir et développer le système de manière à respecter les droits d'accès établis

Les différents éléments du système tels que les sous-systèmes, les programmes, les bases de données, les transactions sous forme électronique ou autres, sont développés selon les droits d'accès établis, en respectant les principes et les obligations légales de PRP.

La réalisation de cette pratique constitue une dimension importante au niveau de l'architecture du système. Elle peut générer des économies substantielles si l'on considère les coûts qui résulteraient de la modification de l'architecture d'un système existant pour se conformer à la Loi sur l'accès. Il est donc important que, dès l'élaboration de l'architecture d'un nouveau système ou avant l'achat d'un progiciel, les exigences de PRP relatives aux droits d'accès soient prises en considération.

Cette pratique vise à ce que le système soit conçu de manière à limiter l'accès du personnel aux seuls renseignements personnels nécessaires pour réaliser ses tâches. Il est donc très important qu'il y ait une correspondance entre les droits d'accès, déterminés en fonction des principes et des obligations légales de PRP et les renseignements personnels accessibles. Cette correspondance permet de contenir les risques et les coûts de la protection des renseignements personnels.

EXEMPLE

Une conception et une réalisation qui tiennent compte des profils d'accès peuvent faire en sorte que la base de données est segmentée de façon à ce qu'il soit facile et rapide d'afficher uniquement les renseignements personnels auxquels une personne a droit d'accès selon son profil d'accès. Cela permet d'éviter notamment d'afficher tout le contenu d'une base de données à une personne qui n'a besoin que d'une petite partie de cette base.

Produits de travail types (biens livrables types)

1. Table de référence croisée entre les différents types de profils d'accès et les différents éléments du système tels que les sous-systèmes, les programmes et les transactions sous forme électronique ou autres.
2. Architecture du système compatible avec les exigences de PRP, notamment des droits d'accès.

PS 3.3 Mettre en œuvre des mesures visant à permettre au personnel de l'organisme public l'accès aux renseignements personnels dans les seuls cas où cela est justifié

Art. 62
Loi sur l'accès

Élaborer, documenter et mettre en œuvre des mesures pour que les membres du personnel de l'organisme public prennent connaissance des renseignements personnels uniquement dans le cadre de l'exercice de leurs fonctions et lorsque cela est nécessaire pour les accomplir adéquatement.

Un des éléments importants à considérer est la sensibilisation des personnes qui ont accès aux renseignements personnels, aux conséquences possibles de consulter ou d'utiliser des renseignements personnels pour des motifs non justifiés. Cela pourrait être intégré, notamment dans le plan de formation prévu lors du déploiement du système.

Produits de travail types (biens livrables types)

1. Programme de sensibilisation concernant l'accès aux renseignements personnels et destiné à être diffusé aux membres du personnel.
2. Liste des mesures administratives et techniques, établies *a priori*, afin de prévenir des accès non autorisés par les membres du personnel.
3. Liste des mesures administratives et techniques, établies *a posteriori,* afin de contrôler des accès non autorisés par les membres du personnel.

Sous-pratiques

1. Élaborer et diffuser un programme de sensibilisation aux membres du personnel.

EXEMPLE

Ce programme de sensibilisation pourrait être diffusé lors du déploiement du système d'information. Il pourrait être intégré dans le processus de gestion du changement.

2. Déterminer des mesures administratives et techniques afin de prévenir et de contrôler des accès non autorisés par les membres du personnel.

   Ces mesures peuvent viser un contrôle des accès *a priori* ou *a posteriori*.

EXEMPLE

A priori

- des mesures administratives sont établies pour que les droits d'accès, en fonction des profils d'accès, soient autorisés par une personne en position d'autorité avant que ces droits soient activés dans le système ;
- les employés peuvent signer un formulaire d'engagement à la confidentialité ;
- des sessions de sensiblisation sont offertes aux employés (utilisation de mot de passe, écran de veille, etc.).

A posteriori

La journalisation des accès permet notamment de repérer un employé qui aurait pris connaissance de renseignements personnels sans raison et pour des motifs non professionnels. La CAI recommande, dans le cas des dossiers médicaux, de journaliser les accès en indiquant les éléments permettant de connaître :

- le code d'identification de l'utilisateur ;
- le nom du fichier auquel il a eu accès ;
- le numéro du dossier concerné ;
- l'accès en cause (création, lecture, modification, destruction d'un dossier) ;
- le code de transaction ou le nom du programme (indiquer le plus précis des deux) ;
- la date (année, mois, jour) de l'accès ;
- l'heure (heure, minute, seconde) de l'accès.

Consultez à ce sujet les *Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la Santé et des Services sociaux*, disponibles sur le site Web de la CAI : www.cai.gouv.qc.ca/fra/docu/exigence.pdf

Il est suggéré d'effectuer une analyse périodique et continue des données enregistrées concernant des accès et des transactions réalisées dans le système (journalisation). L'analyse des données de journalisation peut être manuelle ou partiellement automatisée et en temps réel afin de détecter automatiquement les anomalies d'accès. Des mesures de vérification comme une vérification aléatoire des accès à un renseignement personnel par une personne ou un groupe de personnes pourraient également être réalisées.

EXEMPLE

Si un employé consulte le dossier d'un client ou d'un bénéficiaire de services à un moment qui ne correspond à aucun événement prévu au cycle de traitement régulier du dossier, cela indique une éventuelle irrégularité qui nécessiterait une investigation plus approfondie.

D'autres analyses des données de journalisation devraient être également réalisées de façon ponctuelle.

Dans le cas des systèmes disponibles sur le Web, il est de plus en plus courant, dans les pratiques réalisées lors du développement des systèmes, de procéder à des « tests d'intrusion » pour déterminer s'il est possible d'accéder de façon illicite à des renseignements personnels dans le système d'information, et ce, tant en ce qui a trait à la partie informatique qu'à la partie administrative de celui-ci. De tels tests sont réalisés autant avant la mise en production que durant l'exploitation et l'utilisation, mais aussi à la suite d'une modification du système.

Cette pratique se complètera par les pratiques de sécurité du système et de l'ensemble de l'organisme public.

PS 3.4 Décrire, dans le formulaire de déclaration de fichiers des renseignements personnels, les catégories de personnes qui ont accès à des renseignements personnels

Art. 62 et 76 4° Loi sur l'accès

La description des catégories de personnes qui ont accès aux renseignements personnels du système dans l'exercice de leurs fonctions apparaît dans le formulaire de déclaration de fichiers de l'organisme public, en respectant les obligations légales de PRP.

Formulaire de déclaration de fichiers de renseignements personnels :

Formulaire produit par la CAI afin de permettre aux organismes publics de lui déclarer ses fichiers et de produire un répertoire de ceux-ci accessible au public.

Cette pratique a une portée plus grande que la pratique *PS 1.5 Déterminer les modalités de collecte des renseignements personnels*, car elle vise à porter à la connaissance de l'ensemble des citoyens les catégories de membres du personnel d'un organisme public qui ont accès aux renseignements personnels, par le biais des déclarations de fichiers qu'un organisme public doit produire à la CAI.

Catégories de personnes :

Les personnes qui ont accès aux renseignements et qui sont identifiées, non pas par leur nom, mais selon l'unité administrative à laquelle elles appartiennent, et leur corps d'emploi, titre de fonction ou leur rôle ou responsabilités.

La description des catégories de personnes qui ont accès aux renseignements personnels du système est réalisée pour chacun des fichiers créés dans le nouveau système ou modifiés dans le système existant.

Produit de travail type (bien livrable type)

1. Description des catégories de personnes qui ont accès aux renseignements personnels dans l'exercice de leurs fonctions, dans les formulaires de déclaration de fichiers.

Sous-pratique

1. Informer la personne responsable de la PRP des catégories de personnes qui ont accès aux renseignements personnels du système.

   L'organisme public a la responsabilité de mettre à jour les formulaires de déclaration de fichiers et de les transmettre à la CAI. *Se référer à cet effet à la pratique* PS 8.1 Constituer et maintenir à jour un inventaire des fichiers de renseignements personnels créés ou transférés dans le nouveau système ou modifiés dans le système existant et les déclarer à la Commission d'accès à l'information (CAI).

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 2.3

DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques spécifiques de PRP qui seront réalisées dans le projet pour atteindre le but spécifique BS 3 (colonne « À faire »)
- déterminer les dispositions légales qui y sont associées (colonne « Article de loi »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts/coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe G – Produits de travail types (biens livrables types) des buts spécifiques
- annexe F – Pratiques spécifiques, sous-pratiques et dispositions légales
- tableau 1 – Légende des rôles des parties prenantes dans un projet de développement
- tableau 2 – Légende des responsabilités des parties prenantes dans un projet de développement

LÉGENDE DES SYMBOLES À UTILISER

ARTICLE DE LOI : insérer le numéro de l'article et le titre de la loi associés à cette pratique

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

À FAIRE : indique si la pratique sera réalisée (O, N, N/A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres		Membres de l'équipe de développement	
Responsable de la PRP de l'organisme	RPRP	Directeur de projet	DP
Conseiller juridique	CJ	Chef et chargé de projet	CP
Vérificateur interne	VI	Pilote de projet	PP
Responsable de la sécurité de l'information	RS	Répondant du processus de PRP dans le projet	RPPP
Responsable des méthodes	RM	Autres membres	A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable	R	Valide	Va
Réalise	Ré	Approuve	A
Offre un soutien et conseille	SC	Coordonne	C
Vérifie	Vé		

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié	P	Réalisé	Ré
En cours de réalisation	ER	Approuvé	A
En suspens	ES		

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

EFFORTS/COÛTS : exprimés en jours-personnes ou en $

PARTIE 1 – RÉALISER LA PRP	BS 3	ATTRIBUER AU PERSONNEL, LES DROITS D'ACCÈS AUX RENSEIGNEMENTS PERSONNELS

AIDE-MÉMOIRE nº 2.3 DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	Nº	Article de loi	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
								Début	Fin	Prévus	Réels
Déterminer les droits d'accès aux renseignements personnels	PS 3.1										
Concevoir et développer le système de manière à respecter les droits d'accès établis	PS 3.2										
Mettre en œuvre des mesures visant à permettre au personnel de l'organisme public l'accès aux renseignements personnels dans les seuls cas où cela est justifié	PS 3.3										
Décrire, dans le formulaire de déclaration de fichiers des renseignements personnels, les catégories de personnes qui ont accès à des renseignements personnels	PS 3.4										

BS 4 UTILISER DES RENSEIGNEMENTS PERSONNELS À L'INTÉRIEUR DE L'ORGANISME PUBLIC

La protection des renseignements personnels est réalisée lors de leur utilisation par le personnel de l'organisme public, en respectant les principes et les obligations légales de PRP.

Les pratiques décrites dans cette section visent l'utilisation des renseignements personnels par l'organisme public qui les a en sa possession.

L'Organisation de coopération et de développement économiques (OCDE), le *Code civil du Québec* et la jurisprudence associée à la Loi sur l'accès orientent les pratiques de ce but.

L'OCDE a énoncé en 1980 deux principes reliés à ce but dans son document *Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières des données de caractère personnel**. Le principe de la spécification des finalités et celui de la limitation de l'utilisation des renseignements personnels prévoient :

« Principe de la spécification des finalités

9. Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.

Principe de la limitation de l'utilisation

10. Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au paragraphe 9, si ce n'est :

    a) avec le consentement de la personne concernée ; ou

    b) lorsqu'une règle de droit le permet ».

Le *Code civil du Québec* énonce par ailleurs que toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. Elle ne peut utiliser des données à caractère personnel à des fins incompatibles avec celles de sa constitution ; elle ne peut non plus, dans la constitution ou l'utilisation du dossier, porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation (article 37).

Les pratiques décrites dans cette section sont énoncées en se fondant sur les principes et règles mentionnés précédemment et sur des décisions de la Commission d'accès à l'information relativement à l'application de l'article 65, paragraphe 2 et des articles 72, 73 et 76 de la Loi sur l'accès**.

---

* Consultez à ce sujet le site de l'OCDE : www1.oecd.org/publications/e-book/9302012e.pdf

** Pour plus d'information sur la portée de ces articles au regard du principe de respect des finalités initiales prévues lors de la collecte des renseignements personnels (ou de la limitation de leur utilisation), consultez le document : *Loi annotée*, R. Doray et F. Charrette, p. III/65-5 à 65-7.

Les auteurs, M[e] Doray et M[e] Charrette, mentionnent par ailleurs « *Cependant, force est de reconnaître qu'aucune de ces dispositions n'interdit formellement à un organisme public d'utiliser un renseignement nominatif à une fin autre que celle pour laquelle il a été obtenu ou à une fin autre que celle déclarée lors de sa collecte, par l'application de l'article 65* »*. Il est donc important de consulter un conseiller juridique pour s'assurer de réaliser la bonne pratique selon le contexte particulier du projet.

Les pratiques décrites dans cette section visent, d'une part, à faire en sorte que l'utilisation des renseignements personnels consignés dans le système d'information en développement soit limitée à ce qui est nécessaire. Elles visent, d'autre part, dans le contexte de l'entretien ou de l'évolution d'un système existant, à ce que le principe de respect des finalités initiales d'un renseignement (ou de limitation de leur utilisation), qui est un élément important de la protection des renseignements personnels, soit mis en application.

Il importe de rappeler l'importance de se référer au répondant de la PRP dans le projet ou au responsable de la PRP de l'organisme public afin de déterminer la portée des pratiques *PS 4.2 Déterminer et évaluer les utilisations des renseignements personnels projetées lors de la modification des systèmes existants* et *PS 4.3 Utiliser, dans la mesure du possible, des renseignements anonymes*.

Art. 37
Code civil du Québec
Art. 65 2°, 72, 73 et 76 5°
Loi sur l'accès

PS 4.1 Appliquer, dans tous les éléments du système d'information, les règles d'utilisation des renseignements personnels

Appliquer les règles d'utilisation des renseignements personnels convenues, et qui respectent les principes et obligations légales de PRP, dans chacun des éléments du système d'information et des différentes actions associées à ce système.

Le système d'information est développé ou modifié en fonction :

- des règles d'accès aux renseignements personnels, définies dans le but spécifique *BS 3 Attribuer au personnel, les droits d'accès aux renseignements personnels* ;
- des utilisations prévues lors de la collecte, au but spécifique *BS 1 Recueillir des renseignements personnels* ; et
- de l'information des personnes concernées par ces utilisations par la réalisation de la pratique *PS 1.6 Déterminer les modalités d'information de la personne auprès de qui les renseignements personnels seront recueillis*.

Le système d'information est ainsi développé ou modifié de telle sorte qu'il facilite la mise en œuvre de ces pratiques par les différents intervenants qui auront à interagir avec le futur système. Chacun des éléments (transactions, rapports, base de données, etc.) du système est développé ou modifié de façon à intégrer les exigences de PRP convenues. De même, les particularités d'utilisation des renseignements personnels en matière de statistique et sondage sont définies et incorporées au système d'information.

* Consultez à ce sujet le site de l'OCDE : www1.oecd.org/publications/e-book/9302012E.PDF

Enfin, lors de la réalisation du but spécifique *BS 8 Diffuser l'information sur la gestion des renseignements personnels*, la façon dont les renseignements personnels seront utilisés fera partie de l'information diffusée.

Produits de travail types (biens livrables types)

1. Éléments du système d'information développés selon les règles d'utilisation des renseignements personnels établies pour ce système.
2. Liste des conditions particulières à satisfaire par l'organisme public dans le cas d'utilisations des renseignements personnels à des fins d'étude, de recherche et statistique ou de sondage.

Sous-pratiques

1. Déterminer les règles d'utilisation des renseignements personnels pour ce système.

   Les règles d'utilisation sont déterminées de manière à respecter les utilisations prévues des renseignements personnels lors de leur collecte.

   Se référer à la pratique PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système *et la* sous-pratique n° 1 Déterminer et documenter l'usage projeté des renseignements personnels qui seront gérés dans le système.

2. Déterminer les éléments du système d'information qui devront être développés selon les règles d'utilisation des renseignements personnels établies pour ce système.
3. Déterminer et documenter les conditions particulières à satisfaire pour l'utilisation des renseignements personnels à des fins d'étude, de recherche et de statistique ou de sondage, et les réaliser.

   Cette sous-pratique porte uniquement sur l'utilisation des renseignements personnels à l'intérieur de l'organisme public. Lors de la réalisation des sondages par un organisme public ou dans le cadre d'un mandat confié à un tiers pour le compte de cet organisme, il est important de respecter les conditions fixées par la CAI. Consultez à ce sujet les *Exigences minimales relatives à la protection des renseignements personnels lors de sondages réalisés par un organisme public ou son mandataire et l'Aide-mémoire* sur le site Web de la CAI : www.cai.gouv.qc.ca/fra/docu/sondages.pdf et www.cai.gouv.qc.ca/fra/docu/sondag-2.pdf

   Se référer à ce sujet à la pratique PS 5.1 Déterminer les situations où l'organisme public projette de communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public.

   Par ailleurs, les cas où des renseignements personnels sont communiqués, à des fins d'étude, de recherche et de statistique, à une personne œuvrant à l'extérieur de cet organisme, nécessitent une autorisation préalable de la CAI (article 125, Loi sur l'accès).

Art. 37
Code civil du Québec
Art. 53, 65 2°, 72, 73 et 76 5°
Loi sur l'accès

PS 4.2 Déterminer et évaluer les utilisations des renseignements personnels projetées lors de la modification des systèmes existants

Déterminer les utilisations des renseignements personnels projetées dans le cadre des modifications des systèmes existants, indiquer et documenter les critères à respecter pour les évaluer et réaliser cette évaluation en fonction des principes et des obligations légales de PRP.

Cette pratique est réalisée dans le contexte de la modification d'un système existant. Elle est réalisée uniquement dans les cas où des renseignements personnels sont en jeu et lorsque l'utilisation des renseignements personnels vise l'une ou l'autre des finalités suivantes :

- une finalité qui n'avait pas été prévue initialement lors de leur collecte ;
- une finalité non pertinente ou non compatible avec la finalité première ;
- une finalité qu'une personne raisonnable considérerait non appropriée ou non justifiée, compte tenu des circonstances.

Les finalités premières, prévues lors de la collecte des renseignements personnels, servent de point de référence afin de déterminer si les utilisations projetées des renseignements personnels sont compatibles ou pertinentes par rapport aux finalités prévues initialement, et donc acceptables pour l'organisme public.

Se référer à la pratique PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système *et la* sous-pratique n° 1 Déterminer et documenter l'usage projeté des renseignements personnels qui seront gérés dans le système *pour connaître la finalité première des renseignements personnels*.

Dans le cas où l'une ou l'autre des conditions énumérées précédemment est remplie, l'organisme public évalue si le consentement de la personne concernée peut (ou devrait) être obtenu et, dans la négative, il déterminera les mesures à prendre pour informer la personne concernée de ce type d'utilisation des renseignements personnels.

Produits de travail types (biens livrables types)

1. Liste des types d'utilisations et documentation de leur justification (légale et administrative).
2. Lorsque cela est requis, formulaire de consentement pour les renseignements personnels pour lesquels une nouvelle utilisation est projetée et description des modalités selon lesquelles il sera obtenu auprès de la personne concernée.
3. Documentation, au besoin, des raisons justifiant pourquoi le consentement des personnes à la nouvelle utilisation des renseignements personnels ne sera pas obtenu.
4. Mesures d'information, au besoin, auprès des personnes concernées par la nouvelle utilisation de renseignements personnels sans leur consentement.

Sous-pratiques

1. Déterminer les finalités visées par l'utilisation des renseignements personnels dans le contexte des changements apportés au système d'information.
2. Indiquer et documenter les critères d'évaluation des types d'utilisations des renseignements personnels ainsi que le seuil d'acceptation de ces utilisations.

   Les critères retenus dans le cadre du projet pour faire cette évaluation sont établis en fonction des principes de PRP et des obligations de la Loi sur l'accès, de l'article 37 du *Code civil du Québec*, des autres dispositions légales qui encadrent les activités d'un organisme public et, enfin, de la jurisprudence.

EXEMPLE

Un traitement des renseignements personnels, qui établirait un profil détaillé d'une personne à son insu et à des fins non légitimes, peut poser des risques particuliers d'atteinte à la PRP. L'organisme public portera une attention particulière aux programmes de traitement qui permettent de prendre des décisions concernant des personnes de façon automatisée. Il évaluera s'il y a lieu d'informer les personnes concernées et de recueillir leurs commentaires avant que la décision soit prise.

   Une attention particulière sera accordée aux situations où l'on projette d'utiliser les identifiants pour relier différentes banques de données ou pour effectuer des transactions électroniques automatiques.

3. Déterminer :

   - les mandats, les attributions, les programmes et les dispositions légales pertinentes qui autorisent ce type d'utilisation des renseignements personnels ;
   - si le consentement des personnes à ce type d'utilisation des renseignements personnels peut (ou devrait) être obtenu.

   Dans le cas où l'option du consentement ne serait pas retenue, l'organisme public documente les raisons le justifiant, notamment les dispositions légales qui l'autorisent à procéder de telle sorte. Il évaluera, le cas échéant, s'il y a lieu d'informer les personnes concernées d'une telle utilisation des renseignements en fonction des obligations légales.

4. Déterminer les modalités selon lesquelles le consentement sera obtenu de la personne concernée et produire un formulaire de consentement.

   Cette sous-pratique s'applique uniquement dans les cas où l'organisme public détermine que le consentement de la personne concernée pour cette nouvelle utilisation des renseignements personnels doit être obtenu avant de les utiliser.

   Il est important que le libellé et les modalités d'obtention du consentement soient vérifiés ou approuvés par le répondant de la PRP ou le responsable de la PRP de l'organisme public.

   Se référer à la pratique PS 5.4 Mettre en œuvre des mesures pour obtenir le consentement des personnes *afin de connaître plus en détail cette sous-pratique*.

PS 4.3 Utiliser, dans la mesure du possible, des renseignements anonymes

Déterminer et mettre en œuvre les conditions à satisfaire pour que les renseignements personnels soient utilisés de façon anonyme et que les résultats (ou produits) de l'utilisation des renseignements personnels soient présentés de façon anonyme.

Une mesure importante de PRP consiste, dans tous les cas où cela est possible, à utiliser des renseignements (sous forme électronique ou autres) qui ne permettent pas d'identifier ou de reconnaître la personne concernée. Cela contribue également à réduire les coûts inhérents aux mesures de sécurité, qui doivent être mises en place lorsqu'il s'agit de renseignements personnels, ainsi que les risques de bris de confidentialité.

C'est pourquoi dès le premier but qui porte sur la collecte des renseignements personnels (BS 1), un organisme public évalue s'il est vraiment nécessaire de recueillir et de consigner dans le système des renseignements personnels (ou nominatifs), c'est-à-dire qui permettent d'identifier ou de reconnaître une personne en particulier.

Se référer à la pratique PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système *et sa* sous-pratique n° 2 Déterminer, pour chaque renseignement personnel, s'il est nécessaire à l'exercice des attributions de l'organisme public ou à la mise en œuvre d'un programme dont il a la gestion.

Dans plusieurs cas, lorsqu'une personne sollicite un service auprès d'un organisme public, celui-ci doit recueillir et consigner des renseignements personnels.

EXEMPLE

Le nom, l'adresse ou le revenu sont des renseignements indispensables pour établir l'admissibilité d'une personne à une prestation de la sécurité du revenu.

Toutefois, les renseignements peuvent être, dans certains cas, utilisés ultérieurement de façon anonyme.

EXEMPLE

S'ils sont utilisés à des fins statistiques ou de gestion, le résultat final peut être présenté avec des renseignements ne permettant pas d'identifier une personne.

Cette pratique vise, dans tous les cas où cela est réalisable, à ce que les renseignements soient utilisés de façon anonyme et à ce que les résultats (ou produits) de l'utilisation des renseignements personnels (sous forme électronique ou autres) soient présentés, rendus accessibles ou diffusés de façon à ce qu'il soit impossible d'identifier ou de reconnaître une personne en particulier.

Produits de travail types (biens livrables types)

1. Liste des conditions à satisfaire pour que des renseignements personnels soient utilisés de façon à ce que les produits (rapports sous forme électronique ou autres), résultant de l'utilisation de renseignements personnels, puissent être présentés de façon anonyme.
2. Liste des types de résultats des traitements des renseignements personnels (principalement les rapports) présentés de façon anonyme.

Sous-pratiques

1. Déterminer les conditions à satisfaire pour que des renseignements soient utilisés de façon anonyme et que les produits (rapports sous forme électronique ou autres) résultant de l'utilisation de renseignements personnels puissent être présentés, rendus accessibles ou diffusés de façon anonyme.

   Cette sous-pratique s'applique uniquement dans les cas où il n'est pas nécessaire de produire des rapports comprenant des renseignements personnels, de les rendre accessibles ou de les diffuser.

EXEMPLE

Certains rapports de gestion ou autres peuvent être réalisés initialement à partir de renseignements personnels, mais le résultat final est transmis aux gestionnaires sous la forme de données regroupées, tel un rapport statistique.

Pour déterminer les conditions à respecter afin que le résultat de l'utilisation ne révèle pas l'identité de la personne concernée, se référer à la pratique PS 1.1 Déterminer tous les renseignements personnels que l'on projette de gérer dans le système *et sa* sous-pratique n° 1 Déterminer les renseignements qui sont de nature personnelle.

Lorsque l'utilisation s'effectue de façon électronique, il est important de déterminer quels sont les types de technologies qui peuvent contribuer à traiter les renseignements de manière efficace et efficiente, sans qu'il soit possible de connaître l'identité des personnes concernées (ou de les reconnaître), et de les prendre en considération dans le processus d'évaluation des options technologiques.

EXEMPLE

L'utilisation d'un « protecteur d'identité » peut constituer une mesure préventive permettant de masquer l'identité des personnes dans un système. Un « protecteur d'identité » est utilisé pour convertir l'identité de la personne concernée en une ou plusieurs « pseudo-identités ». Deux domaines différents sont créés dans le système : le domaine d'identité où l'identité est connue et au moins un domaine où l'identité n'apparaît pas, le domaine de « pseudo-identité »*.

* Borking, J. et Raab C. *Laws*, *PETs and Other Technologies for Privacy Protection* disponible à : http://elj.warwick.ac.uk/jilt/01-1/borking.html.

Toutefois, le simple fait de masquer un renseignement d'identité, tel que le nom, l'adresse ou le sexe de la personne, ne peut assurer l'anonymat des renseignements dans tous les cas. D'autres caractéristiques peuvent permettre tout de même de la reconnaître, par exemple lorsqu'il s'agit d'un groupe restreint de personnes. Cela amène des organismes publics qui publient des statistiques à prévoir des règles particulières pour assurer que les renseignements ne permettent pas de reconnaître une personne en particulier. Il est très important de se référer au responsable de la PRP pour s'assurer de l'anonymat des renseignements.

PS 4.4 Mettre en œuvre des mesures pour prévenir l'utilisation illicite de renseignements personnels au sein de l'organisme public

Élaborer, documenter et mettre en œuvre des mesures techniques et administratives pour prévenir et contrôler toute forme d'utilisation illicite de renseignements personnels.

Il est important que chaque demande d'utilisation des renseignements personnels (sous forme automatisée, manuelle ou autres), à l'intérieur de l'organisme public, soit autorisée, au préalable, par les autorités compétentes.

EXEMPLE

Mesures de prévention :

l'enregistrement automatique des utilisations de renseignements personnels effectuées et une directive établissant les modalités d'autorisation des nouvelles demandes d'utilisations des renseignements personnels.

Se référer à la pratique PS 3.3 Mettre en œuvre des mesures visant à permettre au personnel de l'organisme public l'accès aux renseignements personnels dans les seuls cas où cela est justifié, *pour la réalisation de cette pratique*.

Se référer aux pratiques d'assurance qualité du processus de « Gestion des ententes avec les fournisseurs » pour s'assurer de la mise en œuvre des mesures de PRP par une personne, une entreprise privée ou un organisme public, dans le cadre de l'exercice d'un mandat ou de l'exécution d'un contrat de services. *Consultez à ce sujet l'*annexe L – Clause type de protection des renseignements personnels.

Produits de travail types (biens livrables types)

1. Programme de sensibilisation des membres du personnel.
2. Liste des mesures techniques et administratives pour prévenir et contrôler toute forme d'utilisation illicite des renseignements personnels, que l'utilisation soit faite sous forme automatisée, manuelle ou autres.

Sous-pratiques

1. Élaborer et diffuser un programme de sensibilisation aux membres du personnel.

EXEMPLE

Ce programme de sensibilisation pourrait être diffusé lors du déploiement du système d'information. Il pourrait être intégré dans le processus de gestion du changement.

2. Déterminer des mesures administratives et techniques afin de prévenir et de contrôler les utilisations illicites de renseignements personnels par le personnel de l'organisme public.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 2.4

DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques spécifiques de PRP qui seront réalisées dans le projet pour atteindre le but spécifique BS 4 (colonne « À faire »)
- déterminer les dispositions légales qui y sont associées (colonne « Article de loi »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts/coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe G – Produits de travail types (biens livrables types) des buts spécifiques
- annexe F – Pratiques spécifiques, sous-pratiques et dispositions légales
- tableau 1 – Légende des rôles des parties prenantes dans un projet de développement
- tableau 2 – Légende des responsabilités des parties prenantes dans un projet de développement

LÉGENDE DES SYMBOLES À UTILISER

ARTICLE DE LOI : insérer le numéro de l'article et le titre de la loi associés à cette pratique

---

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N/A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable de la sécurité de l'information . . . . . .RS
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Pilote de projet . . . . . .PP
Répondant du processus de PRP dans le projet . . . .RPPP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié . . . . . .P
En cours de réalisation . . . . . .ER
En suspens . . . . . .ES
Réalisé . . . . . .Ré
Approuvé . . . . . .A

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

AIDE-MÉMOIRE nº 2.4 DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	Nº	Article de loi	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
								Début	Fin	Prévus	Réels
Appliquer, dans tous les éléments du système d'information, les règles d'utilisation des renseignements personnels	PS 4.1										
Déterminer et évaluer les utilisations des renseignements personnels projetées lors de la modification des systèmes existants	PS 4.2										
Utiliser, dans la mesure du possible, des renseignements anonymes	PS 4.3										
Mettre en œuvre des mesures pour prévenir l'utilisation illicite de renseignements personnels au sein de l'organisme public	PS 4.4										

BS 5 COMMUNIQUER DES RENSEIGNEMENTS PERSONNELS À DES TIERS, À L'EXTÉRIEUR DE L'ORGANISME PUBLIC

La protection des renseignements personnels est réalisée lorsqu'ils sont communiqués à des tiers, à l'extérieur de l'organisme public, en respectant les principes et les obligations légales de PRP.

La confidentialité des renseignements personnels est un principe fondamental : les renseignements personnels sont confidentiels, à moins que la personne concernée n'autorise leur communication (article 53).

Dans le cas des communications effectuées avec le consentement des personnes concernées, l'organisme a l'obligation de s'assurer que le consentement respecte les obligations légales.

Dans certains cas et à certaines conditions, la Loi sur l'accès autorise un organisme à communiquer des renseignements personnels sans le consentement de la personne concernée. Deux types de situations peuvent se présenter. Selon le premier type, l'organisme jouit d'un pouvoir discrétionnaire ; « il peut » communiquer des renseignements personnels à un tiers (articles 59, 61 et 125). Selon le deuxième type, les renseignements personnels lui sont demandés par le Protecteur du citoyen ou par assignation, mandat ou ordonnance, par une personne ou un organisme qui a des pouvoirs particuliers (article 171 par. 3). Toutes les communications des renseignements doivent s'effectuer de manière à en préserver le caractère confidentiel (article 69).

EXEMPLE

Cette dernière situation se produit, notamment lorsque la demande origine du Protecteur du citoyen ou d'une personne ou d'un organisme ayant un pouvoir de contraindre à leur communication, tels les tribunaux (article 171 3°).

La communication de renseignements personnels à des tiers, sans le consentement est considérée comme une situation d'exception. Toute communication de renseignements personnels à un tiers à l'extérieur de l'organisme public est régie par une disposition de la Loi sur l'accès et, le cas échéant, des lois sectorielles auxquelles l'organisme public est assujetti.

Certaines communications devront être enregistrées (article 60) ou faire l'objet d'un registre qui sera accessible à toute personne qui en fait la demande (articles 60.1, 67.3, 67.4).

PS 5.1 Déterminer les situations où l'organisme public projette de communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public

Décrire et documenter les situations où l'organisme public projette de communiquer des renseignements personnels à des tiers à l'extérieur de l'organisme public.

Il s'agit ici des situations où l'organisme public projette de communiquer des renseignements personnels à un tiers à l'extérieur de l'organisme public, soit à une personne, à un autre organisme public ou à une entreprise privée.

Ces situations de communication de renseignements personnels se divisent en deux grandes catégories :

- avec le consentement de la personne concernée ;
- sans le consentement de la personne concernée.

Les situations où des renseignements personnels sont rendus accessibles au procureur de l'organisme public, sans le consentement de la personne concernée, sont incluses dans cette pratique, bien que dans certains cas, le procureur puisse être un employé de l'organisme.

Se référer au but spécifique BS 2 Traiter les demandes d'accès à des renseignements personnels et de rectification *et à la pratique* PS 2.1 Mettre en œuvre les modalités de traitement des demandes d'accès à des renseignements personnels et de rectification de ceux-ci, *en ce qui concerne les situations où les renseignements personnels sont communiqués à la personne concernée*.

L'identification des situations où l'on projette de communiquer des renseignements personnels à des tiers, sans le consentement des personnes concernées, ainsi que des personnes, entreprises privées et organismes publics qui les recevront, est la première étape à réaliser afin d'évaluer ultérieurement si la loi autorise de telles communications et de déterminer les mesures d'encadrement requises.

Toutefois, la liste finale des renseignements communiqués sera la liste des communications de renseignements personnels autorisées (avec et sans le consentement de la personne concernée), qui est le produit de travail de la pratique *PS 5.2 Évaluer les situations où des renseignements personnels seront communiqués à des tiers, à l'extérieur de l'organisme public*.

Produit de travail type (bien livrable type)

1. Liste des situations où l'organisme projette de communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public, avec indication des processus d'affaires concernés, des renseignements personnels communiqués et des personnes, des organismes ou des entreprises privées qui les recevront.

Sous-pratique

1. Déterminer les situations où l'organisme public projette de communiquer des renseignements personnels et déterminer celles où des renseignements seront communiqués :
   - avec le consentement de la personne concernée ;
   - sans le consentement de la personne concernée.

EXEMPLE

Situations où la Loi sur l'accès permet la communication de renseignements personnels sans le consentement de la personne concernée, à des personnes, des entreprises privées ou des organismes publics et qui sont soumises à des obligations particulières dans la Loi sur l'accès. Ce sont des communications :

- au procureur de l'organisme si le renseignement personnel est requis aux fins d'une poursuite pour infraction à une loi que cet organisme est chargé d'appliquer, ou au Procureur général si le renseignement est requis aux fins d'une poursuite pour infraction à une loi applicable au Québec (article 59 1°) ;
- au procureur de l'organisme, ou au Procureur général lorsqu'il agit comme procureur de cet organisme, si le renseignement personnel est requis aux fins d'une procédure judiciaire autre qu'une procédure visée dans le paragraphe précédent (article 59 2°) ;
- à une personne qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement personnel est requis aux fins d'une poursuite pour infraction à une loi applicable au Québec (article 59 3°) ;
- à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée (article 59 4°) ;
- à une personne qui est autorisée par la Commission d'accès à l'information, conformément à l'article 125, à utiliser un renseignement personnel à des fins d'étude, de recherche ou de statistique (article 59 5°) ;
- à une personne, un organisme public ou une entreprise privée, dans le cadre de l'exercice d'un mandat ou l'exécution d'un contrat de services que lui confie un organisme public (article 67.2) ;
- à une personne ou à un organisme, lorsque cela est nécessaire à l'exercice de la mise en œuvre d'un programme ou à l'application d'une loi au Québec, dans des circonstances exceptionnelles, à des fins de couplage ou d'appariement de fichiers lorsque cela est nécessaire à l'application d'une loi au Québec (articles 67, 68, 68.1, 69 et 70) ;
- à une personne impliquée dans un événement ayant fait l'objet d'un rapport par un corps de police, lorsqu'il s'agit d'un renseignement sur l'identité de toute autre personne qui a été impliquée dans cet événement, sauf s'il s'agit d'un témoin, d'un dénonciateur ou d'une personne dont la santé ou la sécurité serait susceptible d'être mise en péril par la communication d'un tel renseignement à des personnes qui ont le pouvoir de contraindre à la communication (tribunaux, protecteur du citoyen, enquêteurs investis des pouvoirs d'enquête, etc.) (article 59 9°) ;
- en vue de prévenir un acte de violence, dont un suicide, lorsqu'il existe un motif raisonnable de croire qu'un danger imminent de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable. Les renseignements peuvent alors être communiqués à la ou aux personne(s) exposée(s) à ce danger, à leur représentant ou à toute personne susceptible de leur porter secours (article 59.1) ;
- de documents ou de renseignements exigés par le Protecteur du citoyen ou par assignation, mandat ou ordonnance d'une personne ou d'un organisme ayant le pouvoir de contraindre à leur communication (article 171 3°).

Art. 53, 59, 59.1, 60, 60.1, 61, 67 à 70, 171 3° Loi sur l'accès

PS 5.2 Évaluer les situations où des renseignements personnels seront communiqués à des tiers, à l'extérieur de l'organisme public

Indiquer et documenter les critères à considérer pour évaluer les situations où des renseignements personnels seront communiqués à des tiers, à l'extérieur de l'organisme public ainsi que les mesures de PRP à respecter, et réaliser leur évaluation.

Indiquer et documenter les critères à considérer pour évaluer les situations où des renseignements personnels seront communiqués à des tiers, à l'extérieur de l'organisme public et réaliser leur évaluation.

Les critères retenus dans le cadre du projet pour faire cette évaluation doivent être indiqués et documentés en fonction des principes de PRP et des obligations de la Loi sur l'accès, des dispositions légales qui encadrent les activités d'un organisme public et de la jurisprudence.

Cette évaluation sera réalisée en étroite collaboration avec les personnes compétentes en sécurité assignées au projet, le répondant de la PRP et le responsable de la PRP de l'organisme public, afin de s'assurer que les obligations légales associées à la PRP sont prises en compte et que les mesures appropriées de suivi et de sécurité seront mises en œuvre lors de la communication des renseignements personnels à des tiers.

Afin d'obtenir plus d'information sur les obligations de la Loi sur l'accès relativement aux communications de renseignements personnels à des tiers et les conditions particulières à satisfaire, consultez le site Web du MRCI :
http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=5

Consultez également les documents suivants : *Loi annotée*, R. Doray et F. Charrette, p. III / 59-1 à III / 59-23, III / 67-1 à III / 70-3, et *Loi annotée*, L. Desbiens et D. Poitras, p. 282 à 288, 300 à 315.

Produits de travail types (biens livrables types)

1. Liste des communications de renseignements personnels à des tiers, qui sont autorisées avec ou sans le consentement de la personne concernée.
2. Dans le cas où des renseignements personnels seraient communiqués à des tiers, sans le consentement, liste des informations suivantes :
   - processus d'affaires concernés ;
   - renseignements personnels communiqués ;
   - personnes, organismes ou entreprises privées qui les recevront ;
   - conditions particulières de PRP à satisfaire pour effectuer ce type de communication.

Sous-pratiques

1. Indiquer et documenter les critères à considérer lors de l'évaluation des situations où des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public, ainsi que les conditions particulières de PRP à satisfaire.

   Les critères à considérer et les conditions à satisfaire sont déterminés en prenant notamment en considération :

   - la possibilité d'obtenir le consentement de la personne à la communication des renseignements personnels ;
   - la nécessité des renseignements personnels pour la personne, l'organisme ou l'entreprise privée receveur, notamment la nécessité d'obtenir des renseignements sous forme nominative ;
   - l'usage projeté des renseignements personnels communiqués ;
   - les raisons justifiant la communication des renseignements personnels sans le consentement des personnes concernées et la démonstration de sa nécessité ;
   - les dispositions légales (Loi sur l'accès et lois sectorielles) qui autorisent la communication des renseignements sans le consentement des personnes concernées ;

- l'obligation de conclure une entente écrite avec la personne, l'organisme ou l'entreprise privée qui reçoit les renseignements personnels et de la soumettre pour avis à la CAI avant que la communication puisse s'effectuer. L'entente précise les autres conditions particulières de PRP exigées par la loi pour effectuer ce type de communication et les moyens mis en œuvre pour préserver le caractère confidentiel des renseignements personnels ;

  À cet effet, se référer à la pratique PS 5.3 Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité, lorsque des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public ;

  *Consultez l'*annexe L – Clause type de protection des renseignements personnels, *proposée dans le* Guide de rédaction des contrats de services professionnels *du ministère de la Justice* ;

- le respect des conditions fixées par la CAI lorsque des renseignements personnels sont communiqués à une personne, un organisme public ou une entreprise à des fins de sondage ;

- les mesures de suivi et de sécurité à mettre en œuvre lors de la communication des renseignements personnels.

2. Évaluer et documenter les communications de renseignements personnels à des tiers.

   Cette évaluation s'effectue en fonction des critères énoncés précédemment à la sous-pratique n° 1.

   Se référer au but spécifique BS 1 Recueillir des renseignements personnels *et à la pratique* PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système *pour déterminer s'il est nécessaire de communiquer les renseignements sous forme nominative afin d'atteindre les fins visées*.

   Par ailleurs, dans certains cas, la loi constituante de l'organisme public prévoit des dispositions particulières, relativement à la communication de renseignements personnels, que l'organisme public doit respecter.

EXEMPLE

L'article 65 de la *Loi sur l'assurance maladie* limite les renseignements qui peuvent être communiqués à des tiers.

Art. 59 1° à 4°, 59.1, 60, 60.1, 67 à 70 et 125 Loi sur l'accès

PS 5.3 **Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité, lorsque des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public**

Déterminer, documenter et mettre en œuvre des mesures d'encadrement, de suivi et de sécurité, lorsque des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public.

Plusieurs mesures d'encadrement ou de suivi des communications de renseignements personnels à des tiers sont à mettre en place, et ce, en fonction de la personne, de l'organisme ou de l'entreprise privée à qui les renseignements seront communiqués et de la situation particulière visée.

Les mesures de sécurité sont déterminées une fois que l'on a évalué le bien-fondé et l'autorisation légale à communiquer des renseignements personnels à des tiers, ainsi que les modalités particulières de PRP exigées par la loi pour effectuer ce type de communication. Les mesures de sécurité réfèrent à toute mesure de sécurité propre à assurer la PRP, notamment à en préserver le caractère confidentiel.

La Loi sur l'accès prévoit que le responsable de la PRP de l'organisme public doit enregistrer certaines demandes de communications de renseignements personnels à des tiers (article 60) et tenir un registre de celles faites en vue de prévenir un acte de violence (article 60.1). De plus, l'organisme a l'obligation de constituer, maintenir à jour et rendre disponible un registre des communications de renseignements personnels à des tiers (article 67.3), afin de consigner certaines communications de renseignements personnels à des tiers sans le consentement des personnes concernées (articles 67 à 70).

Par ailleurs, afin d'exercer un contrôle du respect des conditions émises par la CAI (articles 68 à 70 et 125), l'organisme public, par le biais de son système d'information en développement, peut mettre en place un processus de consignation et de suivi des renseignements personnels transmis à des tiers.

Dans le cas des communications à des tiers externes, dont certaines nécessitent une entente écrite et un avis de la CAI, les mesures de PRP et de sécurité devront être décrites afin, notamment que les communications se fassent de manière à assurer le caractère confidentiel des renseignements. Dans certains cas, bien que la Loi sur l'accès n'oblige pas un organisme public à produire une entente écrite et à la soumettre à la CAI, les organismes concluent tout de même des ententes écrites dites « administratives » pour encadrer certaines communications de renseignements personnels (articles 67 à 69).

Les mesures techniques et administratives d'encadrement, de suivi et de sécurité différeront selon que les renseignements seront communiqués par voie électronique ou d'une autre façon et en fonction des exigences particulières de la Loi sur l'accès. Elles seront cohérentes avec les mesures de sécurité qui seront mises en œuvre pour la conservation des renseignements personnels. *Se référer au but spécifique* BS 6 Conserver des renseignements personnels *et à la pratique* PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels.

Produits de travail types (biens livrables types)

Produit de travail type associé à une obligation légale :

Lorsqu'un article de la loi est rapporté dans la description d'un produit de travail type, cela indique que ce produit de travail type est prévu dans une disposition légale expresse et que sa réalisation se fera de manière à la respecter.

1. Les mesures d'encadrement suivantes, lorsque cela s'applique :

- entente écrite avec la tierce partie (personne, organisme ou entreprise privée) et approuvée par la CAI concernant la communication de renseignements personnels à des tiers (articles 68 à 70, Loi sur l'accès) ;
- entente écrite, dite « administrative », avec la tierce partie concernant la communication de renseignements personnels à des tiers (article 67, 67.1 ou autres communications autorisées par la Loi sur l'accès) ;
- contrat écrit avec un mandataire spécifiant les mesures de PRP exigées par la loi (article 67.2, Loi sur l'accès) ;

- liste des mesures d'encadrement prises lorsque l'organisme public communique des renseignements personnels à des fins d'étude, de recherche et de statistique, à la suite d'une autorisation de recherche de la CAI (article 125, Loi sur l'accès) ;
- liste des mesures d'encadrement prises lorsque l'organisme public communique des renseignements personnels à des fins de sondage.

2. Liste des mesures administratives et techniques de suivi et de sécurité des renseignements personnels lorsqu'ils sont communiqués à des tiers, à l'extérieur de l'organisme public.
3. Éléments du système d'information développé ou modifié qui permettent de consigner des communications de renseignements personnels à des tiers et de maintenir cette consignation à jour. Cette consignation pourra se faire dans un document papier ou électronique.

Sous-pratiques

1. Enregistrer ou prévoir l'enregistrement de certaines communications de renseignements personnels.

   L'article 60 de la Loi sur l'accès prévoit que le responsable de la PRP de l'organisme public doit enregistrer les demandes de communications de renseignements personnels visées par les paragraphes 1° à 4° de l'article 59, lorsque l'organisme public accepte de les communiquer.

   Il s'agit des communications au procureur de l'organisme, au Procureur général, à une personne qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois et à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée. Les renseignements peuvent être communiqués à ces personnes selon des conditions particulières énoncées à l'article 59.

   Cet enregistrement peut se faire dans le dossier de la personne concernée ou dans un registre prévu à cet effet. Il est toutefois important de mentionner que cet enregistrement est distinct de la procédure de constitution d'un registre prévu à l'article 67.3. Le registre prévu à l'article 67.3 est accessible à toute personne qui en fait la demande et ne devrait donc pas receler de renseignements personnels lorsqu'il est rendu accessible.

   Se référer à ce sujet à la sous-pratique n° 2 qui suit.

   Par ailleurs, l'article 60.1 prévoit que la personne responsable de la PRP doit inscrire la communication dans un registre qu'elle tient à cette fin. Ce registre ne vise que les communications faites en vue de prévenir un acte de violence (article 59.1). Il est également distinct du registre prévu à l'article 67.3, associé à la sous-pratique n° 2 suivante.

   La personne ayant la plus haute autorité au sein de l'organisme public doit, par directive, établir les conditions et les modalités suivant lesquelles les renseignements peuvent être communiqués par le personnel de l'organisme. Le personnel est tenu de se conformer à cette directive (article 59.1).

2. **Constituer, maintenir à jour et rendre disponible un registre des communications des renseignements personnels à des tiers.**

Cette sous-pratique consiste à déterminer un format de registre, consigner les communications de renseignements personnels à des tiers selon ce format, déterminer les modalités de mise à jour du registre et s'assurer qu'il pourra être accessible à toute personne qui en fera la demande (article 67.3, Loi sur l'accès).

EXEMPLE

Un organisme permet à une personne de consulter le registre sur place pendant les heures habituelles de travail ou lui en transmet une copie.

La constitution d'un registre des communications des renseignements personnels effectuées sans le consentement des personnes permet, notamment à toute personne intéressée de connaître certains types de communications faites par un organisme public. Outre le registre prévu à l'article 60.1 de la Loi sur l'accès, la constitution d'un registre n'est obligatoire qu'en ce qui concerne les communications visées par les articles 67, 67.1, 67.2, 68, 68.1 de la Loi sur l'accès. Il est toutefois suggéré de consigner d'autres communications de renseignements personnels qui nécessitent un suivi et un contrôle appropriés, soit dans le registre expressément prévu par l'article 67.3 de la Loi sur l'accès ou dans un autre document.

EXEMPLE

Les communications à une personne qui est autorisée, par la Commission d'accès à l'information, à utiliser un renseignement personnel à des fins d'étude, de recherche ou de statistique ou à des fins de sondage pourraient être consignées dans le registre, bien que cela ne soit pas obligatoire.

Le registre des communications des renseignements personnels à des tiers est maintenu à jour. Il comprend au minimum les éléments suivants (article 67.3) :

1° la nature ou le type des renseignements personnels communiqués ;

2° les personnes ou organismes qui reçoivent cette communication ;

3° l'usage projeté de ces renseignements ;

4° les raisons justifiant cette communication.

Il est suggéré d'y inscrire également :

- les dispositions légales (Loi sur l'accès et lois sectorielles) qui autorisent la communication des renseignements sans le consentement des personnes concernées, notamment les articles 67, 67.1, 67.2, 68, 68.1 de la Loi sur l'accès ;
- la date de la communication et sa fréquence (hebdomadaire, mensuelle, annuelle ou autre).

Pour obtenir plus d'information au sujet de la constitution d'un registre des communications, consultez la fiche contact *La tenue d'un registre des communications de renseignements nominatifs*, disponible sur le site de la Commission d'accès à l'information : www.cai.gouv.qc.ca/fra/docu/registre.pdf

3. Conclure, lorsque cela est requis, une entente écrite avec la tierce partie et la faire approuver par la CAI.

   Il s'agit d'élaborer, lorsque cela est requis, une entente concernant la communication des renseignements personnels avec le tiers concerné (personne, organisme ou entreprise privée), de la faire approuver par la CAI et de la faire signer par les autorités habilitées à signer une telle entente.

EXEMPLE

Dans le cas des couplages de fichiers ou de la mise en œuvre d'un programme par un organisme public, la rédaction d'une entente entre les organismes visés sera nécessaire, de même qu'un avis favorable de la Commission d'accès à l'information.

Vous pouvez consulter un exemple d'entente de communication de renseignements personnels à des tiers sur le site Web du MRCI à l'adresse suivante : http://www.aiprp.gouv.qc.ca/autre/index.asp?Sect=Documentation

4. Élaborer, dans le cas d'un contrat de services avec un fournisseur de services informatiques, un contrat écrit avec des clauses de PRP et de sécurité.

   Cette sous-pratique s'applique dans l'éventualité où le fournisseur aurait accès à des renseignements personnels dans le cadre de la réalisation du mandat qui lui est confié (articles 67.2 et 69, Loi sur l'accès), à l'exception des situations où le mandat consiste en la réalisation d'un sondage par un tiers. Cette dernière situation est décrite dans la sous-pratique n° 5 qui suit.

   Il y a lieu d'évaluer si la communication est autorisée par la Loi sur l'accès ou d'autres lois auxquelles est assujetti l'organisme public et si les renseignements personnels communiqués sont nécessaires à la réalisation du mandat de l'agent ou du mandataire. Le mandat sera confié par écrit et il devra :

   - prévoir les dispositions de la Loi sur l'accès ou d'autres lois qui s'appliquent aux renseignements personnels communiqués ;
   - décrire les mesures de sécurité prises pour que les renseignements ne soient utilisés que dans l'exercice du mandat et pour qu'ils ne soient pas conservés après son expiration.

     *Consultez à ce sujet l'*annexe L – Clause type de protection des renseignements personnels.

   Les mesures mises en œuvre seront approuvées par le responsable de la PRP et les services juridiques de l'organisme public.

EXEMPLE

Un ministère communique des renseignements personnels à des agents ou des mandataires œuvrant à l'extérieur de l'organisme aux fins de gestion de la paie, de développement d'un système d'information par un fournisseur externe ou de recherche effectuée pour le compte du ministère.

Si le mandat qui est confié à un tiers est la réalisation d'un sondage pour le compte de cet organisme, celui-ci doit alors respecter les conditions fixées par la CAI dans ce cas particulier. Consultez à ce sujet les *Exigences minimales relatives à la protection des renseignements personnels lors de sondages réalisés par un organisme public ou son mandataire* et l'*Aide-mémoire*, disponibles sur le site Web de la CAI aux adresses suivantes : www.cai.gouv.qc.ca/fra/docu/sondages.pdf et www.cai.gouv.qc.ca/fra/docu/sondag-2.pdf

5. **Vérifier, dans le cas des communications de renseignements personnels à un tiers, à des fins d'étude, de recherche ou de statistique, si la CAI a autorisé au préalable la communication, et lorsque cela s'applique, si les exigences relatives au sondage sont respectées.**

   Cette sous-pratique est réalisée dans le cas où l'organisme public communiquerait des renseignements personnels à un tiers (personne, organisme ou entreprise privée) qui, à la différence de la sous-pratique précédente n° 4, agit pour son propre compte et désire obtenir des renseignements personnels à des fins d'étude, de recherche ou de statistique (article 125, Loi sur l'accès).

   Dans ce cas, la CAI doit avoir au préalable autorisé l'organisme à communiquer des renseignements personnels à ce tiers. Il fera sa demande à la CAI en utilisant un formulaire prévu à cet effet.

EXEMPLE

Autorisation de la CAI pour une recherche sur les maladies liées au vieillissement de la population :

la Commission a autorisé le ministère de la Santé et des Services sociaux à transmettre à des chercheurs des renseignements nominatifs provenant du fichier des décès, dans le cadre d'une étude sur la prévalence des maladies cognitives associées à l'âge. Outre le maintien du caractère confidentiel des renseignements personnels, la Commission a exigé qu'ils soient détruits une fois la recherche terminée. Rapport annuel de la CAI 2001-2002, page 49, numéro de dossier de la CAI : 01 14 14.

Pour obtenir une copie du *Formulaire de demande d'autorisation de recevoir des renseignements nominatifs à des fins de recherche, d'étude ou de statistique*, consultez le site Web de la CAI : http://www.cai.gouv.qc.ca/fra/biblio_fr/bib_pub_fr.htm

Par ailleurs, s'il s'avérait que le chercheur œuvre au sein d'un organisme public et que, dans le cadre de sa recherche, il obtienne des renseignements personnels d'un autre organisme public pour faire un sondage, celui-ci devrait également respecter les exigences de la CAI sur les sondages.

6. **Déterminer, documenter et mettre en œuvre des mesures de sécurité lors des communications à des tiers, à l'extérieur de l'organisme public.**

   Cette sous-pratique peut être réalisée en relation avec la pratique *PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels*.

Art. 53
Loi sur l'accès

PS 5.4 Mettre en œuvre des mesures pour obtenir le consentement des personnes

Indiquer, documenter et mettre en œuvre les conditions à respecter pour que le consentement et les modalités de son obtention auprès de la personne concernée par les renseignements personnels respectent les principes et obligations légales de PRP.

Les conditions pour l'obtention d'un consentement doivent être établies en fonction des principes de PRP et des obligations de la Loi sur l'accès, des dispositions légales qui encadrent les activités d'un organisme public, des exigences de la CAI et de la jurisprudence.

Cette pratique s'applique dans tous les cas où le consentement est obtenu auprès de la personne concernée. Elle est réalisée en étroite collaboration avec le répondant de la PRP ou le responsable de la PRP de l'organisme, car il est important que les conditions d'obtention du consentement et le libellé soient vérifiés par ces personnes ou par les services juridiques au sein de l'organisme public.

Produits de travail types (biens livrables types)

1. Description des modalités d'obtention du consentement.
2. Formulaire de consentement.

Sous-pratiques

1. Déterminer les modalités selon lesquelles le consentement sera obtenu auprès de la personne concernée.

   Ces modalités d'obtention d'un consentement jouent un rôle de premier plan pour déterminer un « consentement légalement valide ». Il y a donc lieu de s'assurer que les modalités respectent les exigences légales.

   Consultez à ce sujet la rubrique *Communication de renseignements personnels avec le consentement* sous *Critères d'un consentement valide*, disponible sur le site Web du MRCI :
   http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=5#Li2

2. Produire un formulaire de consentement.

   Lors de la rédaction du libellé de consentement, les modalités qui auront été retenues pour obtenir un consentement légalement valide seront prises en compte.

EXEMPLE

Consentement qui reflète le caractère manifeste et auquel on peut se référer pour élaborer un consentement :

Je *(personne concernée)* …… autorise …….. *(organisme détenteur)* à communiquer à……..

(organisme receveur) les renseignements suivants me concernant …….. *(énumérer les renseignements communiqués)*

aux fins de …….. *(indiquer les motifs justifiant la communication)*.

Ce consentement est valide pour une durée de ……..

Signature …….. Date ……..

3. Faire approuver, par le répondant de la PRP dans le projet ou le responsable de la PRP de l'organisme public (RPRP), le libellé du consentement et les modalités selon lesquelles il sera obtenu.

   Cette sous-pratique est utile uniquement lorsque ce n'est pas le répondant de la PRP ou le RPRP qui a réalisé les deux premières sous-pratiques.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 2.5

DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques spécifiques de PRP qui seront réalisées dans le projet pour atteindre le but spécifique BS 5 (colonne « À faire »)
- déterminer les dispositions légales qui y sont associées (colonne « Article de loi »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts/coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe G – Produits de travail types (biens livrables types) des buts spécifiques
- annexe F – Pratiques spécifiques, sous-pratiques et dispositions légales
- tableau 1 – Légende des rôles des parties prenantes dans un projet de développement
- tableau 2 – Légende des responsabilités des parties prenantes dans un projet de développement

LÉGENDE DES SYMBOLES À UTILISER

ARTICLE DE LOI : insérer le numéro de l'article et le titre de la loi associés à cette pratique

---

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N/A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable de la sécurité de l'information . . . . . .RS
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Pilote de projet . . . . . .PP
Répondant du processus de PRP dans le projet . . . .RPPP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié . . . . . .P
En cours de réalisation . . . . . .ER
En suspens . . . . . .ES
Réalisé . . . . . .Ré
Approuvé . . . . . .A

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 1 – RÉALISER LA PRP	BS 5	COMMUNIQUER DES RENSEIGNEMENTS PERSONNELS À DES TIERS, À L'EXTÉRIEUR DE L'ORGANISME PUBLIC

AIDE-MÉMOIRE nº 2.5 DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	Nº	Article de loi	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
								Début	Fin	Prévus	Réels
Déterminer les situations où l'organisme public projette de communiquer des renseignements personnels à des tiers à l'extérieur de l'organisme public	PS 5.1										
Évaluer les situations où des renseignements personnels seront communiqués à des tiers, à l'extérieur de l'organisme public	PS 5.2										
Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité, lorsque des renseignements personnels sont communiqués à des tiers à l'extérieur de l'organisme public	PS 5.3										
Mettre en œuvre des mesures pour obtenir le consentement des personnes	PS 5.4										

BS 6 CONSERVER DES RENSEIGNEMENTS PERSONNELS

La protection des renseignements personnels est réalisée lorsqu'ils sont conservés, en respectant les principes et les obligations légales de PRP ainsi que le calendrier de conservation et les exigences de sécurité.

Outre les dispositions de la Loi sur l'accès, un organisme public conserve les renseignements personnels consignés et utilisés par le système d'information en développement de manière à respecter :

- la *Loi sur les archives* ;
- la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale* du Conseil du trésor, lorsqu'elle s'applique ;
- les mesures d'encadrement administratif qui s'appliquent plus particulièrement à son organisation, notamment les politiques et autres directives sur la protection et la sécurité de l'information.

Lorsqu'il déterminera les mesures de sécurité à mettre en place pour conserver les renseignements personnels, il prendra par ailleurs en considération d'autres dispositions légales, telles que la *Loi concernant le cadre juridique des technologies de l'information* et toutes autres lois auxquelles il est assujetti.

PS 6.1 Mettre en œuvre des mesures pour conserver les renseignements personnels en respectant le calendrier de conservation, et ce, tout au long de leur cycle de vie

Art. 7, 8 et 15 Loi sur les archives

Élaborer, documenter et mettre en œuvre des mesures pour conserver les renseignements personnels actifs, semi-actifs ou inactifs en fonction des délais prévus au calendrier de conservation, et ce, tout au long de leur cycle de vie.

La *Loi sur les archives* oblige un organisme public à produire un calendrier de conservation qui détermine les délais de conservation. L'article 7 de cette loi prévoit que « tout organisme public doit établir et tenir à jour un calendrier de conservation qui détermine les périodes d'utilisation et les supports de conservation de ses documents actifs et semi-actifs et qui indique quels documents inactifs sont conservés de manière permanente et lesquels sont éliminés »*. Il doit soumettre à l'approbation du ministre son calendrier de conservation et chacune de ses modifications (article 8). Il doit également verser au conservateur les documents inactifs dont le calendrier de conservation prévoit la conservation permanente (article 15).

Ainsi, les renseignements personnels consignés dans le système d'information sont soumis à ces dispositions légales.

* L'article 3 de la *Loi sur les archives* (L.R.Q., chapitre C-1.1) fournit les définitions de : « document, document actif, document inactif, document semi-actif ». Cette loi est disponible à : www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_21_1/A21_1.html

L'organisme public prendra également en considération la *Loi concernant le cadre juridique des technologies de l'information*, notamment les dispositions relatives à l'impartition des services de garde des documents technologiques (article 26) et toute autre loi à laquelle il est assujetti.

De plus, pour réaliser cette pratique, on référera à la politique ou directive de l'organisme sur la gestion des documents. La personne responsable de la gestion documentaire au sein de l'organisme sera associée à la réalisation de cette pratique.

Cette pratique peut être réalisée en relation avec la pratique *PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels*.

Produits de travail types (biens livrables types)

1. Calendrier de conservation ou partie du calendrier de conservation relatifs aux renseignements personnels du système d'information en développement.
2. Liste des mesures techniques et administratives pour conserver des renseignements personnels, incluant ceux qui sont destinés à être conservés de façon permanente, en respectant les délais prévus au calendrier de conservation.
3. Éléments du système d'information développé qui implantent les mesures techniques et administratives de conservation définies par le produit de travail type n° 2.

Sous-pratiques

1. Élaborer les règles de conservation des renseignements personnels en déterminant, d'une part, les durées de conservation pour les renseignements personnels qui :

   - sont d'utilité courante (exploitation du système) ;
   - sont occasionnellement utilisés à des fins administratives ou légales (semi-actifs) ;

   En déterminant, d'autre part, le mode de disposition des renseignements personnels qui :

   - ne sont plus utilisés à des fins administratives ou légales (inactifs) et sont destinés à être détruits ; ou
   - en ce qui a trait aux renseignements personnels ayant une valeur de recherche ou une valeur historique, sont destinés à être conservés de façon permanente.

   Dans le cas du remplacement d'un système d'information existant, ces règles de conservation porteront autant sur les renseignements personnels du système remplacé que sur ceux du nouveau système.
2. Déterminer les mesures techniques et administratives pour conserver (ou « stocker » ou « archiver ») les renseignements personnels identifiés dans la sous-pratique n° 1 en fonction des délais prévus au calendrier de conservation.
3. Mettre en œuvre les mesures techniques et administratives décrites dans la sous-pratique n° 2.

PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels

Chapitre 3
Loi sur l'accès

Élaborer, documenter et mettre en œuvre des mesures de sécurité pour assurer le respect des facteurs de sécurité suivants : disponibilité, intégrité, confidentialité des renseignements personnels, authentification des utilisateurs et irrévocabilité des documents qu'ils rédigent ou des actions qu'ils posent (facteurs DICAI), et ce, tout au long du cycle de vie des renseignements personnels.

Le caractère confidentiel des renseignements personnels, qui constitue le principe fondamental de la Loi sur l'accès (article 53), exige qu'un organisme public mette en œuvre, en tout temps et pour tout le cycle de vie des renseignements personnels, des mesures de sécurité propres à assurer la PRP. Pour réaliser cette pratique, se référer, notamment :

- à la politique et aux directives sur la sécurité de l'organisme public ;
- à la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale* sur le site Web du Conseil du trésor : www.tresor.gouv.qc.ca/doc/acrobat/dirsec1.pdf ;
- aux autres travaux sur la sécurité dans l'intranet du Secrétariat du Conseil du trésor *Sécurité de l'information numérique et ICPG* : http://www.inforoute-gouvernementale.qc/securite.htm

Le responsable de la sécurité de l'information au sein de l'organisme sera associé à la réalisation de cette pratique. Pour les organismes assujettis à cette directive, il s'agit du responsable de la sécurité de l'information numérique (RSIN).

Consultez également la *Loi concernant le cadre juridique des technologies de l'information*, sur le site Web du Secrétariat du Conseil du trésor, qui fournit un texte annoté par article et un texte annoté par sujet de cette loi : www.autoroute.gouv.qc.ca/loi_en_ligne/loi/sujet.html. Cette loi porte sur le cycle de vie complet d'un document.

Produits de travail types (biens livrables types)

1. Liste des mesures de sécurité techniques et administratives mises en œuvre tout au long du cycle de vie des renseignements personnels.
2. Éléments du système d'information développé ou modifié qui implantent les mesures techniques et administratives de sécurité définies par le produit de travail type n° 1.

Sous-pratiques

1. Déterminer et documenter des mesures de sécurité techniques et administratives tout au long du cycle de vie des renseignements personnels.

   Dans le cas des communications à l'extérieur de l'organisme public, se référer à la pratique PS 5.3 Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité, lorsque des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public.

Le Secrétariat du Conseil du trésor a produit un guide qui propose une démarche pour catégoriser l'information numérique. Ce guide, intitulé *Guide relatif à la catégorisation des documents technologiques en matière de sécurité* peut être obtenu en vous adressant par courriel au Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles à l'adresse suivante :
inforoute-gouvernementale@sct.gouv.qc.ca

Il y aura lieu, lors de l'établissement des mesures de sécurité, d'être particulièrement attentif aux renseignements personnels de nature sensible.

Bien que la Loi sur l'accès accorde le même degré de confidentialité et de protection à tous les renseignements personnels, les organismes publics devraient accorder une attention particulière aux renseignements de nature sensible. Il est toutefois difficile de définir *a priori* un ensemble de renseignements qui soient universellement considérés comme sensibles, cela étant tributaire de plusieurs facteurs, notamment des organisations en cause et du contexte d'utilisation des renseignements personnels.

On reconnaît toutefois, parmi les renseignements personnels de nature sensible, ceux dont la divulgation risque de porter préjudice à une personne, pouvant engendrer la perte d'emploi, la discrimination ou la stigmatisation sociale, ou les renseignements tels que des numéros d'identification uniques à une personne qui permettent de regrouper ou de fusionner plusieurs renseignements à son sujet.

EXEMPLE

Des renseignements de nature médicale, des renseignements biométriques, liés au dépistage génétique, à des antécédents judiciaires, l'origine ethnique, les convictions religieuses, des identifiants tels le numéro d'assurance sociale, de permis de conduire ou d'assurance maladie, le code permanent d'un étudiant et des renseignements de nature financière sont généralement considérés comme étant de nature sensible.

Il est reconnu que les renseignements de nature médicale sont parmi les renseignements les plus sensibles. Le Secrétariat du Conseil du trésor et la Commission d'accès à l'information (CAI) ont établi des exigences particulières pour les organismes publics qui recueillent ou ont accès à des renseignements de nature médicale concernant leurs employés. Consultez à ce sujet le *Rapport du comité de travail sur la gestion des diagnostics médicaux des employés de la fonction publique mandaté par le Comité interministériel sur la protection des renseignements personnels*, sur le site Web : www.tresor.gouv.qc.ca/publications/diagnosticsante-employes.pdf et les *Fiches conseil* de la CAI *Le diagnostic médical des employés de la fonction publique* et *La gestion des réclamations dans le cadre d'un programme collectif d'assurance médicaments* sur son site Web : www.cai.gouv.qc.ca/fra/docu/diagnost.pdf et www.cai.gouv.qc.ca/fra/docu/contact.pdf

Les numéros d'identification sont des renseignements uniques et spécifiques qui permettent de situer et de retracer rapidement les personnes sur lesquelles des informations sont colligées. La collecte, la consignation et l'utilisation de tels numéros peuvent certes être légitimes et légalement autorisées dans des situations particulières. Il importe toutefois de garder à l'esprit que, tout en facilitant des transactions (électroniques ou autres) ou le couplage et l'appariement de différentes banques de données, ainsi que la surveillance des personnes, elles constituent également des risques importants d'atteinte à la PRP.

EXEMPLE

Un employeur peut recueillir le numéro d'assurance sociale d'un employé. Ce numéro sera donc consigné dans le dossier de l'employé, mais il ne figurera pas dans le module ou l'écran « recherche personne » qui est accessible à un grand nombre d'employés. Un numéro séquentiel neutre sera plutôt assigné à chaque employé.

Se référer à la pratique PS 3.3 Mettre en œuvre des mesures visant à permettre au personnel de l'organisme public l'accès aux renseignements personnels dans les seuls cas où cela est justifié.

La CAI a par ailleurs précisé, dans certaines enquêtes, les situations où des numéros d'identification uniques, tels que le numéro d'assurance sociale, de permis de conduire ou d'assurance maladie, peuvent être recueillis. Pour obtenir plus d'information sur la collecte et l'utilisation des numéros d'identification, consultez le site Web du MRCI :
http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=2#identification

Certains organismes publics produisent eux-mêmes des numéros d'identification uniques pour répondre à leurs besoins particuliers, tels que le code permanent d'un étudiant (réseau de l'éducation) ou un numéro séquentiel ou autre attribué à une personne en particulier (numéro de dossier d'un client ou d'un employé). Lorsque cela est possible, il est préférable de choisir un numéro d'identification qui n'est pas facilement composable à partir d'éléments d'identification habituels tels le nom, le prénom et la date de naissance.

2. **Déterminer et documenter des mesures techniques et administratives pour que les renseignements personnels soient tenus à jour, exacts et complets, pour servir aux fins pour lesquelles ils sont recueillis.**

   Cette sous-pratique constitue une des mesures de sécurité technique ou administrative de la sous-pratique n° 1 précédente. Elle doit faire l'objet d'une attention particulière, car elle est associée à une obligation de la Loi sur l'accès. L'article 72 de cette loi prévoit qu'un organisme public doit veiller à ce que les renseignements nominatifs qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis.

EXEMPLE

Mesures liées aux sous-pratiques n° 1 et n° 2 :

- l'exactitude des renseignements personnels est validée, avant qu'ils soient recueillis ou consignés ou le plus tôt possible après leur consignation ;
- le système indique notamment la date de la dernière mise à jour d'un dossier comportant un renseignement personnel et la nature de la modification ;
- le système indique la source de l'information utilisée pour faire des changements aux renseignements personnels en indiquant les documents sur un support papier ou l'enregistrement des transactions électroniques ;
- le système est conçu de telle sorte que les accès et les modifications des renseignements personnels sont enregistrés en indiquant la date et l'identification de l'utilisateur ;
- des contrôles assurent que le processus de détermination des privilèges d'accès pour modifier, ajouter ou détruire des renseignements personnels fait l'objet d'une autorisation préalable des autorités désignées ; voir à cet effet la pratique *PS 3.1 Déterminer les droits d'accès aux renseignements personnels*, pour plus d'information concernant les droits d'accès ;
- des contrôles assurent que seules les personnes autorisées peuvent recueillir, inscrire ou faire inscrire des renseignements personnels dans le système.

Dans certains cas, afin d'éviter que l'authenticité des renseignements personnels ne soit contestée, le système sera développé ou modifié de façon à ce que les renseignements déjà inscrits ne puissent être effacés. Consultez à ce sujet les *Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la Santé et des Services sociaux*, disponibles sur le site Web de la CAI : http://www.cai.gouv.qc.ca/fra/docu/exigence.pdf

3. Mettre en œuvre des mesures de sécurité techniques et administratives, tout au long du cycle de vie des renseignements personnels.

   Se référer aux mesures décrites aux sous-pratiques n° 1 et n° 2 précédentes.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 2.6

DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques spécifiques de PRP qui seront réalisées dans le projet pour atteindre le but spécifique BS 6 (colonne « À faire »)
- déterminer les dispositions légales qui y sont associées (colonne « Article de loi »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts/coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe G – Produits de travail types (biens livrables types) des buts spécifiques
- annexe F – Pratiques spécifiques, sous-pratiques et dispositions légales
- tableau 1 – Légende des rôles des parties prenantes dans un projet de développement
- tableau 2 – Légende des responsabilités des parties prenantes dans un projet de développement

LÉGENDE DES SYMBOLES À UTILISER

ARTICLE DE LOI : insérer le numéro de l'article et le titre de la loi associés à cette pratique

---

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N/A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable de la sécurité de l'information . . . . . .RS
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Pilote de projet . . . . . .PP
Répondant du processus de PRP dans le projet . . . .RPPP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié . . . . . .P
En cours de réalisation . . . . . .ER
En suspens . . . . . .ES
Réalisé . . . . . .Ré
Approuvé . . . . . .A

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 1 – RÉALISER LA PRP	BS 6	CONSERVER DES RENSEIGNEMENTS PERSONNELS

AIDE-MÉMOIRE nº 2.6 DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	Nº	Article de loi	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
								Début	Fin	Prévus	Réels
Mettre en œuvre des mesures pour conserver les renseignements personnels en respectant le calendrier de conservation, et ce, tout au long de leur cycle de vie	PS 6.1										
Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels	PS 6.2										

BS 7 DÉTRUIRE DES RENSEIGNEMENTS PERSONNELS

La protection des renseignements personnels est réalisée lorsqu'ils sont détruits en respectant les principes et les obligations légales de PRP et d'élimination des archives publiques.

Dans le but de protéger les renseignements personnels, notamment d'en préserver la confidentialité, la Loi sur l'accès prévoit que l'on doit détruire un renseignement lorsque l'objet pour lequel il a été recueilli est accompli (article 73). Cette obligation doit, toutefois, tenir compte des dispositions de la *Loi sur les archives* et du *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques*.

C'est donc la *Loi sur les archives* qui permet de déterminer les délais de conservation, selon un calendrier de conservation, et le moment où un renseignement personnel doit être détruit. À cet égard, elle l'emporte sur l'article 73 de la Loi sur l'accès*.

La CAI a recommandé de prendre des mesures de sécurité particulières tant à l'intérieur de l'organisme que dans le cas où ce dernier confierait un mandat de destruction à une firme externe. Consulter à ce sujet le *Guide pour la destruction des documents renfermant des renseignements personnels de la CAI*, disponible sur le site de la CAI à l'adresse suivante : www.cai.gouv.qc.ca/fra/docu/destruct.pdf

Il y a lieu d'accorder une attention particulière à la destruction des renseignements personnels contenus dans un système existant et qui est destiné à être remplacé par un nouveau système.

Art. 73 Loi sur l'accès
Art. 7, 8 et 15 Loi sur les archives

PS 7.1 Mettre en œuvre des mesures de destruction des renseignements personnels

Élaborer, documenter et mettre en œuvre des mesures techniques et administratives pour détruire des renseignements personnels en fonction des principes et des obligations légales de PRP et du calendrier de conservation.

Produits de travail types (biens livrables types)

1. Liste des mesures techniques et administratives pour détruire des renseignements personnels.
2. Éléments du système d'information développé ou modifié qui implantent les mesures techniques et administratives de destruction définies par le produit de travail type n° 1.

Sous-pratiques

1. Déterminer, en respectant les délais de conservation établis par le calendrier de conservation, ainsi que leur caractère confidentiel, les mesures techniques et administratives pour détruire les renseignements personnels.

* Loi annotée, R. Doray et F. Charrette, p. III/73-1.

La destruction des renseignements personnels s'effectue de manière à en préserver le caractère confidentiel. La destruction de renseignements personnels de nature plus sensible pourrait exiger la mise en place de mesures particulières. Leur destruction s'effectue en tenant compte des obligations découlant de la *Loi sur les archives*, que vous pouvez consulter sur le site Web des Publications du Québec : http://www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_21_1/A21_1.html

Se référer à la pratique PS 6.1 Mettre en œuvre des mesures pour conserver les renseignements personnels en respectant le calendrier de conservation, et ce, tout au long de leur cycle de vie.

EXEMPLE

Lorsque l'on détruit un fichier sur un disque rigide, un organisme public s'assure que non seulement le répertoire des fichiers est mis à jour, mais que le fichier lui-même est effacé du disque rigide ainsi que ses copies, et ce, de manière irréversible.

La CAI a, par ailleurs, recommandé de prendre des mesures de sécurité particulières tant à l'intérieur de l'organisme que dans le cas où il confierait un mandat de destruction à une firme externe. Consultez à ce sujet le *Guide pour la destruction des documents renfermant des renseignements personnels*, disponible sur le site Web de la CAI : www.cai.gouv.qc.ca/fra/docu/destruct.pdf

Consultez également la *Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasinés dans un équipement micro-informatique ou un support informatique amovible*, disponible sur le site Web du Conseil du trésor : www.tresor.gouv.qc.ca/doc/acrobat/directivemicro99.pdf et d'autres directives du Conseil du trésor.

2. Effectuer la destruction des renseignements personnels selon les modalités décrites.

   Cette sous-pratique se réalisera, lors du développement d'un système d'information, uniquement pour les renseignements personnels provenant d'un système existant qui sera remplacé ou mis au rancart pour faire place au nouveau système.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 2.7

DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques spécifiques de PRP qui seront réalisées dans le projet pour atteindre le but spécifique BS 7 (colonne « À faire »)
- déterminer les dispositions légales qui y sont associées (colonne « Article de loi »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts/coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe G – Produits de travail types (biens livrables types) des buts spécifiques
- annexe F – Pratiques spécifiques, sous-pratiques et dispositions légales
- tableau 1 – Légende des rôles des parties prenantes dans un projet de développement
- tableau 2 – Légende des responsabilités des parties prenantes dans un projet de développement

LÉGENDE DES SYMBOLES À UTILISER

ARTICLE DE LOI : insérer le numéro de l'article et le titre de la loi associés à cette pratique

---

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N/A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable de la sécurité de l'information . . . . . .RS
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Pilote de projet . . . . . .PP
Répondant du processus de PRP dans le projet . . . .RPPP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié . . . . . .P
En cours de réalisation . . . . . .ER
En suspens . . . . . .ES
Réalisé . . . . . .Ré
Approuvé . . . . . .A

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 1 – RÉALISER LA PRP	BS 7	DÉTRUIRE DES RENSEIGNEMENTS PERSONNELS

AIDE-MÉMOIRE nº 2.7 DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

Projet :	Sous-projet :

Pratiques du Modèle	Nº	Article de loi	Pratique équi-valente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
								Début	Fin	Prévus	Réels
Mettre en œuvre des mesures de destruction des renseignements personnels	PS 7.1										

BS 8 DIFFUSER L'INFORMATION SUR LA GESTION DES RENSEIGNEMENTS PERSONNELS

L'information relative à l'existence des fichiers de renseignements personnels et à la manière dont l'organisation gère et assure la protection des renseignements personnels consignés dans le système d'information est rendue disponible à toute personne, dans un langage clair et facilement compréhensible, en respectant les principes et obligations légales de PRP.

Les organismes publics ont la responsabilité de gérer les renseignements personnels en toute transparence et de manière à inspirer confiance aux personnes concernées. Un des principes fondamentaux de la PRP est à l'effet que chaque personne a le droit de connaître quels renseignements les organismes publics recueillent à son sujet, les personnes qui y ont accès, les utilisations qui peuvent en être faites, les mesures prises pour en préserver le caractère confidentiel et leurs conditions de conservation et de destruction.

Les organismes publics veillent à ce que ces personnes soient informées des politiques et des modalités de gestion des renseignements personnels mises en œuvre au sein de l'organisation et les rendent facilement accessibles et compréhensibles.

EXEMPLE

L'élaboration et la diffusion des pratiques courantes de PRP, par la reddition de comptes dans le rapport annuel de gestion ou par des politiques de confidentialité et de PRP diffusées sur le site Web de l'organisme ou au moyen de dépliants transmis à la clientèle.

Un des mécanismes prévus explicitement dans la Loi sur l'accès, et qui repose sur ce principe de transparence, est l'obligation de constituer des fichiers de renseignements personnels, de les mettre à jour et de les déclarer à la Commission d'accès à l'information.

Fichier de renseignements personnels :

Selon la CAI, il s'agit d'une collection organisée de renseignements personnels, c'est-à-dire de renseignements qui concernent des personnes physiques et permettent de les identifier.

Ainsi, la Loi sur l'accès prévoit l'obligation de verser des renseignements personnels, lorsqu'ils répondent à certaines conditions, dans un fichier de renseignements personnels, de déclarer ce fichier à la CAI et d'en assurer la mise à jour (articles 71, 76 et 77, Loi sur l'accès).

« Le premier objectif d'une déclaration de fichier en est un d'information : porter à la connaissance du public l'existence des fichiers de renseignements personnels. Un second objectif peut être attribué aux déclarations de fichiers : permettre à la CAI d'exercer son pouvoir de surveillance et d'établir des normes relatives à la protection des renseignements personnels recueillis et détenus par les organismes publics »*.

* *La déclaration d'un fichier de renseignements personnels*, CAI, page 5. La CAI définit également la notion de fichier de renseignements personnels à la page 8 de ce document.

PS 8.1 Constituer et maintenir à jour un inventaire des fichiers de renseignements personnels créés ou transférés dans le nouveau système ou modifiés dans le système existant et les déclarer à la Commission d'accès à l'information (CAI)

Art. 71, 76, 77
Loi sur l'accès

Constituer un inventaire des « fichiers de renseignements personnels » créés, modifiés ou transférés dans le système d'information, les déclarer à la CAI, effectuer leur mise à jour selon des modalités déterminées et informer la CAI de toute modification ultérieure.

Le terme « inventaire des fichiers » prend un sens particulier dans le contexte de la Loi sur l'accès. L'inventaire ne se limite pas à une simple énumération de fichiers, mais comprend aussi d'autres informations de gestion concernant ces fichiers, notamment le volume, le type et la provenance des renseignements personnels, leur localisation, leur utilisation et leur circulation au sein de l'organisme*.

Produits de travail types (biens livrables types)

1. Inventaire des « fichiers de renseignements personnels » créés ou transférés dans le nouveau système ou modifiés dans le système existant et comportant pour chaque fichier les indications suivantes (article 76, Loi sur l'accès) :

   1° la désignation de chaque fichier, les types de renseignements personnels qu'il contient, l'usage projeté de ces renseignements et le mode de gestion de chaque fichier ;

   2° la provenance des renseignements personnels versés à chaque fichier ;

   3° les catégories de personnes concernées par les renseignements personnels versés à chaque fichier ;

   4° les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions ;

   5° les mesures de sécurité prises pour assurer le caractère confidentiel des renseignements personnels et leur utilisation suivant les fins pour lesquelles ils ont été recueillis ;

   6° le titre, l'adresse et le numéro de téléphone de la personne responsable de la protection des renseignements personnels ;

   7° les modalités d'accès offertes à la personne concernée.

2. Formulaires de déclaration de fichiers complétés pour chaque fichier de renseignements personnels, mis à jour et transmis à la CAI (articles 76 et 77, Loi sur l'accès).

* *La déclaration d'un fichier de renseignements personnels*, CAI, page 5.

Sous-pratiques

1. En référant aux processus d'affaires qu'ils supportent, déterminer, parmi les renseignements personnels à recueillir et consigner dans le système et ses sous-systèmes, ceux qui correspondent à la définition légale de « fichiers de renseignements personnels », c'est-à-dire qui répondent à l'une ou l'autre des deux conditions suivantes (article 71, Loi sur l'accès) :

   1° sont identifiés ou se présentent de façon à être retrouvés par référence au nom d'une personne ou à un signe ou symbole propre à celle-ci ; ou

   2° ont servi ou sont destinés à servir pour une décision concernant une personne.

   Lorsqu'ils répondent à l'une ou l'autre de ces conditions, les renseignements personnels font partie d'un « fichier de renseignements personnels », tel qu'il est désigné dans la Loi sur l'accès.

   L'objectif visé est de rassembler les renseignements personnels et de déterminer s'ils font partie ou non d'un fichier de renseignements personnels. Comme la loi ne définit pas expressément le terme « fichier », si ce n'est par son contenu ou par certaines conditions qui doivent présider à son organisation, il y a lieu de s'en remettre à une définition usuelle. Selon la CAI, un fichier correspond à une « collection organisée de renseignements personnels suivant des modalités fixées par l'organisme dans le cadre de ses mandats ». Pour plus d'information, se référer au document *La déclaration d'un fichier de renseignements personnels* de la CAI et consulter la rubrique *Inventaire des fichiers de renseignements personnels* sur le site Web du MRCI : http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=1

   Se référer également à la pratique PS 1.1 Déterminer tous les renseignements personnels que l'on projette de gérer dans le système.

   Dans un même système d'information, il peut exister des sous-systèmes et des transactions ou des rapports sous forme électronique, papier ou autres qui contiennent des renseignements personnels. Il y a donc lieu de déterminer également s'ils font partie d'un « fichier de renseignements personnels ».

EXEMPLE

Fichiers de renseignements personnels :

- fichier des ressources humaines, comprenant des renseignements sur un employé relatifs au travail, à la carrière, à la profession, à l'embauche, etc. ;
- fichier des bénéficiaires d'un établissement de santé et services sociaux, comprenant des renseignements personnels relatifs à la santé d'une personne : examens, diagnostics, soins médicaux ou psychosociaux, analyses, etc. ;
- fichier de la clientèle, comprenant des renseignements permettant d'établir le droit d'une personne à des services dispensés par des organismes publics, telle la prestation de la sécurité du revenu.

2. Déterminer un format d'inventaire des fichiers de renseignements personnels.

   La Loi sur l'accès ne prévoit pas, pour les organismes publics, l'obligation explicite de produire un inventaire des fichiers de renseignements personnels. Toutefois, afin de faciliter la production de la déclaration de fichiers à la CAI, l'organisme public peut effectuer un tel inventaire. Pour ce faire, il peut référer à l'article 76 de la Loi sur l'accès.

Selon l'article 76, la déclaration de fichiers à la CAI doit comprendre les indications suivantes :

1° La désignation de chaque fichier, les types de renseignements qu'il contient, l'usage projeté de ces renseignements et le mode de gestion de chaque fichier ;

Se référer à la pratique PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système.

2° La provenance des renseignements versés à chaque fichier ;

Se référer à la pratique PS 1.3 Déterminer les sources d'obtention des renseignements personnels.

3° Les catégories de personnes concernées par les renseignements versés à chaque fichier ;

4° Les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions ;

Se référer aux pratiques PS 3.1 Déterminer les droits d'accès aux renseignements personnels *et* PS 3.2. Concevoir et développer le système de manière à respecter les droits d'accès établis.

5° Les mesures de sécurité prises pour assurer le caractère confidentiel des renseignements personnels et leur utilisation suivant les fins pour lesquelles ils ont été recueillis ;

Se référer à la pratique PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels.

6° Le titre, l'adresse et le numéro de téléphone de la personne responsable de la protection des renseignements personnels ;

7° Les modalités d'accès offertes à la personne concernée.

Se référer au document La déclaration d'un fichier de renseignements personnels *et au* Formulaire de déclaration de fichiers de renseignements personnels *que vous pouvez obtenir auprès du responsable de la PRP de l'organisme public ou de la CAI en adressant la demande par courriel à l'adresse suivante : cai.communications@cai.gouv.qc.ca.*

La déclaration de fichiers de renseignements personnels doit être faite conformément aux règles établies par la CAI.

3. **Déterminer les modalités de mise à jour des déclarations de fichiers de renseignements personnels et les maintenir à jour.**

   L'article 77 de la Loi sur l'accès prévoit qu'un organisme public doit aviser la CAI de tout changement rendant inexacte ou incomplète la déclaration de fichiers de renseignements personnels.

4. **Informer le responsable de la PRP de l'organisme public des « fichiers de renseignements personnels » créés ou transférés dans le système d'information ou de leur mise à jour.**

5. **Déclarer les fichiers de renseignements personnels à la CAI et l'informer des mises à jour.**

   L'organisme public est tenu d'aviser la CAI de tout changement rendant inexacte ou incomplète la déclaration de fichiers (article 77, Loi sur l'accès).

PS 8.2 Diffuser l'information sur les modalités de gestion des renseignements personnels

Déterminer et mettre en place des mécanismes pour rendre accessible l'information relative aux modalités de gestion des renseignements personnels, visant à respecter les principes et obligations légales de PRP, et la diffuser aux personnes au sujet desquelles des renseignements personnels sont consignés et utilisés dans le système d'information.

La transparence à l'égard des modalités de gestion des renseignements personnels se concrétise habituellement par la mise en place de mécanismes facilitant l'accès à l'information et sa diffusion. De façon générale, et plus particulièrement dans le contexte des services en ligne offerts aux citoyens, la diffusion de l'information sur les modalités de gestion des renseignements personnels contribue à renforcer et maintenir la confiance des citoyens à l'égard de l'Administration gouvernementale, ainsi qu'à les inciter à utiliser des moyens électroniques pour obtenir des services.

Dans le cas où une personne désirerait obtenir de l'information complémentaire sur les modalités de gestion des renseignements personnels ou faire part de ses préoccupations sur les façons de faire d'un organisme public à cet égard, elle peut s'adresser au responsable de la PRP de cet organisme.

La Loi sur l'accès prévoit des modalités d'information des citoyens. Un organisme public doit notamment :

- Informer la personne auprès de qui les renseignements sont recueillis (article 65) ;

  Se référer à la pratique PS 1.5 Déterminer les modalités de collecte des renseignements personnels.

- Constituer, maintenir à jour et rendre accessible à toute personne qui en fait la demande un registre des communications de renseignements personnels effectuées sans le consentement des personnes concernées (articles 67.3, 67.4) ;

  Se référer à la sous-pratique n° 2 de la pratique PS 5.3 Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité, lorsque des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public.

- Établir des fichiers de renseignements personnels et les déclarer à la CAI (articles 71, 76 et 77) ;

  Se référer à la pratique PS 8.1 Constituer et maintenir à jour un inventaire des fichiers de renseignements personnels créés ou transférés dans le nouveau système ou modifiés dans le système existant et les déclarer à la Commission d'accès à l'information (CAI).

- Déposer les ententes de communications de renseignements personnels à des tiers, effectuées selon les articles 68 et 68.1, ainsi que l'avis de la CAI à l'Assemblée nationale et publier les ententes dans la Gazette officielle du Québec (article 70).

  Se référer à la pratique PS 5.2 Évaluer les situations où des renseignements personnels seront communiqués à des tiers à l'extérieur de l'organisme public.

Toutefois, afin de faire connaître aux citoyens et à ses employés la façon dont il gère les renseignements qu'il détient, respecte les principes de PRP et s'acquitte de l'ensemble de ses obligations légales à cet égard, il est souhaitable qu'un organisme public prenne d'autres initiatives qui complètent celles énoncées dans la loi. Ainsi, cette pratique est présentée comme un complément aux obligations de la Loi sur l'accès.

Produits de travail types (biens livrables types)

1. Information à diffuser sur les modalités de gestion des renseignements personnels.

   Le formulaire de déclaration de fichiers, dans la mesure où il est complet et à jour, décrit sommairement les modalités de gestion des renseignements personnels tout au long de leur cycle de vie. Il constitue un outil de départ pour recenser les modalités de gestion des renseignements personnels pour chacun des fichiers de renseignements personnels.

   Se référer à la pratique PS 8.1 Constituer et maintenir à jour un inventaire des fichiers de renseignements personnels créés ou transférés dans le nouveau système ou modifiés dans le système existant et les déclarer à la Commission d'accès à l'information (CAI).

2. Plan de diffusion de l'information sur les modalités de gestion des renseignements personnels.

3. Document de diffusion de l'information sur les modalités de gestion des renseignements personnels. Ce document peut être produit sur différents médias.

Sous-pratiques

1. Déterminer l'information, portant sur les modalités de gestion des renseignements personnels du système d'information, qui sera diffusée aux personnes pour lesquelles des renseignements personnels sont consignés et utilisés dans le système d'information.

   Il s'agit de déterminer quelle information sera diffusée aux personnes concernées par les renseignements personnels consignés dans le système d'information, afin de les informer des modalités que l'organisme met en œuvre pour assurer la protection des renseignements personnels dans ce système. Ceci inclut l'information sur leurs droits d'accès et de rectification et sur la procédure à suivre pour faire part à l'organisme public de toute question reliée aux modalités de gestion des renseignements personnels mises en œuvre au sein de celui-ci.

   Une partie de l'information provient des choix spécifiques de gestion de la PRP reliés à ce système, alors qu'une autre partie de l'information provient des politiques et orientations gouvernementales de PRP ou de celles de l'organisme public. La diffusion de cette information contribue à maintenir et à accroître la confiance des personnes envers l'organisation.

   Lorsque l'information doit être diffusée à un utilisateur externe, il y aura lieu de ne pas préciser certaines mesures spécifiques de sécurité en place (nom des produits, pratiques internes, etc.). En effet, certains renseignements reliés aux mesures de sécurité sont susceptibles de constituer un élément de vulnérabilité pour l'organisme s'ils sont portés à la connaissance de personnes mal intentionnées.

Par ailleurs, dans la mesure où un système s'insère dans un service « à guichet unique » ou « grappe de services » composé de plusieurs systèmes, il existe habituellement un mode de fonctionnement préétabli du service « à guichet unique » ou de la « grappe de services ». Il y aura donc lieu d'en tenir compte lorsque l'on établira quel type d'information sera diffusée relativement au système d'information concerné.

De même, lorsque des modifications importantes sont apportées à la protection des renseignements personnels dans le contexte d'un système d'information existant (nouvelle utilisation, par exemple), il y a lieu de souligner ce changement de façon à ce que les utilisateurs puissent en prendre connaissance facilement.

Par la suite, il y aura lieu de recenser l'information disponible selon les sources énumérées précédemment et de déterminer l'information à produire, le cas échéant.

Il est important de faire le choix des modes de diffusion de l'information très tôt dans le processus, car cela constitue un facteur déterminant dans l'usage du contenu et de son organisation.

2. Établir un plan de diffusion de l'information sur les modalités de gestion des renseignements personnels.

   Il s'agit de déterminer les modalités de diffusion de l'information ainsi que les activités à réaliser et de planifier la diffusion de l'information sur les modalités de gestion des renseignements personnels. Voici des éléments à prendre en compte dans l'élaboration du plan de diffusion :

   - les personnes responsables de l'élaboration et de la réalisation du plan de diffusion de l'information ;
   - les ressources humaines, financières, matérielles et technologiques requises ;
   - l'échéancier ;
   - les personnes auprès de qui l'information sera diffusée ;
   - le contenu de l'information (disponible et à produire) et des messages à diffuser ;
   - les règles éditoriales et de présentation compatibles avec les orientations gouvernementales, de l'organisme ou du système d'information ;
   - la forme sous laquelle l'information sera diffusée.

EXEMPLE

Les informations peuvent être diffusées dans le site Web de l'organisme public :

- capsules de PRP du système d'information accessibles automatiquement aux personnes qui consultent le site ;
- énoncé de politique sur la PRP, dans le cadre de l'obtention de services par voie électronique ou de demande d'information, indiquant les mesures de PRP prises tout au long du cycle de vie des renseignements personnels ;
- nom(s) de la (ou des) personne(s) désignée(s) responsable(s) de l'accès et de la PRP et ses (ou leurs) coordonnées, ainsi que celles d'autres personnes-ressources au sein de l'organisme (désignées à titre de répondant de la Loi sur l'accès) et à qui les demandes doivent être adressées ;
- marche à suivre pour faire une demande d'accès et de rectification et les droits de recours auprès de l'organisme ou de la Commission d'accès à l'information (CAI) ;
- marche à suivre pour obtenir de l'information ou faire part de certaines questions sur les modalités de gestion des renseignements personnels ;
- énoncé de politique globale de PRP pour l'ensemble de l'organisme public ;
- déclaration de services aux citoyens ;
- déclaration des valeurs et orientations éthiques de l'organisme public ;
- références sur la PRP (hyperliens avec les sites Web de la CAI, du MRCI et d'autres sites d'intérêt sur la PRP).

Ces informations peuvent aussi être diffusées par d'autres moyens, tels que :

- des dépliants ou autres documents transmis aux personnes concernées ;
- dans la publicité associée au service offert ;
- dans le rapport annuel de gestion ;
- dans des publications de l'organisme public.

Consultez à ce sujet le *Cadre de diffusion de l'information gouvernementale*, destiné aux personnes qui ont à concevoir et à administrer un site Web gouvernemental. Ce document fixe les balises d'un cadre de diffusion de l'information gouvernementale de nature publique sur les inforoutes et prévoit la diffusion d'une politique de confidentialité sur le site Web de l'organisme. Vous pouvez consulter ce document à l'adresse suivante : http://www.webmaestro.gouv.qc.ca/ress/cadre/Cadre/cadre.htm#obj

3. Produire l'information à diffuser sur les modalités de gestion des renseignements personnels.

   Compléter l'information manquante et éditer l'information à diffuser selon le format et le style appropriés retenus dans le plan de diffusion. Il est important de noter que même si l'information est disponible, il est nécessaire de la rédiger dans un langage clair et accessible au public. De plus, il peut y avoir un besoin de créer une information nouvelle. Cette information peut prendre différentes formes : écrite, sonore, vidéo, audio, etc.

   Se référer également à ce sujet au *Cadre de diffusion de l'information gouvernementale*, rapporté dans l'exemple précédent.

   Publier l'information produite

   Il s'agit essentiellement de transférer l'information rédigée ou réalisée sur le média de diffusion choisi.

4. Diffuser l'information.

   Il s'agit de rendre disponible l'information ainsi publiée lors du déploiement du système d'information.

EXEMPLE

Cela peut consister à « mettre l'information en ligne » pour un service en ligne ou distribuer un dépliant pour une information sur un support papier.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 2.8

DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques spécifiques de PRP qui seront réalisées dans le projet pour atteindre le but spécifique BS 8 (colonne « À faire »)
- déterminer les dispositions légales qui y sont associées (colonne « Article de loi »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts/coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe G – Produits de travail types (biens livrables types) des buts spécifiques
- annexe F – Pratiques spécifiques, sous-pratiques et dispositions légales
- tableau 1 – Légende des rôles des parties prenantes dans un projet de développement
- tableau 2 – Légende des responsabilités des parties prenantes dans un projet de développement

LÉGENDE DES SYMBOLES À UTILISER

ARTICLE DE LOI : insérer le numéro de l'article et le titre de la loi associés à cette pratique

---

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N/A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable de la sécurité de l'information . . . . . .RS
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Pilote de projet . . . . . .PP
Répondant du processus de PRP dans le projet . . . .RPPP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié . . . . . .P
En cours de réalisation . . . . . .ER
En suspens . . . . . .ES
Réalisé . . . . . .Ré
Approuvé . . . . . .A

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 1 – RÉALISER LA PRP	BS 8	DIFFUSER L'INFORMATION SUR LA GESTION DES RENSEIGNEMENTS PERSONNELS

AIDE-MÉMOIRE nº 2.8 DÉTERMINER LES PRATIQUES SPÉCIFIQUES DE PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	Nº	Article de loi	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
								Début	Fin	Prévus	Réels
Constituer et maintenir à jour un inventaire des fichiers de renseignements personnels créés ou transférés dans le nouveau système ou modifiés dans le système existant et les déclarer à la Commission d'accès à l'information (CAI)	PS 8.1										
Diffuser l'information sur les modalités de gestion des renseignements personnels	PS 8.2										

Partie 2 Gérer la PRP dans les projets de développement

La Partie 2 décrit, selon une approche d'amélioration continue, un ensemble de buts et de pratiques de gestion qu'un organisme public peut réaliser dans un projet particulier ou un ensemble de projets de développement. La PRP est abordée selon une perspective de gestion, soit la planification, l'organisation, le suivi et le contrôle du processus de PRP, tant à l'échelle d'un projet que de tous les projets de l'organisation. La Partie 2 propose un chemin à suivre pour faciliter l'intégration de la PRP dans la culture de l'organisation relativement aux projets de développement.

Après avoir effectué un survol rapide du Modèle à l'aide du *Guide de lecture de l'ensemble du Modèle* (page XVII), le mode de lecture de la Partie 2 décrit ci-après permet :

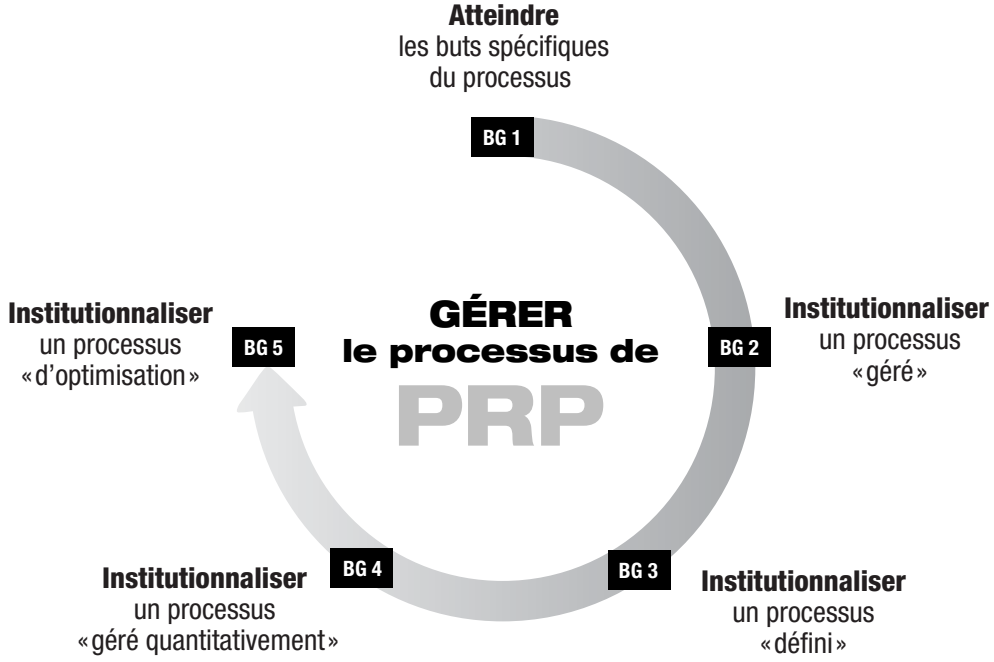
- d'aborder l'intégration de la PRP dans les projets de développement selon une perspective de gestion ;
- d'établir la stratégie d'intégration du Modèle dans l'organisme public ou le projet ;
- de prendre connaissance des composants du Modèle qui ont trait à la gestion de la PRP ;
- de déterminer les buts et les pratiques de gestion (de la PRP) à réaliser dans l'organisme ou le projet ;
- de déterminer les rôles et les responsabilités des intervenants ;
- de faire une lecture détaillée des buts et pratiques de gestion (de la PRP) pour comprendre les pratiques à réaliser et identifier les adaptations à faire selon la stratégie d'intégration retenue.

MODE DE LECTURE SUGGÉRÉ AFIN DE FACILITER LA GESTION DE LA PRP

1. Lire le chapitre : *Comment intégrer le Modèle dans l'organisme public ?* (p. 13 à 22).
2. Lire l'*aide-mémoire n° 3.1 – Déterminer les buts de gestion de la PRP à atteindre dans le projet* (p. 198 et 199).
3. Consulter le *Schéma de la Partie 2 – Gérer la PRP dans les projets de développement* (p. 108) pour déterminer les pratiques à examiner en fonction des buts retenus.
4. Lire le chapitre : *Composants du Modèle – Partie 2* (p. 110 à 117).
5. Lire les pratiques correspondantes et les *aide-mémoire nos 4.1 à 4.5 Déterminer les pratiques de gestion de la PRP à réaliser dans le projet* (p. 117 à 155), pour déterminer les pratiques de gestion à réaliser et établir l'adaptation à faire, le cas échéant.

SCHÉMA DE LA PARTIE 2

Gérer la protection des renseignements personnels (PRP) dans les projets de développement



BG 1 **Atteindre les buts spécifiques du processus**

Niveau de capacité 1

PG 1.1 Réaliser les pratiques spécifiques

BG 2 **Institutionnaliser un processus «géré»**

Niveau de capacité 2

PG 2.1 Établir une politique

PG 2.2 Planifier le processus

PG 2.3 Fournir les ressources

PG 2.4 Assigner la responsabilité

PG 2.5 Former le personnel

PG 2.6 Gérer les configurations

PG 2.7 Identifier et faire participer les parties prenantes pertinentes

PG 2.8 Suivre et contrôler

PG 2.9 Évaluer objectivement la conformité

PG 2.10 Passer en revue l'état d'avancement avec la haute direction

BG 3 **Institutionnaliser un processus «défini»**

Niveau de capacité 3

PG 3.1 Établir un processus «défini»

PG 3.2 Recueillir l'information d'amélioration

BG 4 **Institutionnaliser un processus «géré quantitativement»**

Niveau de capacité 4

PG 4.1 Établir des objectifs quantitatifs

PG 4.2 Stabiliser la performance des sous-processus

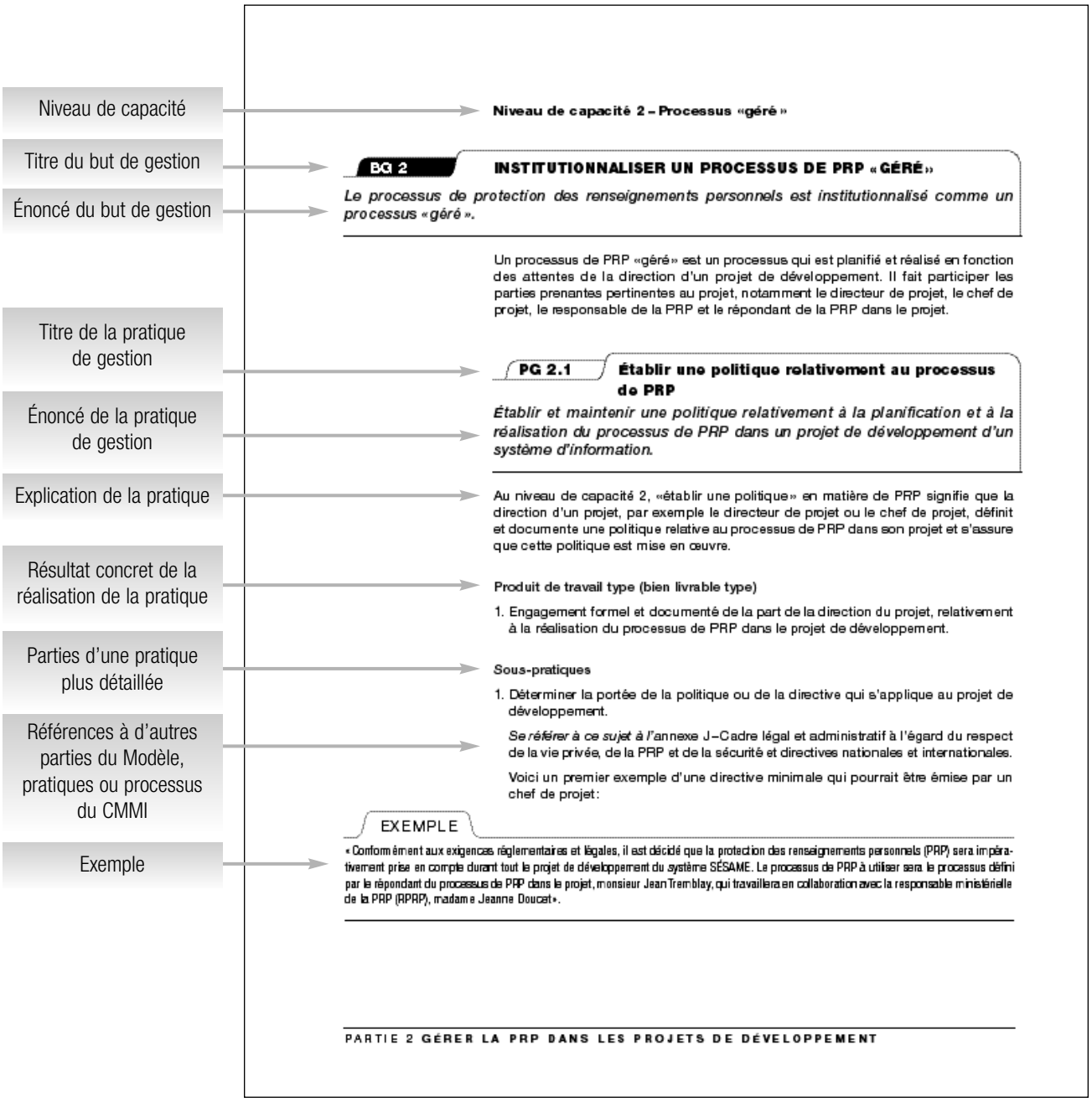
BG 5 **Institutionnaliser un processus «d'optimisation»**

Niveau de capacité 5

PG 5.1 S'assurer de l'amélioration continue

PG 5.2 Corriger les principales causes des problèmes

EXEMPLE DE LECTURE – PARTIE 2



COMPOSANTS DU MODÈLE – PARTIE 2

Ce chapitre décrit les définitions et conventions de représentation des différents composants du Modèle, pour la Partie 2. Ces composants sont similaires aux composants de la Partie 1. Ils comprennent des buts et pratiques de gestion, au lieu des buts et pratiques spécifiques de la Partie 1, lesquelles se détaillent, comme pour la Partie 1, par des explications, des produits de travail types (ou biens livrables types) découlant de la réalisation des pratiques, des sous-pratiques, qui viennent expliciter une pratique, des définitions, des exemples de pratiques et des références. À la différence de la Partie 1, on retrouve dans la Partie 2 du Modèle un nouveau composant, soit le niveau de capacité. Ajoutés aux composants de la Partie 1, ces composants sont représentés dans la figure 5 qui suit :

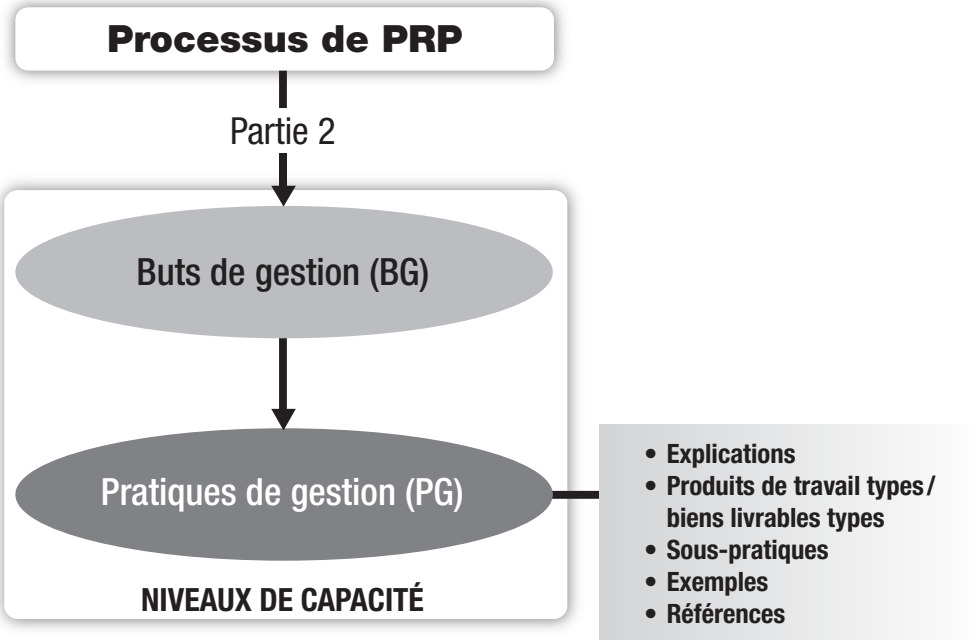


Figure 5 *Composants du processus de PRP – Partie 2 du Modèle*

Pour la Partie 2, la définition et la convention de représentation des composants du Modèle traitent uniquement des composants comportant des différences par rapport aux composants de la Partie 1. Il s'agit de se référer, pour les composants identiques, à leur définition et convention de représentation qui se retrouvent dans la Partie 1 du Modèle.

PROCESSUS DE PRP

Un processus est un ensemble de pratiques regroupées par buts qui, lorsqu'elles sont réalisées, permettent d'atteindre les buts considérés comme étant importants pour réaliser ce processus.

Dans le contexte de la PRP, le processus de PRP comprend un ensemble de pratiques de PRP regroupées par buts. Dans la Partie 1, les buts et pratiques sont qualifiés de spécifiques, car ils touchent une dimension propre à la PRP dans les projets de développement. Dans la Partie 2, les buts de gestion sont au nombre de cinq et correspondent aux cinq des six niveaux de capacité possibles. Ces niveaux de capacité correspondent aux différents modes de réalisation et de gestion que l'organisme public désire appliquer pour réaliser le processus de PRP.

Se référer au schéma de la Partie 2 – Gérer la PRP dans les projets de développement *apparaissant précédemment pour une illustration des niveaux de capacité*.

Ces buts et pratiques sont caractérisés « de gestion » et ils correspondent aux buts et pratiques génériques de gestion proposés dans le modèle de référence CMMI, pouvant s'appliquer à tout processus relié au développement des systèmes d'information et donc, au processus de PRP.

Par exemple, le but de gestion *BG 2 Institutionnaliser un processus de PRP « géré »* et les pratiques de gestion qui s'y rattachent font appel à un mode de gestion qui peut être appliqué à tout processus réalisé lors du développement des systèmes d'information, incluant le processus de PRP.

BUTS DE GESTION

Chaque but de gestion s'applique à un seul niveau de capacité (1 à 5) et correspond à un mode distinctif de réalisation ou de gestion du processus de PRP. Chaque mode de gestion distinctif représente un niveau de gestion « institutionnalisé » qu'un organisme public désire appliquer pour gérer son processus de PRP. Le terme « institutionnalisé » réfère au degré selon lequel l'organisme a intégré ce processus de PRP dans ses activités régulières de développement et au degré de contrôle ou de maîtrise de son processus de PRP.

L'atteinte d'un but de gestion de plus en plus élevé signifie une gestion améliorée du processus de PRP dans sa planification, sa mise en œuvre et son contrôle. Le niveau du but de gestion indique si le processus de PRP est vraisemblablement efficace, répétable et durable, traduisant ainsi son niveau d'intégration dans la culture de l'organisme public relativement au développement des systèmes d'information.

Les buts de gestion sont intrinsèquement liés à l'atteinte des buts spécifiques. On peut atteindre les buts de gestion de la PRP et réaliser les pratiques associées à ces buts dans la mesure où les buts spécifiques de PRP sont en voie d'être atteints.

En somme, on peut gérer le processus de PRP dans la mesure où un tel processus est en voie d'être réalisé. Ainsi, il est pratiquement impossible d'atteindre le but de gestion *BG 2 Institutionnaliser un processus de PRP « géré »* si les buts spécifiques de PRP ne sont pas en voie d'être atteints.

Les buts de gestion de la PRP sont présentés de façon similaire aux buts spécifiques décrits dans la Partie 1 du Modèle. Ils sont numérotés BG 1 à BG 5.

PRATIQUES DE GESTION

Une pratique de gestion (de la PRP) est une activité ou un ensemble d'activités importantes pour atteindre le but de gestion (de la PRP) associé. Les pratiques de gestion décrivent les activités devant permettre d'atteindre les buts de gestion d'un processus.

Comme dans tout processus basé sur le modèle de référence CMMI, le processus de PRP comprend dix-sept (17) pratiques de gestion. Ces pratiques constituent une proposition d'activités à réaliser pour atteindre le but associé à ces pratiques. Ce sont les pratiques de gestion que l'on retrouve normalement dans un organisme public pour atteindre un but de gestion.

Étant donné que le Modèle n'est pas un document normatif, les pratiques de gestion, tout comme les pratiques spécifiques, demeurent des propositions de pratiques pour la PRP. L'organisme public peut réaliser une « pratique équivalente » différente de la pratique proposée, mais qui permet d'atteindre quand même le but associé à la pratique.

Il est important de souligner qu'une pratique de gestion sera réalisée, bien sûr, par du personnel en situation de gestion, comme le chef de projet (qui assigne les responsabilités), mais aussi par le personnel administratif (qui donne la formation) et le personnel technique (qui gère la configuration).

Les pratiques de gestion sont présentées d'une façon similaire aux pratiques spécifiques décrites dans la Partie 1 du Modèle. Elles sont numérotées PG 1.1 à PG 5.2.

NIVEAUX DE CAPACITÉ

Les niveaux de capacité correspondent à des phases d'accomplissement dans la réalisation et la gestion du processus de PRP. Les niveaux de capacité réfèrent à la croissance, au sein de l'organisation, de la capacité de réalisation et de contrôle, permettant d'améliorer sa performance par rapport au processus de PRP.

Chacun des niveaux de capacité correspond à l'une des phases d'accomplissement. Il existe six niveaux de capacité, désignant chacun un état atteint pour le processus de PRP :

- niveau 0 – processus incomplet ;
- niveau 1 – processus « réalisé » ;
- niveau 2 – processus « géré » ;
- niveau 3 – processus « défini » ;
- niveau 4 – processus « géré quantitativement » ;
- niveau 5 – processus « d'optimisation ».

Ces niveaux de capacité servent à organiser les composants de la Partie 2 du Modèle. Un niveau de capacité donné comprend un seul but de gestion (par exemple BG 2) et un ensemble de pratiques de gestion (par exemple PG 2.1 à PG 2.10). Le tableau 4 suivant résume les relations entre les niveaux de capacité, les buts et les pratiques de gestion.

TABLEAU 4 *Relations entre les niveaux de capacité, les buts et les pratiques de gestion*

NIVEAU DE CAPACITÉ	ÉTAT DU PROCESSUS	BUT DE GESTION	PRATIQUES DE GESTION
0	Incomplet	Aucun	Aucune n'est possible tant que les pratiques spécifiques de la Partie 1 du Modèle ne sont pas en voie d'être réalisées
1	Réalisé	BG 1	PG 1.1 : réaliser les pratiques spécifiques de la Partie 1 du Modèle
2	Géré	BG 2	PG 2.1 à PG 2.10
3	Défini	BG 3	PG 3.1 et PG 3.2
4	Géré quantitativement	BG 4	PG 4.1 et PG 4.2
5	D'optimisation	BG 5	PG 5.1 et PG 5.2

Les niveaux de capacité 0 et 1 ont trait au degré d'atteinte des buts spécifiques de PRP ou au degré de réalisation des pratiques spécifiques de PRP. Les niveaux de capacité 2 à 5 ont trait au degré de gestion appliqué au processus de PRP.

Sommairement, on peut définir les niveaux de capacité de la façon suivante :

Niveau de capacité 0 – Processus incomplet

Cela signifie que les buts spécifiques pertinents du processus de PRP définis à la Partie 1 du Modèle ne sont pas entièrement atteints dans l'ensemble des projets de développement de l'organisme public. Par « but spécifique pertinent », on entend un but spécifique qui s'applique au projet concerné. Ainsi, si un projet ne comporte pas de communication de renseignements personnels à des tiers, le but spécifique *BS 5 Communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public* ne s'applique pas et n'est pas pertinent.

Niveau de capacité 1 – Processus « réalisé »

Cela signifie que tous les buts spécifiques pertinents (BS 1 à BS 8) sont atteints dans l'ensemble des projets de développement de l'organisme public.

Niveau de capacité 2 – Processus « géré »

Cela signifie que les pratiques de gestion associées au but de gestion du niveau de capacité 2 sont réalisées et donc, que le but de gestion BG 2 est atteint dans l'ensemble des projets de développement de l'organisme public. Cela signifie également que le processus de PRP est géré : sa réalisation est planifiée, suivie et contrôlée.

Niveau de capacité 3 – Processus « défini »

Cela signifie que les pratiques de gestion associées au but de gestion du niveau de capacité 3 sont réalisées et que le but de gestion BG 3 est atteint dans l'ensemble des projets de développement de l'organisme public.

Cela signifie également que le processus de PRP est géré et défini : l'organisme public possède un processus de PRP standard et il est en mesure d'appliquer ce processus standard dans chaque projet de développement. Ainsi, un processus de PRP est « défini » en adaptant le processus de PRP standard de l'organisme selon des règles d'adaptation proposées par celui-ci. Le résultat de l'adaptation est un processus de PRP modulé à chaque projet particulier.

Il importe de souligner qu'une adaptation peut signifier tout simplement de faire le choix de ne réaliser aucune adaptation au processus standard et de l'utiliser tel quel. Ce choix ne peut se faire qu'après avoir pris connaissance du processus standard de l'organisme public et de ses règles d'adaptation, à la lumière des exigences du projet de développement concerné.

Niveau de capacité 4 – Processus « géré quantitativement »

Cela signifie que les pratiques de gestion associées au but de gestion du niveau de capacité 4 sont réalisées et que le but de gestion BG 4 est atteint dans l'ensemble des projets de développement de l'organisme public.

Cela signifie également qu'une fois le niveau de capacité 3 atteint, l'organisme dispose d'un processus de PRP standard qui est utilisé dans l'ensemble de ses projets. Il peut alors commencer à gérer quantitativement son processus de PRP, car les mesures et statistiques accumulées (sur le coût, les efforts, le délai, la qualité, etc.) sont comparables : elles proviennent de projets qui ont utilisé un processus de PRP semblable, sinon identique.

Niveau de capacité 5 – Processus « d'optimisation »

Cela signifie que les pratiques de gestion associées au but de gestion de la PRP du niveau de capacité 5 sont réalisées et que le but de gestion BG 5 est atteint dans l'ensemble des projets de développement de l'organisme public.

Cela signifie également qu'une fois le niveau de capacité 4 atteint (processus géré quantitativement), il est possible d'apporter des améliorations au processus de PRP et de pouvoir évaluer leur impact sur une base quantitative. Même si l'organisme public peut apporter des améliorations à son processus de PRP à n'importe quel niveau de capacité, c'est seulement au niveau de capacité 5 qu'il peut apprécier de façon quantitative l'incidence d'une amélioration sur son processus de PRP en termes de coût, de qualité et de délai, par exemple.

Dans la Partie 2 du Modèle les niveaux de capacité résultent d'un effet cumulatif des niveaux inférieurs. Ainsi, un niveau de capacité 3 atteint signifie que ce niveau a été atteint, de même que les niveaux inférieurs à 3. On se base sur les acquis de l'atteinte d'un niveau pour atteindre le suivant. Ceci est illustré par la figure 6 qui suit :

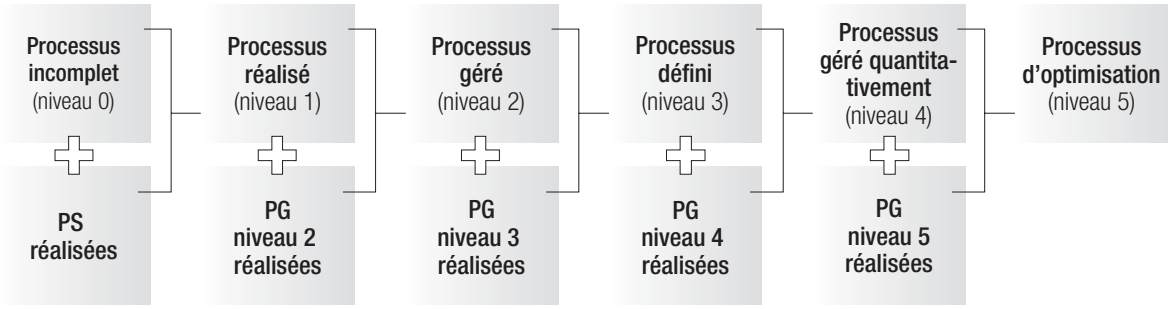


Figure 6 *Interrelations entre les niveaux de capacité*

Les niveaux de capacité proposent donc un chemin d'amélioration du processus de PRP. Ils fournissent un ordre recommandé d'amélioration continue.

PRODUITS DE TRAVAIL TYPES (BIENS LIVRABLES TYPES)

Les produits de travail types associés aux pratiques spécifiques de PRP sont tous énumérés dans la Partie 1 du Modèle. Par contre, les produits de travail types associés aux pratiques de gestion ne sont pas tous énumérés explicitement dans la Partie 2 du Modèle. En effet, il arrive que les produits de travail types de certaines pratiques de gestion correspondent à des produits de travail types déjà définis dans d'autres processus du modèle de référence CMMI. Afin de ne pas répéter ce qui est déjà défini dans le modèle de référence CMMI, des références à des processus précis de ce modèle sont souvent fournies en guise de produits de travail types. Les produits de travail types des pratiques de gestion comprennent donc des énumérations à des niveaux de détail variés selon les trois cas suivants :

- Certaines pratiques de gestion peuvent inclure, comme c'est le cas pour les pratiques spécifiques, tous les produits de travail types associés. C'est le cas des pratiques de gestion PG 2.1 à PG 2.5 et PG 2.10.
- D'autres pratiques de gestion, soit les PG 2.6 à PG 2.9, comportent une énumération de certains produits de travail types à titre d'illustration et une référence à un ou plusieurs autre(s) processus du modèle de référence CMMI, où les produits de travail types correspondants sont déjà déterminés. C'est le cas par exemple de la pratique de gestion *PG 2.7 Identifier et faire participer les parties prenantes pertinentes au processus de PRP*, où deux produits de travail types sont énumérés et une référence à des processus du modèle de référence CMMI est fournie. La formulation utilisée pour ce cas est illustrée dans la pratique de gestion PG 2.7 :

  « Pour réaliser les produits de travail du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans les processus "*Planification de projet*" et "*Suivi et contrôle de projet*". Cependant, il convient de souligner ces produits de travail types :

  1. Demandes documentées de participation.
  2. Engagements de participation ».
- Enfin, les pratiques de gestion associées aux buts de gestion BG 3, BG 4 et BG 5 comprennent uniquement une référence aux produits de travail types contenus dans des processus du modèle de référence CMMI. Une formulation standardisée des produits de travail types est utilisée pour les décrire et se présente comme suit, dans la pratique de gestion *PG 3.1 Établir un processus de PRP « défini »* :

  « Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus "*Gestion de projet intégrée*" ».

SOUS-PRATIQUES

Dans la Partie 2, les pratiques de gestion ne comportent pas toutes des sous-pratiques. Les sous-pratiques sont absentes d'une pratique de gestion dans l'un des deux cas suivants :

- lorsque la pratique de gestion ne nécessite pas d'être expliquée davantage en sous-pratiques, telle la pratique de gestion *PG 2.3 Fournir les ressources pour le processus de PRP ;*
- lorsque la pratique de gestion nécessiterait de copier littéralement des pratiques ou sous-pratiques se retrouvant dans d'autres processus du modèle de référence CMMI, telle la pratique de gestion *PG 2.6 Gérer les configurations du processus de PRP*.

RÉFÉRENCES

Les pratiques spécifiques peuvent présenter des interrelations à l'intérieur d'un même but spécifique ou entre des buts spécifiques différents. De même, les pratiques de gestion du processus de PRP peuvent présenter des interrelations, mais cette fois avec d'autres processus reliés au développement des systèmes d'information et définis dans le modèle de référence CMMI. C'est pourquoi les pratiques de gestion comportent des références à des processus externes, mais complémentaires au processus de PRP. Deux types d'interrelations avec des processus externes peuvent se présenter :

- **Certaines pratiques de gestion dépendent du soutien d'un processus particulier.** La pratique de gestion *PG 2.6 Gérer les configurations du processus de PRP* en est un exemple. Le processus « Gestion des configurations » offre un soutien à la réalisation de cette pratique de gestion. Cela signifie que le processus « Gestion des configurations » pourrait être mis en œuvre entièrement ou partiellement afin de réaliser cette pratique de gestion du processus de PRP.
- **Certaines autres pratiques de gestion ne peuvent pas être réalisées sans avoir obtenu au préalable le résultat d'un autre processus.** La pratique de gestion *PG 3.1 Établir un processus de PRP « défini »* en est un exemple. Cette pratique de gestion requiert au préalable l'existence d'un processus standard de l'organisation pour, notamment le processus de PRP. Ce processus standard aura été établi auparavant lors de la réalisation du processus « Définition du processus de l'organisation » décrit dans le modèle de référence CMMI. C'est à partir de ce processus standard de PRP de l'organisation qu'il sera possible de définir un processus de PRP modulé pour un projet donné.

  Pour les organismes publics qui n'utilisent pas le CMM ou le CMMI, mais qui désirent positionner leur processus de PRP à un niveau de gestion (que ce soit au niveau de capacité 2, 3, 4 ou 5), les références à un processus externe au présent Modèle peuvent en fait correspondre à un processus interne existant (ou en devenir) au sein de l'organisme public.

Ainsi, même si la pratique de gestion *PG 2.2 Planifier le processus de PRP* réfère au processus *Planification de projet* du CMMI, l'organisme public peut tout aussi bien référer à son propre processus de « gestion de projet », qui inclut la phase de planification de projet. La référence permet de souligner, dans cet exemple, que le résultat de cette pratique de gestion servira à compléter le plan de projet qui est réalisé dans un processus intitulé *Planification de projet*. Ces références fournissent une indication précieuse pour l'organisme public qui désire intégrer les pratiques de ce Modèle dans son environnement de développement et de gestion de projet, qu'il utilise ou non le CMM ou le CMMI.

Il est important de rappeler que le CMMI contient des processus reliés au développement de systèmes qui sont le résultat d'un large consensus international. Les noms des processus référencés peuvent varier d'un organisme à l'autre, mais l'essence même de ces processus se retrouve dans tout environnement de développement et de gestion de projet qui supporte un certain niveau de maîtrise dans la réalisation et la gestion.

Les autres références à d'autres documents ou à une annexe du Modèle sont identiques à la Partie 1 du Modèle.

COMPOSANTS ASSOCIÉS À UNE OBLIGATION LÉGALE

Aucun composant de la Partie 2 du Modèle n'est associé à une obligation légale.

PRATIQUES DE GESTION (PG) PAR BUT (BG) ET NIVEAUX DE CAPACITÉ

Ce chapitre débute par la description des processus dont il y a lieu de tenir compte dans un projet de développement, mais qui ne sont pas décrits dans le *Modèle de pratiques de PRP*. Il comprend par la suite la description des buts et pratiques de gestion ainsi que les produits de travail types (ou biens livrables types). Afin de faciliter l'atteinte de chacun des cinq buts de gestion, des gabarits ou aide-mémoire complètent la description des pratiques.

PROCESSUS RELIÉS

Le *Modèle de pratiques de PRP* se limite à la réalisation et à la gestion des pratiques relatives à la protection des renseignements personnels qui sont caractéristiques de ce domaine. Cependant, il ne faut pas en déduire que la PRP, lors du développement de système, est entièrement couverte par les pratiques spécifiques décrites à la Partie 1 ou par les pratiques de gestion qui sont décrites dans cette Partie 2.

La prise en charge complète de la PRP, dans le développement d'un système d'information et dans la gestion de projet, exige que d'autres pratiques soient mises en application. Ces pratiques ne sont pas décrites dans le présent Modèle, car elles le sont déjà dans le modèle qui a servi de base de référence pour la structuration des pratiques, soit le modèle de référence CMMI. Elles sont présentées à titre de référence dans la Partie 2 qui traite des pratiques de gestion.

Pour les organismes publics qui n'utilisent pas le CMMI, il s'agit de transposer ces références dans leur propre environnement de développement et de gestion de projet.

Le processus de gestion des risques représente un processus important de la PRP. Étant donné qu'il est déjà défini dans le modèle de référence CMMI, il ne se retrouve pas dans le *Modèle de pratiques de PRP*. Il y est tout simplement indiqué à titre de référence.

Ainsi, ce n'est pas parce qu'un processus ne se retrouve pas défini dans le *Modèle de pratiques de PRP* que ce processus n'est pas important pour prendre en charge complètement la PRP dans un projet de développement. De plus, il sera important de tenir compte des particularités de la PRP lorsque les processus auxquels on fait référence seront réalisés.

Lors de la réalisation du processus de planification de projet, il sera important de tenir compte des exigences de la PRP découlant des pratiques du *Modèle de pratiques de PRP* et des autres processus auxquels il fait référence, afin d'établir le temps requis et le budget approprié.

Dans la Partie 2 du Modèle, les références à d'autres processus sont fournies dans le but de porter deux éléments importants à l'attention des parties prenantes au projet :

- la prise en charge de la PRP est complétée par les autres processus auxquels on fait référence, selon les niveaux de capacité concernés ;
- il importe de tenir compte de façon explicite de l'exigence de la PRP lors de la réalisation de ces autres processus.

Les principaux processus du CMMI auxquels il est fait référence dans le *Modèle de pratiques de PRP* sont décrits dans les lignes qui suivent. Les processus du CMMI pertinents à la PRP se retrouvent également indiqués à l'intérieur des pratiques de gestion.

Se référer aux processus « Gestion des exigences et Développement des exigences » pour plus d'information sur la façon dont les exigences sont prises en compte dans le développement d'un système d'information, en considérant que la PRP est associée à plusieurs obligations légales, constituant ainsi une exigence pour tout système d'information.

Se référer aux processus « Planification de projet, Suivi et contrôle de projet » pour plus d'information sur le plan de projet, afin de tenir compte des différentes exigences d'un système d'information, en considérant que la PRP constitue une des dimensions à prendre en compte lors de l'élaboration du plan de projet, de son suivi et de son contrôle.

Se référer au processus « Assurance qualité du processus et du produit » pour plus d'information sur l'assurance qualité à appliquer, notamment à la PRP et au produit développé, acquis ou maintenu.

Se référer au processus « Gestion des risques » pour plus d'information sur la façon dont les différentes catégories de risques, incluant celle reliée à la PRP, sont prises en compte.

NIVEAU DE CAPACITÉ 0 – PROCESSUS INCOMPLET

Un processus de PRP incomplet est un processus qui n'est pas réalisé ou qui n'est que partiellement réalisé. Un ou plusieurs des buts spécifiques du processus de PRP décrits dans la *Partie 1 – Réaliser la PRP dans les projets de développement* n'est pas ou ne sont pas atteint(s). Dans un organisme public, le niveau de capacité 0 relié au processus de PRP signifie que sur l'ensemble de ses projets, il possède au moins un projet où les buts spécifiques pertinents de PRP (décrits dans la Partie 1 du Modèle) ne sont pas tous atteints.

NIVEAU DE CAPACITÉ 1 – PROCESSUS « RÉALISÉ »

Ce niveau de capacité, qualifié de « réalisé », correspond à la réalisation des pratiques spécifiques décrites dans la Partie 1 du Modèle, permettant d'atteindre tous les buts spécifiques de PRP. Toutefois, la différence fondamentale avec les pratiques spécifiques demeure la perspective de réalisation de ces pratiques, soit une perspective de réalisation pour l'ensemble des projets de développement de l'organisme public. Au niveau de capacité 1, l'organisme public réalise donc les pratiques spécifiques du processus de PRP pour l'ensemble de ses projets.

BG 1 ATTEINDRE LES BUTS SPÉCIFIQUES DU PROCESSUS DE PRP

Le processus de PRP soutient et rend possible l'atteinte des buts spécifiques de PRP par la réalisation des produits de travail types (biens livrables types) de PRP.

La réalisation des pratiques spécifiques, présentées dans la Partie 1 Réaliser la PRP dans les projets de développement, permet d'atteindre les buts spécifiques du processus de PRP (BS 1 à BS 8) couvrant tout le cycle de vie de la protection des renseignements dans tous les projets de développement des systèmes d'information de l'organisme public.

*Se référer à l'*aide-mémoire n° 1.1 Déterminer les buts spécifiques de PRP à atteindre dans le projet, *afin de déterminer sommairement, dès les études préliminaires du projet, les buts spécifiques de PRP à atteindre dans le système d'information développé ou modifié, en fonction du cheminement projeté des renseignements personnels*.

PG 1.1 Réaliser les pratiques spécifiques du processus de PRP

Réaliser les pratiques spécifiques du processus de PRP afin de développer les produits de travail et de fournir les services attendus pour atteindre les buts spécifiques de PRP.

Le but de cette pratique de gestion est de réaliser les produits de travail types (ou biens livrables types) et de fournir les services découlant de la réalisation de toutes les pratiques spécifiques du processus de PRP. En fait, cette pratique signifie que, contrairement au niveau de capacité 0 où aucune ou seulement certaines des pratiques spécifiques sont réalisées, le niveau de capacité 1 signifie que chacune des pratiques spécifiques du processus de PRP est réalisée. Bien sûr, une pratique équivalente peut être réalisée à la place d'une pratique spécifique attendue, du moment qu'elle permet d'atteindre le but associé à la pratique.

Les pratiques spécifiques peuvent être réalisées de façon informelle, sans suivre une description documentée de processus ou un plan documenté. La rigueur avec laquelle ces pratiques sont réalisées dépend des personnes qui gèrent et réalisent le travail et elle peut varier considérablement autant d'un projet à l'autre qu'à l'intérieur d'un même projet.

Même si le niveau de capacité 1 peut apparaître comme un niveau de capacité faible dans l'échelle de capacité, ce niveau demeure quand même exigeant pour un organisme public, car il nécessite que soient atteints non seulement les buts spécifiques associés à une obligation légale, mais aussi tous les autres buts spécifiques de tout le cycle de vie de la protection des renseignements personnels (BS 1 à BS 8). Cela inclut la réalisation de toutes les pratiques spécifiques (ou des pratiques équivalentes) associées ou non à des dispositions légales (PS 1.1 à PS 8.2). Ce niveau constitue la base de la réalisation des pratiques spécifiques du processus de PRP, à partir duquel un organisme public pourra tabler pour mettre en place des mécanismes de gestion lui permettant de maîtriser de plus en plus son processus de PRP.

L'atteinte de ce niveau de capacité 1 représente donc un premier jalon franchi pour l'organisme public qui désire poursuivre cette évolution ou cette amélioration continue vers les niveaux supérieurs de capacité, soit vers un niveau de maîtrise supérieure des coûts, des délais et de la qualité du processus de PRP mis en place.

EXEMPLE

Au niveau de capacité 1, les pratiques de PRP sont réalisées sans qu'elles soient planifiées ou suivies. Ainsi, dans un projet donné, un organisme fonctionnant selon le niveau de capacité 1 ignore quand elles seront complétées réellement et quel en sera leur coût réel de réalisation.

On pourra cependant constater qu'elles ont toutes été réalisées.

Se référer aux buts spécifiques et aux pratiques spécifiques PS 1.1 à PS 8.2.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 4.1

DÉTERMINER LES PRATIQUES DE GESTION DE LA PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques de gestion qui seront réalisées dans le projet pour atteindre le but de gestion BG 1 (colonne « À faire »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts / coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe H – Produits de travail types (biens livrables types) des buts de gestion

LÉGENDE DES SYMBOLES À UTILISER

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N / A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Haute direction . . . . . .HD
Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Répondant du processus de PRP dans le projet . . . .RPPP
Pilote de projet . . . . . .PP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié . . . . . .P
En cours de réalisation . . . . . .ER
En suspens . . . . . .ES
Réalisé . . . . . .Ré
Approuvé . . . . . .A

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 2 – GÉRER LA PRP	NIVEAU DE CAPACITÉ 1 BG 1	ATTEINDRE LES BUTS SPÉCIFIQUES DU PROCESSUS DE PRP

AIDE-MÉMOIRE nº 4.1 DÉTERMINER LES PRATIQUES DE GESTION DE LA PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	Nº	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
							Début	Fin	Prévus	Réels
Réaliser les pratiques spécifiques du processus de PRP	PG 1.1									

NIVEAU DE CAPACITÉ 2 – PROCESSUS « GÉRÉ »

À partir du niveau de capacité 2 jusqu'au niveau de capacité 5, le terme « institutionnaliser » est utilisé pour décrire chacun des buts associés aux niveaux 2 à 5. Ce terme représente une notion de base importante des pratiques de gestion du processus de PRP. Le terme « institutionnalisation » correspond à l'élaboration et au renforcement des méthodes, pratiques et procédures soutenues par la culture d'un organisme public, de sorte qu'elles deviennent la façon courante de fonctionner. En d'autres mots, cela signifie que c'est une façon de faire répandue dans toute l'organisation ou une partie de l'organisation et suivie ou intériorisée par chacune des personnes de l'organisation. Cette notion d'institutionnalisation au regard des niveaux de capacité se traduit concrètement par la réalisation des pratiques décrites à chacun de ces niveaux.

Ainsi, « institutionnaliser un processus géré » au niveau de capacité 2 signifie que le personnel de chaque projet de l'organisme public réalise le processus de PRP selon une façon gérée, soit en le planifiant, en le réalisant, en le suivant et en le contrôlant selon le plan établi. Le processus de PRP ainsi géré devient une partie intégrale de la culture de l'organisme public.

Cependant, contrairement aux niveaux 3, 4 et 5, l'institutionnalisation au niveau de capacité 2 s'effectue projet par projet : chaque projet gère son processus de PRP, mais de façon non uniforme. On peut donc retrouver, au niveau de capacité 2, beaucoup de variations du processus de PRP d'un projet à l'autre dans un même organisme public. Ce ne sera qu'à partir du niveau 3 qu'on aura une institutionnalisation au niveau de tout un organisme public, c'est-à-dire que l'organisme public aura une façon standardisée de « gérer » un processus.

Dans la réalité des organismes publics, cette distinction de niveaux n'est pas aussi nette. Ainsi, un organisme public peut avoir un processus de PRP standardisé utilisé uniquement dans certains de ses projets. Il peut également utiliser une partie seulement du processus standardisé de PRP dans tous ses projets. Les pratiques du processus de PRP peuvent donc chevaucher deux niveaux de capacité.

BG 2 INSTITUTIONNALISER UN PROCESSUS DE PRP « GÉRÉ »

Le processus de protection des renseignements personnels est institutionnalisé comme un processus « géré ».

Description du processus de PRP :

Une expression documentée d'un ensemble d'activités réalisées pour atteindre un objectif tel que « respecter les principes et les obligations légales de PRP » et fournissant une définition opérationnelle des composants majeurs du processus de PRP.

Un processus de PRP « géré » est un processus qui est planifié et réalisé en fonction des attentes de la direction d'un projet de développement d'un système d'information et des orientations de PRP établies relativement à ce projet. Ces attentes et orientations peuvent également être établies par la haute direction de l'organisme pour un projet particulier. Il convient de rappeler que le terme « développement » inclut, comme dans la Partie 1 du Modèle, à la fois « développement » et « modification ».

Un processus de PRP « géré » se traduit par la mise en place d'une infrastructure permettant d'institutionnaliser, c'est-à-dire d'établir de manière officielle ou formelle, un processus afin que la PRP soit réalisée dans un projet de développement d'un système d'information ayant recours à des renseignements personnels, et ce :

- dès le début d'un projet de développement d'un nouveau système d'information ou de modification d'un système d'information existant ;
- tout au long du cycle de développement ou de modification jusqu'à son déploiement.

Partie prenante :

Groupe ou individu concerné ou d'une certaine façon imputable du résultat d'un projet. Les parties prenantes au projet peuvent inclure des membres du projet, des fournisseurs, des clients, des utilisateurs et d'autres personnes.

Partie prenante pertinente :

Terme utilisé pour désigner une partie prenante qui est identifiée pour une participation dans certaines activités du projet et qui est incluse dans un plan approprié. Ainsi, même s'il y a dix parties prenantes pour le processus de PRP, il n'y en aura peut-être que deux qui seront pertinentes pour participer à la réalisation d'une activité donnée. Il serait en effet inefficace de faire participer toutes les parties prenantes à toutes les activités.

Établir et maintenir :

Ce terme signifie définir, documenter, utiliser ou mettre en œuvre dans toute l'organisation. Au niveau 2, l'organisation se limite à le faire projet par projet et non pas de façon standardisée pour tous ses projets.

Il est important de rappeler qu'un système d'information comprend autant une partie administrative qu'une partie automatisée.

Le processus de PRP « géré » est planifié et exécuté avec la participation du personnel qualifié pour produire les résultats attendus en PRP. Des ressources adéquates assurent leur réalisation, leur suivi et leur contrôle.

Il fait participer les parties prenantes pertinentes au projet, notamment le directeur de projet, le chef de projet, le responsable de la PRP et le répondant de la PRP dans le projet. Le processus de PRP mis en œuvre dans le projet est documenté, suivi, contrôlé et passé en revue et il est évalué quant à sa conformité à la description de processus de PRP qui a été établi pour le projet.

Les pratiques de niveau de capacité 2 permettent de gérer la réalisation des pratiques spécifiques de PRP et de fournir ainsi à la direction du projet une vision du processus de PRP et de son état d'avancement selon des jalons prédéterminés.

PG 2.1 Établir une politique relativement au processus de PRP

Établir et maintenir une politique relativement à la planification et à la réalisation du processus de PRP dans un projet de développement d'un système d'information.

Au niveau de capacité 2, « établir une politique » en matière de PRP signifie que les hautes autorités de l'organisme ou la direction d'un projet, par exemple le directeur de projet ou le chef de projet, définissent et documentent une politique relative au processus de PRP dans un projet particulier. La direction d'un projet s'assure que cette politique est mise en œuvre.

Le but de cette pratique de gestion est :

- d'établir les attentes organisationnelles relativement à la réalisation du processus de PRP, dans un projet particulier de développement d'un système d'information ou de modification d'un système d'information existant, qui impliquent des renseignements personnels ;
- de les diffuser aux personnes concernées ; et
- de faire en sorte qu'elles soient bien comprises et mises en œuvre.

Cette pratique de gestion vise donc avant tout à ce que le directeur du projet s'engage formellement à réaliser le processus de PRP dans son projet et prenne les mesures nécessaires à sa mise en œuvre. Cet engagement peut prendre la forme d'orientations, d'une politique ou d'une directive sur la PRP. Il n'est pas nécessaire que cet engagement soit nommé « politique » ; tout autre terme conviendra dans la mesure où il correspond à un tel engagement ou orientation et qu'il est mis en œuvre.

Il est important de noter que la seule existence d'une telle politique ne suffit pas. Il faut s'assurer qu'elle est appliquée ou « maintenue » dans le projet pour que cette pratique soit accomplie.

EXEMPLE

La diffusion de cette politique peut également se faire de différentes façons et s'insérer dans le plan de communication du projet. La communication des orientations en matière de PRP peut se faire lors d'un discours du directeur du projet avant son lancement, dans une politique écrite ou au moyen de tout autre document.

Produits de travail types (biens livrables types)

1. Engagement formel et documenté de la part de la direction du projet relativement à la réalisation du processus de PRP dans le projet de développement.
2. Plan de communication et de diffusion des orientations, de la politique ou de la directive sur la PRP dans le projet de développement.

Sous-pratiques

1. Déterminer la portée de la politique ou de la directive relativement au processus de PRP dans le projet de développement.

   La politique ou la directive est élaborée en fonction du cadre administratif, légal ou réglementaire relié à la PRP de l'organisme public et du projet concerné.

   *Se référer à ce sujet à l'*annexe J – Cadre légal et administratif à l'égard du respect de la vie privée, de la PRP et de la sécurité et directives nationales et internationales.

2. Obtenir l'approbation de la direction du projet.
3. Établir un plan de communication et diffuser la politique ou la directive sur la PRP qui s'applique au projet de développement.

EXEMPLE

Directive minimale qui pourrait être émise par un chef de projet :

« Conformément aux exigences réglementaires et légales, il est décidé que la protection des renseignements personnels (PRP) sera impérativement prise en compte durant tout le projet de développement du système SÉSAME. Le processus de PRP à utiliser sera le processus défini par le répondant de la PRP dans le projet, monsieur Jean Tremblay, qui travaillera en collaboration avec la responsable ministérielle de la PRP (RPRP), madame Jeanne Doucet. Monsieur Tremblay prendra comme base le niveau de capacité 2 du *Modèle de pratiques de PRP*, produit par le ministère des Relations avec les citoyens et de l'Immigration (MRCI). Monsieur Tremblay vous tiendra informé du processus de PRP à suivre dès qu'il sera disponible. Vous pouvez vous référer à lui pour toute question entourant la PRP. Monsieur Tremblay me tiendra régulièrement au courant, lors de la revue périodique, du projet et de son évolution en matière de PRP. Je pourrai intervenir au besoin pour toute question entourant ce sujet. Je compte donc sur la collaboration de chacun et chacune d'entre vous pour faire en sorte que, durant toutes les phases du projet, et ce, dès le début, les principes et obligations légales de PRP soient pris en compte et respectés. »

Si vous désirez obtenir un autre exemple de politique, consultez *La politique sur la protection des actifs informationnels*, Commission de la santé et de la sécurité au travail disponible à l'adresse suivante : http://www.csst.qc.ca/publications/pdf/dc200-1144.pdf

PG 2.2 Planifier le processus de PRP

Établir et maintenir le plan pour réaliser le processus de protection des renseignements personnels.

Objectifs d'amélioration du processus de PRP :

Un ensemble de caractéristiques cibles établi afin de guider l'effort d'amélioration du processus de PRP existant, d'une façon spécifique mesurable, soit en termes de caractéristiques du produit résultant (ex. : qualité, rendement, conformité aux normes), soit de la façon dont le processus est réalisé (ex. : fusion d'étapes du processus, amélioration de la durée du cycle).

Le but de cette pratique de gestion est de déterminer les exigences qui doivent être satisfaites pour réaliser le processus de PRP et atteindre les objectifs d'amélioration de celui-ci, de préparer un plan pour sa réalisation et sa description et, enfin, d'obtenir un accord sur le plan de la part des parties prenantes pertinentes au projet.

Les exigences reliées au processus de PRP découlent de la politique ou directive établie pour ce projet, ainsi que des principes et obligations légales de PRP.

Se référer à la pratique de gestion PG 2.1 Établir une politique relativement au processus de PRP *et à l'*annexe J – Cadre légal et administratif à l'égard du respect de la vie privée, de la PRP et de la sécurité et directives nationales et internationales.

Exigence reliée au processus de PRP :

Représentation documentée d'une condition ou d'une capacité relative au processus.

Les buts spécifiques de PRP à atteindre lors de la mise en œuvre du processus de PRP, ainsi que les objectifs particuliers liés à l'amélioration de ce processus, sont établis par le directeur ou le chef du projet en collaboration avec le répondant de la PRP dans le projet et le responsable de la PRP de l'organisme public. Ils dépendent notamment du type de projet et ils peuvent inclure des préoccupations de qualité, de coût ou de délai de réalisation.

Ainsi, lors de la planification du processus de PRP dans un projet, on tiendra compte, d'une part, du cheminement projeté des renseignements personnels. Cela permettra de déterminer les buts spécifiques à atteindre et les pratiques et biens livrables à réaliser.

EXEMPLE

On développe un système d'information où tout le cycle de vie de la PRP est couvert, à l'exception de la phase consistant à communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme. Ainsi, le plan de processus de PRP couvrira les buts BS 1 à BS 5, BS 7 et BS 8, de même que les pratiques et biens livrables qui y sont associés. Le but spécifique *BS 5 Communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public* ne figurera pas dans le plan, car il n'y a aucune communication de renseignements personnels projetée.

D'autre part, on établira des objectifs visant à améliorer la qualité du processus de PRP dans ce projet.

EXEMPLE

Objectif :

réduction du coût de réalisation du processus de PRP dans ce projet par rapport à une réalisation antérieure d'un tel processus.

Le plan du processus de PRP est élaboré de façon à prendre en compte tout le cycle de vie de la protection des renseignements personnels pertinent pour le projet. Il est enclenché dès les études préliminaires et intégré dans la structure et dans le plan de gestion de projet. Ainsi, le chef de projet arrimera le plan du processus de PRP au plan global du projet.

L'établissement d'un plan du processus de PRP permet de produire un document officiel, documenté et approuvé par les autorités compétentes du projet. Il vise à soutenir la gestion (planification, suivi et contrôle) du processus de PRP dans le projet. Il est basé sur les exigences de PRP que le projet doit satisfaire. Ce plan est évolutif, c'est-à-dire qu'il est ajusté au fur et à mesure de la progression du projet et de la précision des exigences de PRP pour ce projet.

Gestion des risques :

Un processus organisé et analytique destiné à identifier la source d'un dommage ou d'une perte (ou identifier les risques), évaluer et quantifier les risques identifiés, développer et, au besoin, mettre en œuvre une approche appropriée visant à prévenir ou traiter les causes des risques.

Une évaluation des risques du projet sur la PRP pourra accompagner les demandes d'approbation des projets de développement des systèmes d'information qui mènent à la collecte, à la consignation et au traitement des renseignements personnels.

À cet égard, il sera opportun d'inclure de façon explicite la dimension de la PRP dans le processus de gestion des risques du projet. Le plan de réalisation du processus de PRP sera mis à jour, au besoin, à la suite de la production du rapport d'évaluation des risques et du plan de gestion des risques en matière de PRP.

Se référer au processus de « Gestion des risques » et au processus « Planification de projet » pour obtenir plus d'information sur la façon dont les différentes catégories de risques et les différentes stratégies de mitigation des risques, incluant celles reliées à la PRP, sont prises en compte.

Les ministères et les organismes gouvernementaux peuvent consulter la version française du processus de « Gestion des risques » version 1.1 dans l'intranet du Secrétariat du Conseil du trésor sur la gestion des risques :
www.inforoute-gouvernementale.qc/risquesaccueil.htm

La version anglaise est accessible à tous sur le site Web du Software Engineering Institute à l'adresse suivante : www.sei.cmu.edu/cmmi

Pour obtenir plus d'information sur des méthodologies d'évaluation des incidences d'un projet sur la PRP (« Privacy impact assessment »), vous pouvez consulter une liste de références dans la section Documentation du site du MRCI :
http://www.aiprp.gouv.qc.ca/autre/index.asp?Sect=Documentation

En matière de « *Gestion des ententes avec les fournisseurs* », il est important, par ailleurs, que la direction du projet inclut ses exigences particulières en matière de processus de PRP dans les cahiers de charge et les contrats confiés à des fournisseurs, qu'ils soient internes au gouvernement ou externes.

Il sera donc opportun d'inclure de façon explicite la dimension de la PRP dans le processus de « Gestion des ententes avec les fournisseurs ».

*Se référer à l'article 67.2 de la Loi sur l'accès et aux pratiques d'assurance qualité du processus de « Gestion des ententes avec les fournisseurs » pour s'assurer de la mise en œuvre des mesures de PRP par une personne, une entreprise privée ou un organisme public, dans le cadre de l'exercice d'un mandat ou de l'exécution d'un contrat de services. Consultez à ce sujet à l'*annexe L – Clause type de protection des renseignements personnels.

EXEMPLE

Des exigences pour les fournisseurs peuvent figurer dans les cahiers de charge. Elles peuvent s'appliquer dans les cas où l'organisme public projette de développer ou modifier un nouveau système d'information ou encore de faire usage d'un logiciel ou d'une solution d'affaires disponibles commercialement, à des fins d'intégration.

Exigences :

- le fournisseur doit préciser, dans la méthodologie qu'il propose pour développer le système d'information, comment les exigences du processus de PRP seront prises en compte dans les phases du projet qu'il réalisera ;
- le fournisseur doit préciser les mesures qui seront prises pour respecter le caractère confidentiel des renseignements personnels auxquels il aura accès lors du développement du système d'information.

En bref, la réalisation de cette pratique permet de planifier la réalisation de l'ensemble du processus de PRP dans un projet. Elle permet de déterminer, d'une part, de quelle façon les pratiques spécifiques ou des pratiques équivalentes et les produits de travail types (biens livrables types) permettant d'atteindre les buts spécifiques BS1 à BS 8, qui s'appliquent au projet, seront réalisés. D'autre part, elle permet de déterminer de quelle façon les activités visant l'amélioration du processus de PRP seront réalisées.

Produit de travail type (bien livrable type)

1. Plan de réalisation du processus de PRP intégré dans le manuel d'organisation et de gestion du projet.

   Le plan de réalisation du processus de PRP inclut typiquement les éléments suivants :

   - la description du processus de PRP, cette description peut se baser sur les pratiques spécifiques décrites dans la Partie 1 du Modèle (PS 1.1 à PS 8.2) ;
   - les standards pour les produits de travail et les services du processus de PRP ;
   - les exigences pour les produits de travail et les services du processus de PRP ;
   - les objectifs particuliers de performance du processus de PRP (par exemple : la qualité, la période, la durée et l'utilisation des ressources) ;
   - les interrelations entre les activités, les produits de travail et les services du processus de PRP ;
   - les personnes et les ressources (incluant le financement et les outils) nécessaires à la réalisation du processus de PRP ;
   - l'assignation de la responsabilité et de l'autorité ;
   - la formation nécessaire pour réaliser et soutenir le processus de PRP ;
   - les produits de travail à placer sous le contrôle de la gestion de configuration et le niveau de gestion de configuration pour chacun de ces produits ;
   - les exigences de mesure pour offrir « une vue » sur la performance du processus, ses produits de travail et ses services ;
   - l'implication des parties prenantes pertinentes ;
   - les activités pour suivre et contrôler le processus de PRP ;
   - les activités d'évaluation objective du processus de PRP et de ses produits de travail ;
   - les activités de revue, par la direction, du processus de PRP et de ses produits de travail.

Services du processus de PRP :

Une pratique comprend la réalisation d'un ensemble d'activités permettant de produire les biens livrables et les services attendus. À la différence des biens livrables qui comportent un caractère statique, les services sont des processus utilisables à la suite de la réalisation d'une pratique (par exemple un programme de formation). Un service exige la participation d'une personne (et quelques fois l'utilisation d'un logiciel) pour qu'il puisse être offert. Il revêt un caractère dynamique, participatif.

Sous-pratiques

1. Définir et documenter la description du processus de PRP.

   La description du processus de PRP, incluant les standards et procédures pertinents, peut faire partie du plan de réalisation du processus de PRP ou peut être uniquement référencée dans ce plan de réalisation.

   Se référer aux buts spécifiques BS 1 à BS 8 et aux pratiques spécifiques correspondantes.

   *Se référer à l'*aide-mémoire n° 1.1 Déterminer les buts spécifiques de PRP à atteindre dans le projet *de l'*annexe I – Aide-mémoire complémentaires *afin de déterminer sommairement, dès les études préliminaires du projet, les buts spécifiques de PRP à atteindre dans le système d'information développé, en fonction du cheminement projeté des renseignements personnels*.

2. Définir et documenter le plan pour la réalisation du processus de PRP.

   La réalisation du processus de PRP est décrite, la façon dont ce processus est intégré à la gestion du projet est exposée, les rôles et les responsabilités sont présentés et le budget attribué à la PRP est réparti entre les activités des différentes phases de gestion du projet : le suivi, le contrôle et la communication.

Voici quelques éléments à considérer :

- les pratiques spécifiques de PRP sont prises en compte à chaque phase de développement du projet et pour chaque bien livrable du projet concerné par la PRP ;
- les ressources requises (incluant les personnes, les budgets et les outils) pour réaliser le processus de PRP sont déterminées dès le début ;
- le plan de réalisation du processus de PRP est intégré dans le plan de gestion du projet. Se référer aux buts spécifiques de PRP, BS 1 à BS 8, aux pratiques spécifiques correspondantes et aux produits de travail types (biens livrables types) à réaliser. Une attention particulière sera accordée aux pratiques associées à une obligation légale.

Se référer aux processus « Gestion des exigences » et « Développement des exigences » pour obtenir plus d'information sur la façon dont les exigences sont prises en compte, sachant que la PRP constitue une obligation légale et, donc, une exigence pour tout système d'information.

Se référer aux processus « Planification de projet » et « Suivi et contrôle de projet » pour plus d'information sur le plan de projet, afin de tenir compte des différentes exigences d'un système d'information, sachant que la PRP doit obligatoirement être prise en compte lors de l'élaboration du plan de projet, de son suivi et de son contrôle.

*Se référer à l'*aide-mémoire n° 3.2 Déterminer les rôles et responsabilités des intervenants à l'égard de la gestion de la PRP dans le projet *de l'*annexe I – Aide-mémoire complémentaires *pour préciser les rôles et responsabilités des parties prenantes au projet*.

3. Passer en revue le plan avec les parties prenantes pertinentes au projet et obtenir leur approbation.

   Ceci inclut de passer en revue le plan afin de s'assurer, avec les parties prenantes pertinentes, que le processus planifié est conforme aux politiques, plans, exigences et standards applicables.

4. Réviser le plan au besoin.

PG 2.3 Fournir les ressources pour le processus de PRP

Affecter des ressources adéquates pour réaliser le processus de protection des renseignements personnels, développer les produits de travail et fournir les services associés à ce processus.

Le but de cette pratique de gestion est de s'assurer que les ressources nécessaires sont affectées à la réalisation du processus de PRP, tel qu'il est défini dans le plan, et sont disponibles lorsqu'elles sont requises. Ces ressources incluent un financement approprié, des installations physiques, des outils adéquats ainsi que des personnes qualifiées.

Il est important que les membres de l'équipe de projet soient appuyés concrètement dans leurs activités liées à la PRP, tant au plan des ressources financières et matérielles que de l'appui manifesté par la direction du projet lorsque des mesures et des solutions concernant la PRP sont proposées.

Une personne qualifiée pour réaliser le processus de PRP est désignée à titre de répondant de la PRP dans le projet. Elle fait partie à part entière de l'équipe de projet. Elle travaille en étroite collaboration avec le RPRP de l'organisation et elle participe à toutes les phases du projet.

Produit de travail type (bien livrable type)

1. Description des ressources requises pour réaliser le processus de PRP et indication du moment où elles sont requises : financement, personnes, installations physiques et outils appropriés.

PG 2.4 Assigner la responsabilité du processus de PRP

Assigner la responsabilité et l'autorité aux personnes pour réaliser le processus de PRP, développer les produits de travail et fournir les services associés au processus de protection des renseignements personnels.

Le but de cette pratique de gestion est de s'assurer que, dans le projet, l'obligation de rendre compte de la réalisation du processus de PRP et de l'atteinte des résultats spécifiés a été formellement établie. Les personnes désignées doivent avoir le niveau d'autorité approprié pour assumer la responsabilité qui leur est assignée.

EXEMPLE

La responsabilité peut être assignée en référant à des descriptions de tâches ou à des documents tels que le manuel de gestion du projet.

Une assignation dynamique de la responsabilité, soit une assignation juste à temps et non pas longtemps d'avance pour éviter les changements d'assignation, est une autre façon de réaliser cette pratique de gestion, et ce, aussi longtemps que l'assignation et la prise en charge de la responsabilité sont assurées durant tout le processus de PRP.

Il y aura lieu de tenir compte, pour chaque projet, des rôles déjà établis pour ce qui est notamment du responsable de la PRP de l'organisme public et des autres personnes œuvrant dans ce domaine.

Produits de travail types (biens livrables types)

1. Désignation d'une personne pour assurer la réalisation des produits de travail types (biens livrables types) relatifs à la PRP dans le cadre du projet et en rendre compte (répondant de la PRP dans le projet).
2. Description des rôles et des responsabilités des autres parties prenantes pertinentes au processus de PRP.

Sous-pratiques

1. Assigner la responsabilité et attribuer l'autorité requise pour réaliser le processus de PRP, ainsi que l'obligation d'en rendre compte.

La fonction de répondant de la PRP dans le projet est assignée à une personne qui détient l'autorité requise. Cette personne s'assure de la réalisation des produits de travail types (biens livrables types) de PRP, coordonne les activités supportant leur réalisation dans le projet et en rend compte à la direction du projet. De même, les personnes ou les groupes de personnes pouvant intervenir dans le cas de problématiques qui soulèvent des enjeux particuliers de PRP sont identifiés.

EXEMPLE

Les cas où la réalisation de certaines pratiques de PRP ou de biens livrables implique des coûts importants qui n'avaient pas été prévus initialement sont soumis au directeur de projet ou à un comité stratégique.

Dans d'autres cas, lors de la planification du processus de PRP, s'il n'y a pas de consensus quant à l'importance de réaliser telle pratique de PRP, cela peut être soumis, notamment au comité directeur du projet, à la personne responsable de la PRP de l'organisme public ou à des conseillers juridiques.

2. Assigner la responsabilité pour réaliser les tâches spécifiques du processus de PRP.

   *Se référer à l'*aide-mémoire n° 3.2 Déterminer les rôles et responsabilités des intervenants à l'égard de la gestion de la PRP dans le projet *de l'*annexe I – Aide-mémoire complémentaires, *pour préciser les rôles et responsabilités des parties prenantes au projet*.

3. Confirmer que les personnes désignées comprennent et acceptent les responsabilités et l'autorité qui leur sont assignées.

PG 2.5 Former le personnel relativement au processus de PRP

Former, au besoin, le personnel ayant à réaliser ou soutenir le processus de protection des renseignements personnels.

Le but de cette pratique de gestion est de s'assurer que les personnes ont la qualification et l'expertise nécessaires pour réaliser le processus de PRP dans le projet ou offrir un soutien lors de sa réalisation.

L'établissement d'un programme de formation ou de sensibilisation à la PRP vise à développer les compétences et les connaissances des personnes pour qu'elles puissent jouer efficacement le rôle qui leur a été assigné.

Bien que la formation et la sensibilisation soient une responsabilité organisationnelle, chaque projet de réalisation d'un processus de PRP donne lieu à l'identification des compétences essentielles à sa réalisation et inclut, au besoin, la formation et la sensibilisation requises pour répondre aux exigences particulières correspondantes.

Produits de travail types (biens livrables types)

1. Description des compétences requises du personnel pour réaliser le processus de PRP.
2. Plan de sensibilisation et de formation et sa diffusion.

Sous-pratiques

1. Déterminer les compétences requises des membres de l'équipe de projet qui participent à la réalisation du processus de PRP.

   Cela permet de définir les besoins de sensibilisation et de formation à la PRP, afin que les membres de l'équipe puissent jouer efficacement leur rôle respectif.

2. Produire le contenu des sessions de formation et de sensibilisation.
3. Planifier et organiser les activités de formation et de sensibilisation.
4. Diffuser l'information sur la PRP lors des sessions de formation et de sensibilisation aux membres de l'équipe de projet et aux autres parties prenantes pertinentes afin qu'ils soient aptes à jouer leur rôle à cet égard.
5. Fournir des ressources adéquates pour la réalisation des sessions de formation et de sensibilisation.
6. Évaluer la qualité des programmes de formation et de sensibilisation et l'atteinte des résultats visés.

PG 2.6 Gérer les configurations du processus de PRP

Placer les produits de travail désignés du processus de protection des renseignements personnels sous les niveaux appropriés de gestion de configuration.

Gestion des configurations :

Processus visant à établir et maintenir l'intégrité des produits de travail composant un système d'information. Ce processus permet ainsi de gérer la description technique des différents éléments composant un système d'information et des évolutions qui sont successivement apportées à cette description et aux différents exemplaires de ces éléments.

L'objectif de cette pratique de gestion est d'établir et de maintenir un mode d'organisation des produits de travail du processus de PRP (ou leur description) de manière à ce que leur intégrité soit maintenue tout au long de leur cycle de vie utile.

Dans un projet de développement, un système d'information comprend un ensemble d'éléments (dont le nombre peut s'élever à plusieurs centaines, voire des milliers dans des projets d'envergure) dans des états variés de développement (par exemple, version brouillon, version mise à l'essai, version approuvée, etc.). La gestion des configurations permet de pouvoir réaliser l'assemblage d'une version entière ou partielle d'un système d'information à partir des différents éléments devant le composer et de pouvoir aussi conserver une trace (concept de traçabilité) de l'évolution de certains éléments jugés importants.

EXEMPLE

À tout moment, dans un projet, il doit être possible de connaître quels sont les éléments qui composent exactement la version du système d'information dans sa phase d'essai et aussi de pouvoir retracer, à partir de la fonctionnalité implantée dans cette version, la documentation reliée à cette fonctionnalité.

Si des renseignements personnels se retrouvent dans une fonctionnalité donnée du système, il devrait être possible de retracer la bonne version du bien livrable associée à cette fonctionnalité. Cette version fournit le résultat du « test de nécessité » des renseignements personnels et explique les raisons de la présence de tel renseignement personnel dans cette fonctionnalité du système. De plus, le système de gestion de configuration devrait pouvoir nous indiquer où se retrouve physiquement cette documentation, qu'elle soit sous la forme papier ou numérique, et qui peut y avoir accès.

En matière de gestion de configuration, tous les éléments composant le système en développement n'ont pas la même importance. Aussi, un niveau approprié de gestion de configuration sera appliqué pour chacun d'eux selon les choix qui auront été faits par le répondant de la PRP dans le projet, en collaboration avec le responsable de la gestion de configuration du projet.

EXEMPLE

Pour des biens livrables intermédiaires qui ne sont pas fournis au client, il ne sera pas nécessaire de conserver tous les historiques de versions relatifs à ces biens livrables, car ils ne seront probablement pas utiles dans la version de production ou lors de la phase de modification du système.

Par contre, certains autres biens livrables jugés de grande importance pour le projet, comme le résultat du « test de nécessité » des renseignements personnels, peuvent faire l'objet d'une gestion de configuration plus serrée, en exigeant notamment une vérification ou une approbation du responsable de la PRP de l'organisme ou du répondant de la PRP dans le projet avant de passer d'une version préliminaire de travail à une version finale.

De plus, on pourra conserver tous les historiques de ce bien livrable afin de pouvoir s'y référer, au besoin, et de comprendre pourquoi certaines informations se retrouvent dans le système d'information, alors que d'autres n'y figurent pas.

La réalisation de cette pratique de gestion s'effectue par les parties prenantes pertinentes, notamment le responsable de la gestion des configurations du projet et le répondant de la PRP dans le projet.

Se référer au processus « Gestion des configurations » pour obtenir plus d'information à ce sujet.

Produits de travail types (biens livrables types)

Pour réaliser les produits de travail du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Gestion des configurations », où le niveau de gestion de configuration approprié pourra être établi. Cependant, il convient de souligner ces produits de travail types :

1. Liste des éléments de configuration
2. Historique de révision des éléments de configuration

PG 2.7 Identifier et faire participer les parties prenantes pertinentes au processus de PRP

Identifier et faire participer les parties prenantes pertinentes au processus de protection des renseignements personnels, tel qu'il est planifié dans le projet.

L'objectif de cette pratique de gestion est d'établir et de maintenir la participation des parties prenantes pertinentes à la réalisation du processus de PRP.

Se référer au processus « Planification de projet » pour obtenir plus d'information.

La planification de la participation des parties prenantes pertinentes dans le processus de PRP vise à ce que les interactions, nécessaires entre les personnes pour réaliser ce processus, se produisent.

Lorsque l'on planifie la participation des parties prenantes, on s'assure que les interactions nécessaires au processus de PRP se produisent, tout en évitant qu'un nombre excessif de personnes ou de groupes de personnes retardent indûment la réalisation du processus de PRP.

Il s'agit de choisir, parmi les parties prenantes au projet, celles qui sont pertinentes pour chacune des activités du projet, c'est-à-dire celles qui peuvent être affectées ou qui peuvent affecter le projet. Le choix s'opère notamment parmi le directeur de projet, le responsable de la PRP de l'organisme public, le répondant de la PRP dans le projet, le spécialiste d'architecture ou de sécurité, le pilote du système, les analystes, les programmeurs, etc.

EXEMPLE

Activités pour faire participer les parties prenantes :

- établissement d'un environnement de collaboration pour une discussion libre et ouverte relativement aux différentes problématiques de PRP soulevées dans le cadre du projet et aux différentes solutions pour les résoudre ;
- résolution des problèmes d'interprétation des obligations légales associées à des pratiques spécifiques de PRP ;
- évaluation des incidences des changements occasionnels des exigences du système d'information sur la PRP ;
- identification des incohérences entre le plan de projet, les produits de travail et les exigences.

Produits de travail types (biens livrables types)

Pour réaliser les produits de travail du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans les processus « Planification de projet » et « Suivi et contrôle de projet ». Cependant, il convient de souligner ces produits de travail types :

1. Demandes documentées de participation des parties prenantes.
2. Engagements de participation.

Sous-pratiques

1. Identifier les parties prenantes au projet dans le processus de PRP et décider quel type de participation sera retenu.
2. Partager cette information, au besoin, avec la ou les personne(s) responsable(s) de la planification.
3. Faire participer les parties prenantes au projet, tel qu'il est planifié.

PG 2.8 Suivre et contrôler le processus de PRP

Suivre et contrôler le processus de PRP par rapport au plan de réalisation et entreprendre les actions correctives appropriées.

L'objectif de cette pratique de gestion est d'effectuer un suivi et un contrôle continus du processus de PRP au regard du plan préalablement établi. Une connaissance appropriée de l'état d'avancement du processus de PRP est maintenue afin d'entreprendre des actions correctives, si cela est nécessaire. Le suivi et le contrôle du processus de PRP impliquent de recueillir des mesures du processus de PRP ou des produits de travail réalisés par ce processus.

EXEMPLE

Mesures de suivi et de contrôle :

- le temps requis pour réaliser certaines pratiques ou sous-pratiques de PRP ;
- les efforts réellement déployés par rapport à la planification en nombre de jours-personnes ;
- le coût réel par rapport au coût estimé pour réaliser les activités de PRP ;
- le taux de changement des exigences ayant une incidence sur la PRP ;
- le degré de couverture des biens livrables de PRP par la revue par les pairs.

Se référer aux processus « Suivi et contrôle de projet » et « Analyse et mesure » afin d'obtenir plus d'information sur le suivi et le contrôle de projet et sur les mesures à utiliser, respectivement.

Produits de travail types (biens livrables types)

Pour réaliser les produits de travail du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans les processus « Suivi et contrôle de projet » et « Analyse et mesure ». Cependant, il convient de souligner ces produits de travail types :

1. Mesures sur la performance du processus.
2. Liste des actions correctives.

Sous-pratiques

1. Mesurer la performance actuelle du processus de PRP par rapport au plan de réalisation.
2. Passer en revue les réalisations et les résultats du processus de PRP par rapport au plan de réalisation.
3. Passer en revue les activités, l'état d'avancement et les résultats du processus de PRP avec la personne qui en est responsable et déterminer les problématiques particulières. Les revues sont destinées à fournir à cette personne une connaissance appropriée du déroulement du processus. Les revues peuvent être à la fois périodiques ou déclenchées ponctuellement selon les événements.
4. Déterminer et évaluer les conséquences des écarts significatifs par rapport au plan de réalisation.
5. Déterminer les problèmes découlant du plan lui-même ou de la réalisation du processus de PRP.
6. Prendre une mesure corrective lorsque les exigences et les objectifs ne sont pas atteints, lorsque des problèmes sont identifiés ou lorsque l'avancement diffère significativement du plan de réalisation du processus de PRP.
7. Suivre les actions correctives jusqu'à ce qu'elles soient complétées.

PG 2.9 Évaluer objectivement la conformité du processus de PRP

Évaluer objectivement la conformité du processus de protection des renseignements personnels réalisé dans le projet, par rapport à la description de ce processus, aux standards et aux procédures et traiter les éléments qui ne sont pas conformes.

L'objectif de cette pratique de gestion est de fournir une assurance à l'effet que le processus de PRP est mis en œuvre tel qu'il est prévu dans le projet et qu'il respecte la description retenue du processus de PRP, ses standards et ses procédures.

Se référer au processus « Assurance qualité du processus et du produit » pour obtenir plus d'information sur l'assurance qualité à appliquer, notamment au processus de PRP et au produit développé, acquis ou maintenu.

Cette pratique est réalisée par du personnel qui n'est pas directement responsable de la gestion ou de la réalisation du processus de PRP. Ainsi, la conformité du processus de PRP dans le projet est évaluée par du personnel de l'organisme qui est externe au processus ou au projet ou encore par une personne externe à l'organisme. Cela permet d'obtenir un niveau d'assurance de conformité à ce qui avait été prévu, et ce, particulièrement dans les cas où le processus de PRP pose un problème (comme dans les cas de retard dans l'échéancier ou de dépassement de budget).

EXEMPLE

Le vérificateur interne de l'organisme pourrait évaluer la conformité du processus de PRP dans le projet.

Dans le cas de divergence d'opinions relativement à la réalisation des exigences de PRP établies comme devant être réalisées dans le projet, on pourra consulter, notamment la personne responsable de la PRP de l'organisme public, les services juridiques ou, le cas échéant, des comités déjà en place.

Il est important de ne pas confondre cette pratique avec toute autre activité réalisée au sein d'un organisme qui viserait à déterminer si telle façon de faire est conforme à une disposition de la Loi sur l'accès.

Si l'on désire faire une telle vérification de conformité légale, il y aura lieu de le prévoir lors de la planification du processus de PRP (voir à ce sujet la pratique de gestion *PG 2.2 Planifier le processus de PRP*) et lors de la réalisation de certaines pratiques spécifiques où la conformité légale est en jeu (voir les pratiques spécifiques des buts spécifiques BS 1 à BS 8 qui sont associées à des dispositions légales).

Produits de travail types (biens livrables types)

Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Assurance qualité du processus et du produit ». Cependant, il convient de souligner ces produits de travail types :

1. Liste des éléments qui ne sont pas conformes au processus de PRP.
2. Résultats découlant d'actions visant à traiter les éléments non conformes, tel un plan ajusté du processus de PRP.

PG 2.10 Passer en revue l'état d'avancement du processus de PRP avec la haute direction

Passer en revue les activités, l'état d'avancement et les résultats du processus de protection des renseignements personnels avec la haute direction et résoudre les éléments problématiques.

Le but de cette pratique de gestion est de faire en sorte que la haute direction soit informée adéquatement de l'état d'avancement du processus de PRP. Ainsi, la haute direction sera en mesure de rendre compte de la PRP dans le projet qui lui a été confié. La haute direction inclut les personnes dont le niveau d'autorité dans l'organisme public est directement au-dessus du répondant de la PRP dans le projet.

Cette revue est réalisée à l'intention des gestionnaires qui, sur un plan hiérarchique supérieur, supervisent et déterminent les orientations du processus de PRP. Elle ne s'adresse pas à ceux qui réalisent les activités courantes de supervision et de contrôle du processus de PRP.

Les gestionnaires, en fonction de leur niveau d'autorité, ont différents besoins d'information par rapport au processus de PRP. Ces revues aident à s'assurer que des décisions éclairées sont prises relativement à la planification et à la réalisation de ce processus.

Les revues de l'état d'avancement du processus de PRP dans le projet sont conduites sur une base périodique ou dans le cas d'un événement particulier. Elles sont réalisées avec les gestionnaires qui détiennent un niveau approprié d'autorité. Cela permet de les informer de l'état d'avancement du processus de PRP et d'entreprendre des actions correctives appropriées.

Produit de travail type (bien livrable type)

1. Compte rendu de la revue, incluant les actions prévues pour résoudre les problèmes soumis à la haute direction.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 4.2

DÉTERMINER LES PRATIQUES DE GESTION DE LA PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques de gestion qui seront réalisées dans le projet pour atteindre le but de gestion BG 2 (colonne « À faire »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts / coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe H – Produits de travail types (biens livrables types) des buts de gestion

LÉGENDE DES SYMBOLES À UTILISER

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N / A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres		Membres de l'équipe de développement	
Haute direction	HD	Directeur de projet	DP
Responsable de la PRP de l'organisme	RPRP	Chef et chargé de projet	CP
Conseiller juridique	CJ	Répondant du processus de PRP dans le projet	RPPP
Vérificateur interne	VI	Pilote de projet	PP
Responsable des méthodes	RM	Autres membres	A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable	R	Valide	Va
Réalise	Ré	Approuve	A
Offre un soutien et conseille	SC	Coordonne	C
Vérifie	Vé		

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié	P	Réalisé	Ré
En cours de réalisation	ER	Approuvé	A
En suspens	ES		

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 2 – GÉRER LA PRP	NIVEAU DE CAPACITÉ 2 BG 2	INSTITUTIONNALISER UN PROCESSUS DE PRP « GÉRÉ »

AIDE-MÉMOIRE nº 4.2 DÉTERMINER LES PRATIQUES DE GESTION DE LA PRP À RÉALISER DANS LE PROJET

Projet : Sous-projet :

Pratiques du Modèle	Nº	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
							Début	Fin	Prévus	Réels
Établir une politique relativement au processus de PRP	PG 2.1									
Planifier le processus de PRP	PG 2.2									
Fournir les ressources pour le processus de PRP	PG 2.3									
Assigner la responsabilité du processus de PRP	PG 2.4									
Former le personnel relativement au processus de PRP	PG 2.5									
Gérer les configurations du processus de PRP	PG 2.6									
Identifier et faire participer les parties prenantes pertinentes au processus de PRP	PG 2.7									
Suivre et contrôler le processus de PRP	PG 2.8									
Évaluer objectivement la conformité du processus de PRP	PG 2.9									
Passer en revue l'état d'avancement du processus de PRP avec la haute direction	PG 2.10									

NIVEAU DE CAPACITÉ 3 – PROCESSUS « DÉFINI »

BG 3 INSTITUTIONNALISER UN PROCESSUS DE PRP « DÉFINI »

Le processus de protection des renseignements personnels est institutionnalisé comme un processus « défini ».

Au niveau de capacité 3, l'organisme établit un cadre organisationnel qui permet de tenir compte de la PRP selon une même façon de faire pour tous les projets de développement des systèmes d'information. Cette même façon de faire correspond à un processus standardisé de PRP, établi à l'échelle de l'organisme, qui servira à définir un processus de PRP à suivre pour chacun de ses projets impliquant des renseignements personnels.

La première différence fondamentale entre les niveaux de capacité 2 et 3 repose sur le fait qu'au niveau 2, on peut avoir un processus de PRP différent d'un projet à l'autre, alors qu'au niveau 3, chaque projet de PRP gère son processus de PRP « défini » sur la base du processus standardisé de PRP de l'organisme. Ainsi, le processus de PRP est non seulement « géré » comme au niveau 2, mais il est également « défini » à partir d'une base standardisée au niveau de l'organisme et adapté pour chaque projet en respectant des critères d'adaptation que l'organisme a élaborés.

Ainsi, on peut considérer un processus « défini » comme un processus « géré » (niveau de capacité 2) qui est adapté à partir du processus standard de PRP de l'organisme, selon un guide d'adaptation, et qui contribue à réaliser les produits de travail, à fournir des mesures et d'autres informations relatives à l'amélioration du processus de PRP de l'organisme.

Le processus de PRP standardisé de l'organisme public, qui constitue la base de référence d'un processus « défini », est établi, répétable et amélioré de façon continue.

À la différence du processus de PRP « géré » (but de gestion BG 2) qui s'applique à chacun des projets, mais de façon indépendante d'un projet à l'autre, dans un processus de PRP « défini », un organisme public met en œuvre ce processus de manière standardisée et cohérente de façon à ce que la PRP soit réalisée efficacement pour l'ensemble des projets de développement des systèmes d'information ayant recours à des renseignements personnels.

Au niveau de capacité 3, l'organisme est intéressé à déployer un processus standard éprouvé qui, par conséquent, nécessite moins de temps et coûte moins cher qu'au niveau 2, où l'organisation établit et déploie de nouveaux processus de PRP pour chaque projet. En bref, au niveau de capacité 3, l'organisation évite de « réinventer la roue » à chaque projet, pour ainsi se doter rapidement d'un processus de PRP efficace, cohérent et rigoureux.

Ainsi, alors qu'au niveau de capacité 2, les pratiques de gestion PG 2.1 à 2.10 s'appliquent indépendamment d'un projet à l'autre, au niveau de capacité 3, elles s'appliquent à l'ensemble des projets de l'organisme qui impliquent des renseignements personnels, à partir d'une base de référence standardisée.

EXEMPLE

La pratique de gestion *PG 2.1 Établir une politique relativement au processus de PRP*, reprise pour le niveau de capacité 3, comportera comme bien livrable une politique organisationnelle en matière de PRP, non pas pour un seul projet, mais pour l'ensemble des projets de développement des systèmes d'information ayant recours à des renseignements personnels.

Différentes options sont possibles pour établir une telle politique organisationnelle.

Une première option consiste à ce qu'un organisme public établisse une politique organisationnelle visant à assurer la PRP dans l'ensemble de ses opérations. Il inclura dans cette politique une section établissant que tous les projets de développement d'un système d'information doivent prendre en compte et respecter les principes et obligations légales de PRP, avoir recours au processus standard de PRP pour définir le processus de PRP à réaliser dans chacun de ces projets ainsi qu'un processus pour l'adapter. Cela pourrait s'énoncer comme suit : « Un processus standard de PRP est établi (car le terme « défini » est réservé pour un projet bien spécifique qui, à partir du processus standard de l'organisation et du guide d'adaptation, se dote d'un processus « défini ») pour l'ensemble des projets de développement, de même qu'un processus ou un guide d'adaptation de ce processus standard, afin de tenir compte des particularités de chaque projet de développement de systèmes d'information ».

Une autre option est possible dans le cas où l'organisme public ne disposerait pas d'une telle politique organisationnelle. Cet organisme pourrait élaborer une politique spécifique établissant que tous les projets de développement d'un système d'information faisant appel à des renseignements personnels doivent prendre en compte et respecter les principes et obligations légales de PRP et avoir recours au processus standard de PRP pour définir le processus de PRP à réaliser dans chacun de ses projets.

Voici un énoncé de principe directeur dans une politique globale d'une organisation qui s'applique, entre autres, à l'ensemble des projets de développement des systèmes d'information :

« 9) La prévention et la planification

La protection des actifs informationnels doit être prise en compte dès la conception, la planification, la réalisation ou la modification des processus d'affaires, des systèmes d'information et des infrastructures technologiques de la Commission. L'évaluation des risques en matière de sécurité des actifs informationnels et la conformité aux normes en matière de protection des renseignements personnels doivent faire partie des objectifs prioritaires à atteindre dans le cadre de ces projets et les sommes nécessaires à leur atteinte doivent être planifiées. » Consultez à ce sujet *La politique sur la protection des actifs informationnels*, Commission de la santé et de la sécurité au travail : http://www.csst.qc.ca/publications/pdf/dc200-1144.pdf

Une deuxième différence fondamentale entre les niveaux de capacité 2 et 3 est qu'au niveau de capacité 3, le processus de PRP « défini » est décrit de façon plus détaillée et réalisé beaucoup plus rigoureusement qu'un processus « géré ».

Ainsi, un processus « défini » comporte une définition claire, pour chacune des pratiques, d'un ensemble d'éléments tels que le but, les intrants, les critères permettant de déclencher la pratique, les activités associées à cette pratique, les rôles, les mesures, les étapes de vérification, les extrants, ainsi que les critères indiquant que la pratique est considérée comme terminée.

Même si la réalisation d'un tel processus de PRP au niveau 3 est plus exigeante, elle coûte moins cher et est plus rapide à réaliser, car chacun des projets peut réutiliser l'ensemble des actifs reliés au processus standard de PRP de l'organisme (pratiques, gabarits, exemples de biens livrables, leçons apprises, mesures, expertises de membres d'autres projets, etc.).

De plus, un processus de PRP au niveau de capacité 3 permet de produire une plus grande qualité du premier coup et d'éviter ainsi beaucoup de reprises de travail. Dans le contexte de la sensibilité des informations reliées à la PRP, éviter des reprises de travail peut aussi signifier éviter des erreurs de conception ou de réalisation de toute nature reliées aux renseignements personnels et donc, éviter de produire des situations embarrassantes pour l'organisme responsable du système d'information. De plus, cela peut générer des économies substantielles et faciliter l'intégration de la PRP, tout en respectant les délais prévus.

Enfin, une troisième différence fondamentale entre les niveaux de capacité 2 et 3 est qu'au niveau de capacité 3, le processus « défini » permet une compréhension plus détaillée du processus de PRP, en raison de la compréhension même des interrelations entre les activités du processus, des mesures détaillées du processus, des produits de travail et de ses services. Cette différence provient notamment du fait qu'au niveau de capacité 3, étant donné que tous les projets utilisent une même base de processus de PRP, il se construit une bibliothèque des actifs relatifs au processus de PRP, comprenant des produits de travail, des mesures et de l'information d'amélioration.

La connaissance plus précise du processus de PRP permet, notamment de mieux planifier le processus de PRP et de mieux tenir compte des changements des exigences durant le projet, car il est possible de connaître plus facilement et de façon plus exhaustive les incidences réelles de tels changements sur le projet et sur son processus de PRP.

PG 3.1 Établir un processus de PRP « défini »

Établir et maintenir la description du processus « défini » de protection des renseignements personnels.

Le but de cette pratique de gestion est d'établir et de maintenir une description du processus de PRP pour un projet. Ce processus est défini à partir du processus standard de PRP de l'organisme pour l'ensemble des projets et ajusté pour tenir compte des besoins particuliers de ce projet. Il est donc pris pour acquis que l'organisme public possède un processus standard de PRP pour l'ensemble de ses projets, ainsi que des directives pour ajuster ce processus standard afin de répondre aux besoins particuliers de chacun de ses projets.

EXEMPLE

Un processus est en place afin que toutes les propositions de projets de développement d'un système d'information, ayant recours à des renseignements personnels, soient accompagnées d'un rapport d'évaluation des risques du projet sur la PRP lorsqu'elles sont soumises aux autorités.

Avec un processus de PRP « défini », les variations dans la façon dont le processus de PRP est réalisé dans l'organisme sont réduites. De plus, étant donné la standardisation de ce processus, il est vraiment possible de partager, à l'échelle de l'organisme dans chacun des projets, les actifs accumulés (gabarits, exemples, leçons apprises, etc.) reliés au processus standard de PRP et les données de mesure du processus de PRP provenant des projets antérieurs.

EXEMPLE

Les données de mesure sur le temps de réalisation du processus de PRP, pour des projets antérieurs semblables, peuvent être utilisées pour « définir » le plan du processus de PRP (voir à ce sujet la pratique de gestion *PG 2.2 Planifier le processus de PRP*).

Il est également possible de partager et donc de bénéficier des leçons apprises lors de la réalisation du processus de PRP dans le cadre de projets antérieurs.

La description du processus de PRP « défini » fournit la base pour planifier, réaliser, suivre et contrôler le processus de PRP du projet.

Se référer au processus « Définition du processus organisationnel » pour plus d'information sur les actifs des processus standards et sur les guides d'adaptation, ainsi qu'au processus « Gestion de projet intégrée » pour plus d'information sur la façon d'établir et de maintenir un processus défini pour un projet.

Produits de travail types (biens livrables types)

Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Gestion de projet intégrée ».

Sous-pratiques

1. Choisir, à partir de l'ensemble des actifs du processus standard de PRP de l'organisme, les actifs reliés au processus de PRP et qui rencontrent le mieux les besoins particuliers d'un projet.
2. Établir le processus de PRP « défini » en ajustant les processus de PRP choisis selon les directives d'adaptation de l'organisme.
3. S'assurer que les objectifs du processus de PRP de l'organisme sont couverts adéquatement dans le processus de PRP « défini » du projet.
4. Documenter le processus de PRP « défini » et les ajustements apportés.
5. Réviser la description du processus de PRP « défini », au besoin.

PG 3.2 Recueillir l'information d'amélioration du processus de PRP

Recueillir l'information sur les produits de travail, les mesures, les résultats des mesures et celle provenant de la planification et de la réalisation du processus de PRP, afin de soutenir l'utilisation future et l'amélioration du processus de PRP et de ses actifs au sein de l'organisme public.

Artefact :

Partie d'information utilisée ou produite lors du processus de développement.

L'artefact peut prendre la forme d'un modèle d'architecture, d'une description, d'une documentation, etc.

Source : *Grand dictionnaire terminologique*

Le but de cette pratique de gestion est de recueillir des informations et des artefacts provenant de la planification et de la réalisation du processus de PRP, de les consigner et de les partager. Cette information et ces artefacts sont consignés respectivement dans le référentiel de mesures de l'organisme et dans la bibliothèque des actifs liés aux processus de PRP de l'organisme.

Se référer au processus « Définition du processus organisationnel » pour plus d'information sur le référentiel de mesures et la bibliothèque des actifs liés aux processus de l'organisme et au processus « Gestion de projet intégrée » pour plus d'information sur la façon de recueillir de l'information d'amélioration de processus.

Produits de travail types (biens livrables types)

Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Gestion de projet intégrée ».

Sous-pratiques

1. Recueillir et consigner des mesures sur le processus de PRP et ses produits de travail dans le référentiel de mesures de l'organisme.
2. Soumettre la documentation à inclure dans la bibliothèque des actifs liés aux processus de PRP de l'organisme.
3. Documenter les leçons apprises du processus de PRP et les inclure dans la bibliothèque des actifs liés aux processus de PRP de l'organisme.
4. Proposer des améliorations aux actifs liés aux processus de PRP de l'organisme.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 4.3

DÉTERMINER LES PRATIQUES DE GESTION DE LA PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques de gestion qui seront réalisées dans le projet pour atteindre le but de gestion BG 3 (colonne « À faire »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts / coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe H – Produits de travail types (biens livrables types) des buts de gestion

LÉGENDE DES SYMBOLES À UTILISER

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N / A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Haute direction . . . . . .HD
Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Répondant du processus de PRP dans le projet . . . .RPPP
Pilote de projet . . . . . .PP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié . . . . . .P
En cours de réalisation . . . . . .ER
En suspens . . . . . .ES
Réalisé . . . . . .Ré
Approuvé . . . . . .A

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 2 – GÉRER LA PRP	NIVEAU DE CAPACITÉ 3 BG 3	INSTITUTIONNALISER UN PROCESSUS DE PRP « DÉFINI »

AIDE-MÉMOIRE nº 4.3 DÉTERMINER LES PRATIQUES DE GESTION DE LA PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	Nº	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
							Début	Fin	Prévus	Réels
Établir un processus de PRP « défini »	PG 3.1									
Recueillir l'information d'amélioration du processus de PRP	PG 3.2									

BG 4 INSTITUTIONNALISER UN PROCESSUS DE PRP « GÉRÉ QUANTITATIVEMENT »

Le processus de protection des renseignements personnels est institutionnalisé comme un processus « géré quantitativement. »

Au niveau de capacité 4, l'organisme gère et exploite la capacité qu'il a établie par le processus standard de PRP. L'organisme est en mesure non seulement de reproduire le processus de PRP d'un projet à un autre, mais également de prédire quantitativement son comportement. Les décideurs disposent ainsi d'informations quantitatives, appuyées sur la réalité de leur organisme, facilitant leurs prises de décisions relativement au processus de PRP dans leurs projets de développement.

Ainsi, au niveau de capacité 4, le processus « géré quantitativement » est un processus de PRP « défini » (niveau de capacité 3) et géré sous contrôle statistique. Des objectifs quantitatifs sont établis, relativement à la qualité et à la performance du processus de PRP, et ils sont utilisés comme critères dans la gestion de ce processus. La qualité et la performance du processus de PRP sont comprises en termes statistiques et sont gérées durant tout le cycle de vie du processus de PRP.

En fait, le niveau de capacité 4 s'appuie sur les acquis du niveau de capacité 3. Au niveau de capacité 3, l'organisme s'est doté d'un processus standard de PRP et a accumulé des données de mesure et des artefacts relatifs à la réalisation de ce processus, provenant de chacun de ses projets de développement d'un système d'information. Une fois que l'organisme a réussi à accumuler une quantité suffisante de données à des fins statistiques, il peut commencer à le gérer de façon quantitative.

EXEMPLE

Ainsi, il est invraisemblable ou très peu probable qu'un organisme qui ne gère qu'un projet de développement faisant appel à des renseignements personnels à tous les trois ans puisse atteindre le niveau de capacité 4 pour le processus de PRP. En effet, dans ce cas, il ne pourrait pas accumuler suffisamment de données quantitatives pour appliquer des techniques statistiques sur celui-ci.

L'organisme dispose de données sur la performance du processus de PRP et est ainsi en mesure de déterminer sur une base quantitative les mesures correctives à prendre. Les mesures correctives consistent principalement à apporter des changements au processus de PRP, aux endroits qui comportent une variation non souhaitée du processus, afin qu'elle ne se répète plus à l'avenir.

EXEMPLE

S'il a été décelé que le temps requis pour réaliser le « test de nécessité » des renseignements personnels, pour un projet particulier, dépasse de beaucoup les limites supérieures de la durée allouée à cette activité (il aurait pris 2 semaines et aurait dépassé de 2 fois le délai maximum observé), l'analyse des causes de cet écart est réalisée et une explication est donnée pour ce cas. La mesure corrective est alors appliquée. Une mesure corrective peut être très variée, même pour ce cas.

Cela peut être une formation additionnelle offerte à la personne qui réalise ce test, une modification du contenu de la formation pour qu'elle corresponde davantage aux besoins ou une précision des exigences d'informations à fournir avant que cette activité, le « test de nécessité », puisse être déclenchée efficacement. On fournit à la personne responsable la liste des critères à respecter lorsqu'on effectue le « test de nécessité » ainsi qu'un questionnaire standardisé.

La différence fondamentale entre les niveaux de capacité 3 et 4 est le caractère prévisible de façon quantitative du niveau de capacité 4. Le terme « géré quantitativement » implique le recours à des techniques statistiques ou quantitatives appropriées, afin de gérer la performance d'un ou plusieurs des sous-processus du processus de PRP, de sorte que la performance future du processus de PRP puisse être prédite à l'intérieur d'un intervalle de confiance connu.

PG 4.1 Établir des objectifs quantitatifs pour le processus de PRP

Établir et maintenir des objectifs quantitatifs pour le processus de protection des renseignements personnels, concernant la qualité et la performance du processus, en se basant sur les besoins du client et les objectifs d'affaires.

Le but de cette pratique de gestion est de déterminer et d'obtenir l'accord des parties prenantes pertinentes au processus de PRP dans le projet sur des objectifs quantitatifs particuliers à atteindre. Ces objectifs quantitatifs peuvent être exprimés en termes de qualité de produit, de qualité de service ou de performance du processus de PRP.

EXEMPLE

Objectifs quantitatifs reliés à la qualité du produit ou du service :

- nombre et gravité des défauts reliés à la PRP dans les produits de travail livrés ou le système livré ;
- nombre et gravité des plaintes de la part du client et des utilisateurs du produit / service.

Objectifs quantitatifs reliés à la performance du processus :

- pourcentage de défauts corrigés à la suite des activités de vérification du produit, avant de livrer les produits de travail reliés à la PRP ou le système tout entier ;
- pourcentage du temps de développement du processus de PRP requis par la reprise de biens livrables.

Se référer au processus de « Gestion quantitative de projet » pour de l'information sur la façon dont les objectifs quantitatifs sont exprimés pour les sous-processus du processus de PRP.

Produits de travail types (biens livrables types)

Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Gestion quantitative de projet ».

Sous-pratiques

1. Établir les objectifs quantitatifs pertinents au processus de PRP.
2. Allouer les objectifs quantitatifs au processus de PRP et à ses sous-processus.

PG 4.2 Stabiliser la performance des sous-processus du processus de PRP

Stabiliser la performance d'un ou de plusieurs sous-processus du processus de protection des renseignements personnels, afin de déterminer sa capacité à atteindre les objectifs quantitatifs établis de qualité des produits et de performance du processus.

Le but de cette pratique de gestion est de stabiliser la performance d'un ou de plusieurs sous-processus du processus de PRP « défini » (niveau de capacité 3), qui contribue(nt) de façon critique à la performance générale de celui-ci, en ayant recours à des techniques statistiques ou autres techniques quantitatives appropriées. La stabilisation de sous-processus sélectionnés du processus de PRP soutient la prédiction de la capacité du processus de PRP à atteindre les objectifs quantitatifs établis, concernant la qualité des produits et la performance du processus de PRP.

EXEMPLE

Si on reprend l'exemple du « test de nécessité » des renseignements personnels, il est possible que l'organisme ait choisi le sous-processus « test de nécessité », car cette activité critique détermine le contenu de certaines activités subséquentes du processus de PRP. Sa réalisation au moment prévu est cruciale pour le respect de l'échéancier de tout le processus de PRP.

Par la suite, l'organisme identifie les causes de variation du « test de nécessité » d'un projet à l'autre, en termes de qualité du produit livré et de la performance du sous-processus. Il élimine les causes de cette variation qui sont contrôlables : cela permet d'établir les limites inférieures et supérieures de l'intervalle de confiance de ce sous-processus et de dégager une moyenne. Tout sera alors en place pour prédire ou estimer la qualité et la performance du « test de nécessité » lorsque viendra le temps de débuter un nouveau projet contenant des renseignements personnels.

Produits de travail types (biens livrables types)

Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Gestion quantitative de projet ».

Sous-pratiques

1. Gérer statistiquement la performance d'un ou de plusieurs sous-processus qui contribue(nt) de façon critique à la performance générale du processus de PRP.
2. Prédire la capacité du processus de PRP à atteindre les objectifs quantitatifs établis, en considérant la performance des sous-processus « gérés quantitativement ».
3. Intégrer les mesures retenues concernant la performance du processus de PRP dans le référentiel de performance des processus de l'organisme.

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 4.4

DÉTERMINER LES PRATIQUES DE GESTION DE LA PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques de gestion qui seront réalisées dans le projet pour atteindre le but de gestion BG 4 (colonne « À faire »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts / coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe H – Produits de travail types (biens livrables types) des buts de gestion

LÉGENDE DES SYMBOLES À UTILISER

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N / A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres		Membres de l'équipe de développement	
Haute direction	HD	Directeur de projet	DP
Responsable de la PRP de l'organisme	RPRP	Chef et chargé de projet	CP
Conseiller juridique	CJ	Répondant du processus de PRP dans le projet	RPPP
Vérificateur interne	VI	Pilote de projet	PP
Responsable des méthodes	RM	Autres membres	A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable	R	Valide	Va
Réalise	Ré	Approuve	A
Offre un soutien et conseille	SC	Coordonne	C
Vérifie	Vé		

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié	P	Réalisé	Ré
En cours de réalisation	ER	Approuvé	A
En suspens	ES		

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 2 – GÉRER LA PRP	NIVEAU DE CAPACITÉ 4 BG 4	INSTITUTIONNALISER UN PROCESSUS DE PRP « GÉRÉ QUANTITATIVEMENT »

AIDE-MÉMOIRE n° 4.4 DÉTERMINER LES PRATIQUES DE GESTION DE LA PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	N°	Pratique équivalente	À faire	Rôle	Resp.	État	Date réalisation		Efforts/Coûts	
							Début	Fin	Prévus	Réels
Établir des objectifs quantitatifs pour le processus de PRP	PG 4.1									
Stabiliser la performance des sous-processus du processus de PRP	PG 4.2									

BG 5 INSTITUTIONNALISER UN PROCESSUS DE PRP « D'OPTIMISATION »

Le processus de protection des renseignements personnels est institutionnalisé comme un processus « d'optimisation ».

Au niveau de capacité 5, l'ensemble de l'organisme met l'accent sur l'amélioration continue du processus de PRP dans ses projets de développement des systèmes d'information. Le processus de PRP fait partie intégrante des projets faisant appel à des renseignements personnels, et ce, sur une base régulière. Il est valorisé et les personnes sont encouragées à évaluer leurs méthodes de travail et à apporter des améliorations de façon continue.

À ce niveau, l'organisme utilise les résultats des activités du processus de PRP, obtenus au niveau 4, pour déterminer les améliorations à apporter au processus de PRP. Il évalue constamment les derniers développements relativement aux meilleures pratiques de PRP et aux technologies de l'information pour déterminer celles qui pourraient le mieux contribuer à l'atteinte de ses objectifs de PRP. Il met en œuvre des pratiques innovatrices qui ont déjà fait leurs preuves. Il fait également figure de pionnier en expérimentant et implantant de nouvelles façons de faire qui n'ont pas encore été utilisées ailleurs.

L'objectif de ce but est l'amélioration continue du processus de PRP et des technologies qui contribuent à réaliser les objectifs de qualité des produits et de performance du processus de PRP.

PG 5.1 S'assurer de l'amélioration continue du processus de PRP

S'assurer de l'amélioration continue du processus de protection des renseignements personnels, au regard de l'atteinte des objectifs d'affaires pertinents de l'organisme public.

Objectifs d'affaires :

Les stratégies conçues par la direction afin d'assurer à l'organisation une existence continue et d'améliorer son efficacité et son efficience, son service à la clientèle et tous autres facteurs influençant son succès.

Lorsqu'ils sont appliqués au développement de systèmes, de tels objectifs peuvent inclure la réduction du nombre de requêtes de changement durant la phase d'intégration du système, la réduction de la durée du cycle de développement et la réduction du nombre de défauts rapportés par le client.

Le but de cette pratique de gestion est de choisir et de déployer systématiquement les améliorations de processus et de technologie qui contribuent à l'atteinte des objectifs de qualité du produit et de performance du processus de PRP.

Un processus « d'optimisation » dynamique et innovateur dépend de la participation d'un personnel qualifié et sensible aux valeurs et aux objectifs de PRP de l'organisme. La capacité de l'organisme à répondre rapidement aux changements et aux opportunités est constamment améliorée en trouvant des façons d'accélérer et de partager l'apprentissage acquis. L'amélioration du processus de PRP fait partie des rôles de chaque membre du personnel de l'organisme et se traduit par la réalisation d'un cycle d'amélioration continue.

Produits de travail types (biens livrables types)

Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Innovation organisationnelle et déploiement ».

Sous-pratiques

1. Établir et maintenir des objectifs quantitatifs d'amélioration du processus de PRP qui contribuent à l'atteinte des objectifs d'affaires de l'organisme.
2. Déterminer les améliorations du processus de PRP qui pourraient générer des améliorations mesurables de la performance de ce processus.
3. Définir des stratégies et gérer le déploiement d'améliorations projetées dans le processus de PRP, sur la base de bénéfices quantifiés attendus, de coûts et des incidences estimés et de changements à la performance du processus de PRP.

PG 5.2 Corriger les principales causes des problèmes du processus de PRP

Déterminer et corriger les principales causes des défauts et des autres problèmes dans le processus de protection des renseignements personnels.

Le but de cette pratique de gestion est d'analyser les défauts et les autres problèmes rencontrés dans le processus de PRP, de corriger les causes principales de ces défauts et problèmes, ainsi que de prévenir l'apparition de ces défauts et de ces problèmes à l'avenir.

Se référer au processus « Analyse causale et résolution » pour plus d'information sur l'identification et la correction des principales causes de défauts.

Produits de travail types (biens livrables types)

Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Analyse causale et résolution ».

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 4.5

DÉTERMINER LES PRATIQUES DE GESTION DE LA PRP À RÉALISER DANS LE PROJET

UTILITÉ

- déterminer les pratiques de gestion qui seront réalisées dans le projet pour atteindre le but de gestion BG 5 (colonne « À faire »)
- planifier et suivre la réalisation des pratiques en déterminant « qui fait quoi » pour chaque pratique à réaliser (colonnes « Rôles » et « Responsabilités »)
- suivre le déroulement des pratiques (colonnes « État », « Date de réalisation » et « Efforts / coûts »)

DOCUMENTS COMPLÉMENTAIRES

- annexe H – Produits de travail types (biens livrables types) des buts de gestion

LÉGENDE DES SYMBOLES À UTILISER

PRATIQUE ÉQUIVALENTE : indiquer si une pratique différente de la pratique proposée sera réalisée, tout en permettant d'atteindre le but associé à la pratique

---

À FAIRE : indique si la pratique sera réalisée (O, N, N / A)

RÔLE : réfère à la fonction exercée par la personne

Direction et autres		Membres de l'équipe de développement	
Haute direction	HD	Directeur de projet	DP
Responsable de la PRP de l'organisme	RPRP	Chef et chargé de projet	CP
Conseiller juridique	CJ	Répondant du processus de PRP dans le projet	RPPP
Vérificateur interne	VI	Pilote de projet	PP
Responsable des méthodes	RM	Autres membres	A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable	R	Valide	Va
Réalise	Ré	Approuve	A
Offre un soutien et conseille	SC	Coordonne	C
Vérifie	Vé		

ÉTAT : permet de suivre l'état des pratiques de PRP dans le projet

Planifié	P	Réalisé	Ré
En cours de réalisation	ER	Approuvé	A
En suspens	ES		

DATE DE RÉALISATION : indique la date de la réalisation des pratiques

---

EFFORTS / COÛTS : exprimés en jours-personnes ou en $

PARTIE 2 – GÉRER LA PRP	NIVEAU DE CAPACITÉ 5 BG 5	INSTITUTIONNALISER UN PROCESSUS DE PRP « D'OPTIMISATION »

AIDE-MÉMOIRE n° 4.5 DÉTERMINER LES PRATIQUES DE GESTION DE LA PRP À RÉALISER DANS LE PROJET

Projet :

Sous-projet :

Pratiques du Modèle	N°	Pratique équi-valente	À faire	Rôle	Resp.	État	Date réalisation		Efforts / Coûts	
							Début	Fin	Prévus	Réels
S'assurer de l'amélioration continue du processus de PRP	PG 5.1									
Corriger les principales causes des problèmes du processus de PRP	PG 5.2									

Conclusion

Les organismes publics sont responsables de la mise en application de la Loi sur l'accès et des autres dispositions légales de PRP auxquelles ils sont assujettis et ils peuvent prendre diverses mesures pour en assurer le respect.

Les principes à la base de la Loi sur l'accès découlent de droits inscrits dans la *Charte des droits et libertés de la personne* du Québec, soit le droit au respect de la vie privée et le droit à l'information. La Loi sur l'accès a préséance sur les autres lois du Québec et les organismes publics ne peuvent y déroger, à moins d'une indication contraire dans une loi. Ainsi, le respect des dispositions légales de PRP est une exigence incontournable des projets de développement des systèmes d'information.

Le ministère des Relations avec les citoyens et de l'Immigration (MRCI) a élaboré ce *Modèle de pratiques de protection des renseignements personnels (PRP)* dans le but d'offrir un soutien aux organismes publics et de faciliter la mise en application des principes et des obligations légales de PRP dans ces projets.

La prise en compte de la PRP dès les premières étapes d'un projet et pendant sa réalisation contribue à son succès. Le MRCI souhaite que l'utilisation de ce Modèle facilite l'intégration de la PRP par les parties prenantes à un projet de développement des systèmes d'information, notamment les gestionnaires, les responsables de la PRP d'un organisme (RPRP), les directeurs et les chefs de projet, ainsi que les autres membres d'une équipe de développement.

Ce Modèle propose, selon une approche d'amélioration continue, un chemin à suivre pour réaliser et gérer la PRP dans les projets de développement. Le Modèle est conçu de telle sorte qu'il peut être utilisé par tous les organismes publics, peu importe leur taille, le type de projets de développement dans lesquels ils désirent intégrer la PRP et les méthodes de développement utilisées. Les outils proposés, tels que des aide-mémoire ou gabarits permettent une utilisation du Modèle adaptée à la situation particulière de chaque organisme public.

Ce Modèle traite seulement des renseignements personnels confidentiels et non de l'ensemble des renseignements de nature confidentielle. Il intègre dans les pratiques qui y sont décrites, des éléments de sécurité pertinents à la PRP. Sa réalisation s'insère dans une préoccupation plus vaste du MRCI, du Secrétariat du Conseil du trésor, du ministère de la Culture et des Communications et du ministère de la Justice relativement au respect du droit à la vie privée, à la gestion intégrée des documents et la protection de leur valeur juridique ainsi qu'à la qualité des services offerts aux citoyens. Il est toutefois important de souligner qu'il n'aborde pas l'ensemble des dimensions ayant trait à la sécurité, à la gestion documentaire et au maintien de l'intégrité des documents ainsi que de leur valeur juridique tout au long de leur cycle de vie.

Dans une perspective intégrée de gestion de l'information dans les projets de développement, les organismes pourront intégrer d'autres pratiques pour englober toutes les dimensions nécessaires à la protection de l'information.

Enfin, la protection de l'information, incluant la PRP et la sécurité, est une des dimensions importantes de la qualité des services offerts aux citoyens. Dans le contexte de l'amélioration des services à la population, le MRCI souhaite que l'utilisation de ce Modèle par les organismes publics contribue à accroître la confiance des citoyens envers ceux-ci et leurs services.

Annexes

ANNEXE – A **Médiagraphie**

DOCUMENTS CONCERNANT LE CADRE LÉGAL ET ADMINISTRATIF DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE LA SÉCURITÉ, AINSI QUE D'AUTRES MESURES D'ENCADREMENT DE LA FONCTION PUBLIQUE

BORKING, J. and C. RAAB. Laws, PETs and Other Technologies for Privacy Protection, in *The Journal of Information, Law and Technology*, [en ligne]. (5 janvier 2004)* [http://elj.warwick.ac.uk/jilt/01-1/borking.html]

COMMISSION D'ACCÈS À L'INFORMATION. *Exigences minimales relatives à la protection des renseignements personnels lors de sondages réalisés par un organisme public ou son mandataire* et *Aide-mémoire,* [en ligne]. (juin 1999) 17 et 4 p. [www.cai.gouv.qc.ca/fra/docu/sondages.pdf] et [www.cai.gouv.qc.ca/fra/docu/sondag-2.pdf]

COMMISSION D'ACCÈS À L'INFORMATION. *Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la Santé et des Services sociaux,* [en ligne]. (avril 1992) 14 p. [http://www.cai.gouv.qc.ca/fra/docu/exigence.pdf]

COMMISSION D'ACCÈS À L'INFORMATION. *Formulaire de déclaration de fichiers de renseignements personnels,* 1984, 7 p. Pour obtenir une copie du document, s'adresser à : cai.communications@cai.gouv.qc.ca

COMMISSION D'ACCÈS À L'INFORMATION. *Formulaire de demande d'autorisation de recevoir des renseignements nominatifs à des fins de recherche, d'étude ou de statistique,* [en ligne]. 4 p. [www.cai.gouv.qc.ca/fra/biblio_fr/bib_pub_fr.htm]

COMMISSION D'ACCÈS À L'INFORMATION. *Guide pour la destruction des documents renfermant des renseignements personnels,* [en ligne]. 2 p. [www.cai.gouv.qc.ca/fra/docu/destruct.pdf]

COMMISSION D'ACCÈS À L'INFORMATION. *La déclaration d'un fichier de renseignements personnels,* 1984, 27 p. Pour obtenir une copie du document, s'adresser à : cai.communications@cai.gouv.qc.ca.

COMMISSION D'ACCÈS À L'INFORMATION. *La gestion des réclamations dans le cadre d'un programme collectif d'assurance médicaments – Un premier constat,* [en ligne]. 2 p. [www.cai.gouv.qc.ca/fra/docu/contact.pdf]

COMMISSION D'ACCÈS À L'INFORMATION. *La tenue d'un registre des communications de renseignements nominatifs,* [en ligne]. 6 p. [http://www.cai.gouv.qc.ca/fra/docu/registre.pdf]

COMMISSION D'ACCÈS À L'INFORMATION. *Le diagnostic médical des employés de la fonction publique,* [en ligne]. 6 p. [www.cai.gouv.qc.ca/fra/docu/diagnost.pdf]

COMMISSION D'ACCÈS À L'INFORMATION. *Rapport annuel de la CAI 2001-2002,* [en ligne]. 100 p. [http://www.cai.gouv.qc.ca/fra/docu/rap2002.pdf]

* La dernière date de consultation de tous les sites Web mentionnés est le 5 janvier 2004.

COMMISSION DE LA SANTÉ ET DE LA SÉCURITÉ AU TRAVAIL. *Politique sur la protection des actifs informationnels,* [en ligne]. (août 2002) 30 p. [http://www.csst.qc.ca/Publications/pdf/DC200-1144.pdf]

CONSEIL DU TRÉSOR. *Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégés par un droit d'auteur, emmagasinés dans un équipement micro-informatique ou un support informatique amovible,* [en ligne]. (octobre 1999) 10 p. [www.tresor.gouv.qc.ca/doc/acrobat/directivemicro99.pdf]

CONSEIL DU TRÉSOR. *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale,* [en ligne]. novembre 1999, 10 p. [www.tresor.gouv.qc.ca/doc/acrobat/dirsec1.pdf]

CONSEIL DU TRÉSOR. *Loi concernant le cadre juridique des technologies de l'information, texte annoté,* [en ligne]. [www.autoroute.gouv.qc.ca/loi_en_ligne/loi/annindex.html]

CONSEIL EXÉCUTIF. *Plan d'action gouvernemental pour la protection des renseignements personnels et le rôle du MRCI à cet égard,* [en ligne]. (mai 1999) 4 p. [http://www.aiprp.gouv.qc.ca/protectionpublic/actions/actions.asp?Sect=1]

DESBIENS, Lina et Diane POITRAS. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et Loi sur la protection des renseignements personnels dans le secteur privé, textes annotés,* Montréal. Société québécoise d'information juridique, 1996, 1076 p.

DORAY, Raymond et François CHARRETTE. *Accès à l'information. Loi annotée, jurisprudence, analyse et commentaires,* Cowansville. Éditions Yvon Blais, 2002, 2394 p.

ÉDITEUR OFFICIEL DU QUÉBEC. *Charte des droits et libertés de la personne : LRQ, c. C-12, articles 5 et 44,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi C-12 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_12/C12.html]

ÉDITEUR OFFICIEL DU QUÉBEC. Code civil du Québec : *LQ, 1991, c. 64, Chapitre 3 « Du respect de la réputation et de la vie privée »,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi CCQ 1 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/CCQ/CCQ_1.html]

ÉDITEUR OFFICIEL DU QUÉBEC. *Loi concernant le cadre juridique des technologies de l'information : LRQ, c. C-1.1,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi C-1.1 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_1_1/C1_1.html]

ÉDITEUR OFFICIEL DU QUÉBEC. *Lois sectorielles qui encadrent les activités des organismes,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi correspondante à l'organisme concerné.

ÉDITEUR OFFICIEL DU QUÉBEC. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels : LRQ, c. A-2.1,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi A-2.1 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html]

ÉDITEUR OFFICIEL DU QUÉBEC. *Loi sur l'administration publique : LRQ, c. A-6.01, articles 66 et 72),* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi A-6.01 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_6_01/A6_01.html]

ÉDITEUR OFFICIEL DU QUÉBEC. *Loi sur l'assurance maladie : LRQ, c. A-29,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi A-29 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_29/A29.html]

ÉDITEUR OFFICIEL DU QUÉBEC. *Loi sur la fonction publique : LRQ, c. F-3.1.1,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi F-3.1.1 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/F_3_1_1/F3_1_1.html]

ÉDITEUR OFFICIEL DU QUÉBEC. *Loi sur la protection des renseignements personnels dans le secteur privé : LRQ, c. P-39.1,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi P-39.1 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1.html]

ÉDITEUR OFFICIEL DU QUÉBEC. *Loi sur le ministère des Relations avec les citoyens et de l'Immigration : LRQ, c. M-25.01, article 11 7°,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi M-25.01 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/M_25_01/M25_01.html]

ÉDITEUR OFFICIEL DU QUÉBEC. *Loi sur les archives : LRQ, c. A-21.1,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », la loi A-21.1 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_21_1/A21_1.html]

ÉDITEUR OFFICIEL DU QUÉBEC. *Loi sur les tribunaux judiciaires : LRQ, c. T-16,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/T_16/T16.html]

ÉDITEUR OFFICIEL DU QUÉBEC. *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques : c. A-21.1, r.1,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », le « règlement correspondant » à la loi A-21.1 ou [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_21_1/A21_1R1.HTM]

ÉDITEUR OFFICIEL DU QUÉBEC. *Règlement sur les frais exigibles pour la transcription, la reproduction et la transmission de documents et de renseignements nominatifs : c. A-2.1, r. 1.1,* [en ligne]. [www.publicationsduquebec.gouv.qc.ca/home.php#] et choisir dans le menu « Lois et règlements » le sous-menu « Lois refondues et règlements » et sous la rubrique « liste alphabétique », le « règlement correspondant » à la loi A-2.1 [www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=3&file=/A_2_1/A2_1R1_1.HTM]

MINISTÈRE DE LA JUSTICE. *Guide de rédaction des contrats de services professionnels. Clause type de protection des renseignements personnels,* [en ligne dans l'intranet du Secrétariat du Conseil du trésor], choisir la rubrique « Services professionnels » [http://www.marches-publics.tresor.qc/doctypes_avispublics/guides/default.asp] (octobre 1995) 91 p. (cette clause a été intégrée dans la mise à jour de 2002).

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Accès aux renseignements par le personnel,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=3]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Cadre de diffusion de l'information gouvernementale sur Internet,* [en ligne]. [http://www.webmaestro.gouv.qc.ca/ress/cadre/Cadre/cadre.htm#obj]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Communication à des tiers,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=5]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Communication de renseignements personnels à caractère public,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=5#Li1]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Critères d'un consentement valide,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=5#Li2]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Demandes d'accès et de rectification,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/demande/demande.asp]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Demandes d'accès, frais exigibles,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/demande/demande.asp?Sect=4]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Accès liens rapides,* [en ligne]. [http://www.aiprp.gouv.qc.ca/autre/index.asp?Sect=Documentation]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Guide d'évaluation des profils d'accès aux fichiers de renseignements personnels dans les organismes publics,* octobre 2000, 53 p. Pour obtenir une copie du document, s'adresser à : webmestre.aiprp@mrci.gouv.qc.ca .

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Inventaire des fichiers de renseignements personnels,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=1]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *La collecte et l'utilisation des numéros d'identification,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp?Sect=2#identification]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *La PRP c'est…,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/prpcest/prpcest.asp]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Les intervenants,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/intervenants/intervenants.asp]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Les principes et les règles à respecter,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/principes/principes.asp]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Les renseignements personnels,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/prpcest/prpcest.asp?Sect=3#renseignements]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Plan d'action gouvernemental pour la protection des renseignements personnels,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/actions/actions.asp?Sect=1]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION (MRCI). *La protection des renseignements personnels,* [en ligne]. [http://www.aiprp.gouv.qc.ca/protectionpublic/prpcest/prpcest.asp#protection]

MINISTÈRE DES RELATIONS AVEC LES CITOYENS ET DE L'IMMIGRATION. *Références sur des méthodologies d'évaluation des incidences d'un projet sur la PRP (« Privacy impact assessment »),* [en ligne]. [http://www.aiprp.gouv.qc.ca/autre/index.asp?Sect=Documentation]

MINISTRE D'ÉTAT À L'ADMINISTRATION ET À LA FONCTION PUBLIQUE ET PRÉSIDENT DU CONSEIL DU TRÉSOR. *Pour de meilleurs services aux citoyens – Un nouveau cadre de gestion pour la fonction publique,* [en ligne]. (juin 1999) 66 p. [http://www.tresor.gouv.qc.ca/ministre/enonce_f.pdf]

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE). *Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières des données de caractère personnel,* [en ligne]. (2001) 72 p. [http://www1.oecd.org/publications/e-book/9302012E.PDF]

SECRÉTARIAT DU CONSEIL DU TRÉSOR. *Cadre de gestion des ressources informationnelles en soutien à la modernisation de l'Administration publique (*chapitre 3.2-4 *Sécurité et protection des renseignements personnels),* [en ligne]. (janvier 2002) 39 p. [http://www.autoroute.gouv.qc.ca/dossiers/cadre_de_gestion_ct197638.pdf]

SECRÉTARIAT DU CONSEIL DU TRÉSOR. *Guide relatif à la catégorisation des documents technologiques en matière de sécurité,* octobre 2003, V 1,2, 71 p. Pour obtenir une copie du document, s'adresser à : inforoute-gouvernementale@sct.gouv.qc.ca

SECRÉTARIAT DU CONSEIL DU TRÉSOR. *Rapport du comité de travail sur la gestion des diagnostics médicaux des employés de la fonction publique mandaté par le Comité interministériel sur la protection des renseignements personnels,* [en ligne]. (février 2002) 60 p. [www.tresor.gouv.qc.ca/publications/diagnosticsante-employes.pdf]

SECRÉTARIAT DU CONSEIL DU TRÉSOR. *Sécurité de l'information numérique et ICPG,* [en ligne]. [http://www.inforoute-gouvernementale.qc/securite.htm]

SECRÉTARIAT DU CONSEIL DU TRÉSOR. Site Web de l'Autoroute de l'information sur la sécurité, [en ligne]. [www.autoroute.gouv.qc.ca/dossiers/secprotec.htm]

SECRÉTARIAT DU CONSEIL DU TRÉSOR. Site Web sur la sécurité, [en ligne dans l'intranet du Secrétariat du Conseil du trésor]. [www.inforoute-gouvernementale.qc/securite.htm]

SECRÉTARIAT DU CONSEIL DU TRÉSOR. Site Web du Conseil du trésor sur la modernisation de la gestion publique, [en ligne]. [www.tresor.gouv.qc.ca/ministre/modernisation/]

SOCIÉTÉ QUÉBÉCOISE D'INFORMATION JURIDIQUE (SOQIJ). Site Web sur les décisions des tribunaux judiciaires, [en ligne]. [http://www.jugements.qc.ca/php/resultat.php?s=lc&recher=3_200302], et choisir sous la rubrique Laval (Société de transport de la Ville de) c.X., 2003-02-21.

DOCUMENTS CONCERNANT LE MODÈLE INTÉGRÉ D'ÉVOLUTION DES CAPACITÉS (CMMI)

AHERN, Dennis M. et autres. *CMMI Distilled: A Practical Introduction to Integrated Process Improvement,* Montréal, Addison-Wesley, 2001, 306 p.

CARNEGIE MELLON UNIVERSITY, SOFTWARE ENGINEERING INSTITUTE (SEI). *CMMI for Systems Engineering, Software Engineering, and Integrated Product and Process Development (CMMISM-SE/SW/IPPD, V 1.1), Continuous Representation (CMU/SEI-2002-TR-003 , ESC-TR-2002-003), Pittsburg,* [en ligne]. (décembre 2001) 703 p. [www.sei.cmu.edu/cmmi/models/models.html]

CARNEGIE MELLON UNIVERSITY, SOFTWARE ENGINEERING INSTITUTE (SEI). *Modèle d'évolution des capacités logiciel.* Traduction officielle du CMM (Capability Maturity Model) par le Centre de recherche informatique de Montréal (CRIM) (CMU/SEI-93-TR-24 et ESC-TR-93-177), V. 1.1, [en ligne]. (février 1993) 93 p. [www.crim.ca/cgla/fichiers/TR-24.pdf]

CARNEGIE MELLON UNIVERSITY, SOFTWARE ENGINEERING INSTITUTE (SEI). *Pratiques du Modèle d'évolution des capacités logiciel.* Traduction officielle du CMM (Capability Maturity Model) par le Centre de recherche informatique de Montréal (CRIM) (CMU/SEI-93-TR-25 et ESC-TR-93-177), V. 1.1, [en ligne]. (février 1993) 499 p. [www.crim.ca/cgla/fichiers/TR-25.pdf]

CARNEGIE MELLON UNIVERSITY, SOFTWARE ENGINEERING INSTITUTE (SEI). *Questionnaire sur la maturité du processus logiciel.* Traduction officielle du CMM (Capability Maturity Model) par le Centre de recherche informatique de Montréal (CRIM). V. 1.1, [en ligne]. (avril 1994) 42 p. [www.crim.ca/cgla/fichiers/qm.pdf]

CARNEGIE MELLON UNIVERSITY, SOFTWARE ENGINEERING INSTITUTE (SEI). *« Risk Management » in CMMI for Systems Engineering, Software Engineering, and Integrated Product and Process Development (CMMI-SE/SW/IPPD, V1.1), Continuous Representation (CMU/SEI-2002-TR-003, ESC-TR-2002-003),* Pittsburg, [en ligne]. (décembre 2001) p. 301 et suivantes. [www.sei.cmu.edu/cmmi/models/models.html]

CARNEGIE MELLON UNIVERSITY, SOFTWARE ENGINEERING INSTITUTE (SEI). Site Web sur le *Modèle intégré d'évolution des capacités* ou CMMI (Capability Maturity Model Integration), [en ligne]. [www.sei.cmu.edu/cmmi]

CENTRE DE GÉNIE LOGICIEL APPLIQUÉ (CGLA), DIVISION DU CENTRE DE RECHERCHE INFORMATIQUE DE MONTRÉAL (CRIM). *Lexique CMM et CBA IPI (anglais-français),* [en ligne]. (novembre 1996) 25 p. [www.crim.ca/cgla/fichiers/lex-a-f.pdf]

ORGANISATION INTERNATIONALE DE NORMALISATION (ISO). *Technologies de l'information – Évaluation des procédés du logiciel,* Genève, ISO, (ISO/CÉI TR 15504-2 :2004 à TR 15504-3 : 2004). [en ligne], (1998 à 2004) http://www.iso.org/iso/fr/CombinedQueryResult.CombinedQueryResult?queryString=15504]

SECRÉTARIAT DU CONSEIL DU TRÉSOR. *Modèle de pratiques du secteur de processus « Gestion des risques »,* [en ligne dans l'intranet gouvernemental du Secrétariat du Conseil du trésor]. (décembre 2001) V. 1.1, 25 p. [www.inforoute-gouvernementale.qc/risquescontrole.htm]

ANNEXE – B **Sigles**

BG	But de gestion
BS	But spécifique
CAI	Commission d'accès à l'information
CÉI	Commission électrotechnique internationale
CMM	*Capability Maturity Model – Modèle d'évolution des capacités logiciel*
CMMI	*Capability Maturity Model Integrated – Modèle intégré d'évolution des capacités*
CMMI-SE / SW / IPPD	CMMI for Software Engineering, Systems Engineering and Integrated Product and Process Development
DSAIPRP	Direction du soutien en accès à l'information et en protection des renseignements personnels
DICAI	Facteurs de sécurité suivants : **D**isponibilité, **I**ntégrité, **C**onfidentialité, **A**uthentification, **I**rrévocabilité
ISO	Organisation internationale de normalisation
MRCI	Ministère des Relations avec les citoyens et de l'Immigration
PG	Pratique de gestion
PRP	Protection des renseignements personnels
PS	Pratique spécifique
Répondant de la PRP	Répondant de la protection des renseignements personnels dans un projet de développement
RP	Renseignements personnels
RPRP	Responsable de la protection des renseignements personnels
RSIN	Responsable de la sécurité de l'information numérique
SCT	Secrétariat du Conseil du trésor

ANNEXE – C Glossaire

Ce glossaire définit les termes particuliers au processus de PRP et les termes propres au modèle de référence CMMI et qui ont été jugés essentiels dans la compréhension du Modèle de pratiques de PRP.

Se référer au glossaire (« Appendix C. Glossary ») du modèle CMMI si vous désirez obtenir plus d'information sur les termes propres au modèle de référence CMMI.

Actifs liés au processus de PRP de l'organisme

Éléments du processus de PRP qui sont utiles à ceux qui définissent, mettent en œuvre et gèrent le processus de PRP dans l'organisme public. Ces éléments comprennent des documents, des aides d'implantation et tout autre artefact. Ces éléments peuvent prendre la forme de politiques, de définitions de processus, de listes de vérification, de listes de « leçons apprises », de gabarits, d'exemples, d'aide-mémoire, de standards, de procédures, de guides, de plans et de matériel de formation. Ces actifs représentent le capital intellectuel de l'organisme public en matière de PRP et aident à réduire l'effort dans la réalisation du processus de PRP dans chacun des projets de l'organisme public. Ces éléments sont constitués à l'échelle de l'organisme public principalement à partir du niveau de capacité 3.

Adéquat, approprié, au besoin

Ces termes sont utilisés de telle sorte que vous puissiez interpréter les buts et les pratiques à la lumière des objectifs d'affaires de votre organisme public et de l'interprétation des exigences légales. Lorsque vous utilisez un modèle CMMI, vous devez interpréter les pratiques de manière à ce qu'elles contribuent à l'atteinte de ces objectifs et au respect de ces exigences dans votre organisation. Ces termes se retrouvent dans la description des buts et des pratiques lorsque certaines activités peuvent ne pas être réalisées tout le temps.

Amélioration de processus / amélioration continue

Comprend un programme d'activités conçu afin d'améliorer la performance et la capacité des processus d'un organisme public de façon régulière et continue, ainsi que les résultats d'un tel programme.

Anonymisation

Action de rendre des renseignements personnels anonymes.

Artefact

Partie d'information utilisée ou produite lors du processus de développement. L'artefact peut prendre la forme d'un modèle d'architecture, d'une description, d'une documentation, etc.

But

Un « but » est un composant du Modèle qui peut être soit un but de gestion soit un but spécifique. Le terme « but » dans le Modèle réfère toujours aux composants du modèle. Un but représente l'essence des pratiques associées à un but. Un but oriente l'interprétation des pratiques qui lui sont associées et représente le point à atteindre ou l'exigence à satisfaire si l'organisme public désire que son processus de PRP se situe à un niveau de capacité correspondant à ce but.

But de gestion

But orientant des pratiques relatives à la gestion du processus de PRP. Il est dit « de gestion », car il permet d'appliquer les principes couramment rencontrés pour gérer les pratiques de PRP, c'est-à-dire planifier, organiser et contrôler. Les buts de gestion correspondent aux buts génériques de gestion définis au modèle de référence CMMI et qui ont été appliqués au processus de PRP.

But spécifique de PRP

But orientant des pratiques relatives à la réalisation du processus de PRP. Il est dit « spécifique », car chacun des buts spécifiques d'un processus particulier traite des caractéristiques uniques de la PRP, qui décrivent ce qui doit être mis en œuvre pour satisfaire aux exigences du processus de PRP lors du développement des systèmes d'information.

But spécifique de PRP pertinent

Un but spécifique de PRP qui s'applique à un projet concerné. Ainsi, si un projet ne comporte pas de communication de renseignements personnels à des tiers, le but spécifique *BS 5 Communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public* ne s'applique pas et n'est pas pertinent.

Capacité du processus

L'étendue des résultats attendus qui peuvent être accomplis en suivant un processus mis en œuvre dans un organisme public à un moment donné.

Catégories de personnes

Les personnes qui ont accès aux renseignements et qui sont identifiées, non pas par leur nom, mais selon l'unité administrative auxquelles elles appartiennent, leur corps d'emploi, titre de fonction, rôle ou responsabilités.

Client

Un client est la partie (individu, projet ou organisation) responsable de l'acceptation du produit ou de l'autorisation du paiement. Le client est externe à l'équipe de projet, mais il n'est pas nécessairement externe à l'organisation. Dans le contexte d'un projet d'envergure découpé en plusieurs sous-projets réalisés en parallèle ou séquentiellement, le client d'un projet peut être un autre sous-projet ou le projet intégrateur. Un client est une des parties prenantes au projet (« stakeholders »).

Composants associés à une obligation légale

Pratiques spécifiques, produits de travail type et sous-pratiques ainsi que les explications qui les accompagnent, qui sont associés à des dispositions légales. Ils indiquent les articles de la Loi sur l'accès, du *Code civil du Québec* et de la *Loi sur les archives* qui y sont associés. Leur réalisation se fera de façon à respecter l'obligation légale correspondante, et ce, en fonction de la jurisprudence établie et du contexte du système d'information en développement.

Cette association est représentée par un pictogramme situé dans la marge de gauche vis-à-vis du composant concerné. Ce pictogramme contient l'image d'une balance représentant la justice pour indiquer la nécessité d'une interprétation de la pratique selon une disposition légale ; cette image est accompagnée des articles de la ou des loi(s) d'où origine la pratique.

Art. 54
Loi sur l'accès

Composants du Modèle

Ensemble des éléments qui composent le Modèle :

- buts (spécifiques et de gestion) ;
- pratiques (spécifiques et de gestion) ;
- niveaux de capacité ;
- explications (des buts et des pratiques) ;
- produits de travail types (biens livrables types) ;
- sous-pratiques ;
- exemples ;
- références.

Conformité du processus de PRP

L'évaluation de la conformité du processus de PRP permet de fournir une assurance à l'effet qu'il est mis en œuvre tel qu'il est prévu dans le projet, et qu'il respecte la description retenue de ce processus de PRP, ses standards et ses procédures. Il est important de ne pas confondre la conformité du processus de PRP avec la conformité à la Loi sur l'accès. Cette dernière réfère à un autre type d'évaluation réalisée au sein d'un organisme public qui viserait à déterminer si telle façon de faire dans un système d'information est conforme à une disposition de la Loi sur l'accès. Ce type d'évaluation peut, par exemple, s'effectuer lors d'un « audit de conformité » par la Commission d'accès à l'information ou le vérificateur interne de l'organisme public.

Cycle de vie de la PRP

Le cycle de vie de la PRP réfère au processus de PRP comprenant un ensemble de pratiques spécifiques de PRP regroupées par buts spécifiques. Ces buts, au nombre de huit, correspondent aux huit phases du cycle de vie de la PRP. Ce sont :

BS 1 Recueillir des renseignements personnels ;

BS 2 Traiter les demandes d'accès à des renseignements personnels et de rectification ;

BS 3 Attribuer au personnel, les droits d'accès aux renseignements personnels ;

BS 4 Utiliser des renseignements personnels à l'intérieur de l'organisme public ;

BS 5 Communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public ;

BS 6 Conserver des renseignements personnels ;

BS 7 Détruire des renseignements personnels ;

BS 8 Diffuser l'information sur la gestion des renseignements personnels.

Cycle de vie d'un système

Ensemble des différents moments qu'un système d'information traverse durant son existence et comprenant les phases suivantes :

- développement ;
- implantation et déploiement ;
- entretien (ou maintenance) ;
- exploitation et utilisation ;
- retrait (ou mise au rancart).

Description de processus de PRP

Une expression documentée d'un ensemble d'activités réalisées pour atteindre un objectif tel que « respecter les principes et les obligations légales de PRP », et fournissant une définition opérationnelle des composants majeurs du processus de PRP. La documentation spécifie, d'une façon complète, précise et vérifiable, les exigences, la conception, le comportement ou les autres caractéristiques d'un processus. Les descriptions d'un processus peuvent se retrouver au niveau d'une activité, d'un projet ou d'une organisation.

Développement

Dans ce Modèle, le terme « développement » comprend non seulement les activités de développement relatives au nouveau système d'information, mais aussi les activités relatives à l'adaptation d'un progiciel, à la maintenance (ou entretien ou évolution) d'un système existant et au déploiement (ou implantation) du nouveau système ou de la nouvelle version d'un système existant.

Droit d'accès du personnel

Autorisation du personnel de l'organisme à prendre connaissance des renseignements personnels en fonction des obligations légales de PRP. Dans un contexte informatique, on réfère souvent aux droits et aux privilèges d'accès de l'utilisateur.

Établir et maintenir

Certains buts et pratiques incluent le terme « établir et maintenir ». Ce terme comporte une signification qui dépasse chacun des mots du terme : il inclut la documentation et l'utilisation. Par exemple, « établir et maintenir une politique organisationnelle » signifie que non seulement une politique est formulée ou définie, mais aussi qu'elle est documentée, tenue à jour, connue des parties prenantes et utilisée ou mise en œuvre dans l'organisme public. Au niveau 2, l'organisme se limite à le faire projet par projet, alors qu'au niveau 3 et plus, elle le fait de façon standardisée à l'échelle de toute son organisation pour tous ses projets.

Exigence

Trois définitions de ce terme sont proposées [IEEE* 610.12-1990] :

1. Une condition ou une capacité dont un utilisateur a besoin afin de résoudre un problème ou atteindre un objectif.

2. Une condition ou une capacité qui doit être satisfaite ou qui fait partie d'un produit ou d'un composant de produit afin de respecter un contrat, une norme, Une spécification ou d'autres documents imposés formellement.

3. Une représentation documentée d'une condition ou d'une capacité décrite en 1 ou 2.

Fichier de renseignements personnels

Selon la Commission d'accès à l'information (CAI) et la Loi sur l'accès, il s'agit d'une collection organisée de renseignements personnels qui répondent à l'une ou l'autre des deux conditions suivantes** :

1° sont identifiés ou se présentent de façon à être retrouvés par référence au nom d'une personne ou à un signe ou symbole propre à celle-ci ; ou

2° ont servi ou sont destinés à servir pour une décision concernant une personne (article 71, Loi sur l'accès).

Formulaire de déclaration de fichiers de renseignements personnels

Formulaire produit par la CAI afin de permettre aux organismes publics de lui déclarer ses fichiers de renseignements personnels et de produire un répertoire de ceux-ci accessible au public.

Gestion des configurations

Processus visant à établir et maintenir l'intégrité des produits de travail composant un système d'information. Ce processus permet ainsi de gérer la description technique des différents éléments composant un système d'information et des évolutions qui sont successivement apportées à cette description et aux différents exemplaires de ces éléments.

Gestion des risques

Processus organisé et analytique destiné à identifier la source d'un dommage ou d'une perte possible, à évaluer et quantifier les risques identifiés, développer et, au besoin, mettre en œuvre une approche appropriée visant à prévenir ou à traiter les causes des risques et ainsi prévenir une perte ou un dommage significatif.

Institutionnalisation

La façon de faire qu'un organisme public suit de façon routinière et faisant partie de sa culture. Appliqué aux niveaux de capacité du processus de PRP, ce concept signifie que l'organisme public applique à tous ses projets un même ensemble de pratiques.

---

* Institute of Electrical and Electronics Engineers.

** La déclaration d'un fichier de renseignements personnels, CAI, 1984, page XX.

Inventaire des fichiers de renseignements personnels

Le terme « inventaire de fichiers » prend un sens particulier dans le contexte de la Loi sur l'accès. L'inventaire ne se limite pas à une simple énumération de fichiers mais comprend aussi d'autres informations de gestion concernant ces fichiers, notamment le volume, le type et la provenance des renseignements personnels, leur localisation, leur utilisation et leur circulation au sein de l'organisme*.

Modèle / Modèle de pratiques de PRP

Description documentée du processus de PRP, comprenant un ensemble de buts spécifiques et de gestion associés à des pratiques, à réaliser et à gérer par une équipe de projet de développement des systèmes d'information.

Modèle intégré d'évolution des capacités

Le *Modèle intégré d'évolution des capacités* (CMMI) contient les éléments essentiels de processus effectifs pour le développement de systèmes. Il décrit aussi un chemin évolutif d'amélioration à partir de processus ad hoc, incomplets et immatures jusqu'à des processus disciplinés et matures permettant d'atteindre une qualité et une efficience améliorées.

Niveau de capacité

Un niveau de capacité est défini par l'atteinte des buts associés à un niveau de capacité particulier et qui sont assortis de la réalisation des pratiques spécifiques ou des pratiques de gestion appropriées au processus de PRP.

Objectifs d'affaires de l'organisme public

Stratégies conçues par la direction afin d'assurer à l'organisme public une existence continue et d'améliorer son efficacité et efficience, son service à la clientèle et tous autres facteurs influençant son succès.

Lorsqu'ils sont appliqués au développement de systèmes, de tels objectifs peuvent inclure la réduction du nombre de requêtes de changement durant la phase d'intégration du système, la réduction de la durée du cycle de développement, l'augmentation du nombre d'erreurs trouvées au début du développement, la réduction du nombre de défauts rapportés par le client, la satisfaction du client dans l'utilisation du système, etc.

Objectifs d'amélioration du processus de PRP

Un ensemble de caractéristiques cibles établi afin de guider l'effort d'amélioration du processus de PRP existant, d'une façon spécifique mesurable soit en termes de caractéristiques du produit résultant (ex. : qualité, rendement, conformité aux normes, etc.), soit de la façon dont le processus est réalisé (ex. : élimination des étapes redondantes du processus, fusion d'étapes du processus, amélioration de la durée du cycle, etc.).

Organisme public

Il y a environ 2 500 organismes publics assujettis à la Loi sur l'accès. Les organismes publics sont : le gouvernement, le Conseil exécutif, le Conseil du trésor, les ministères, les organismes gouvernementaux, les organismes municipaux, les organismes scolaires et les établissements de santé ou de services sociaux. D'autres organismes sont assimilés à des organismes publics, aux fins de la Loi sur l'accès, ce sont : « le lieutenant-gouverneur, l'Assemblée nationale, un organisme dont elle nomme les membres et une personne qu'elle désigne pour exercer une fonction en relevant, avec le personnel qu'elle dirige. Les organismes publics ne comprennent pas les tribunaux au sens de la *Loi sur les tribunaux judiciaires* (L.R.Q., c. T-16) ». Consultez à ce sujet les articles 4 à 7 de la Loi sur l'accès.

Partie prenante (« stakeholder »)

Une « partie prenante » au projet est un groupe ou un individu concerné ou imputable d'une certaine façon du résultat d'un projet. Les parties prenantes au projet peuvent inclure des membres de projet, des fournisseurs, des clients, des utilisateurs et d'autres personnes.

---

* La déclaration d'un fichier de renseignements personnels, CAI, 1984, page 5.

Partie prenante pertinente («stakeholder»)

Le terme « partie prenante pertinente » est utilisé pour désigner une partie prenante qui est identifiée pour une participation dans des activités spécifiées d'un projet et qui est incluse dans un plan approprié. Ainsi, même s'il y a dix parties prenantes pour le processus de PRP, il n'y en aura peut-être que deux qui seront pertinentes pour participer à la réalisation d'une activité donnée. Il serait en effet inefficace de faire participer toutes les parties prenantes à toutes les activités.

Pilote de projet / pilote de système

Personne qui représente les utilisateurs du futur système d'information. C'est une personne qui connaît bien le processus d'affaires couvert par le système d'information concerné et qui est en mesure de fournir des informations sur les besoins précis des utilisateurs et de valider les biens livrables du processus de PRP du projet.

Politique organisationnelle

Un principe d'orientation typiquement établi par la direction et qui est adopté par l'organisation afin d'influencer et de déterminer les décisions.

Pratique

Composant du Modèle qui peut être « de gestion » ou « spécifique ». Une pratique comprend une activité ou un ensemble d'activités (ou sous-pratiques) permettant de réaliser les produits de travail types de cette pratique et ainsi de contribuer à l'atteinte du but auquel la pratique est associée. Chaque pratique soutient un seul but.

Pratique équivalente

Une pratique qui est un substitut ou une alternative pour une ou plusieurs pratiques de gestion ou spécifiques du Modèle, qui accomplit un effet équivalent pour satisfaire le but de gestion ou spécifique associé aux pratiques du Modèle. Les pratiques équivalentes ne correspondent pas nécessairement à des remplacements « un pour un » pour les pratiques de gestion ou spécifiques.

Pratique de gestion

Pratique applicable à tout processus, qui n'appartient pas à un processus en particulier et qui est importante pour la stabilité et l'amélioration à l'intérieur des processus. Des exemples de pratiques de gestion touchent la planification, la formation et la gestion de configuration. Dans ce Modèle, les pratiques de gestion sont exprimées pour être appliquées au processus de PRP.

Pratique spécifique de PRP

Une pratique spécifique est une activité ou un ensemble d'activités importantes pour atteindre le but spécifique de PRP associé. Les pratiques spécifiques décrivent les activités devant permettre d'atteindre les buts spécifiques du processus de PRP. Dans le processus PRP, il y a 24 pratiques spécifiques. Ce sont les pratiques spécifiques que l'on retrouve normalement dans un organisme public pour satisfaire un but spécifique. Étant donné que le Modèle n'est pas une norme, les pratiques spécifiques demeurent des propositions de pratiques. L'organisme public peut réaliser une « pratique équivalente » différente de la pratique proposée, mais qui permet d'atteindre quand même le but associé à la pratique.

Processus défini

Un processus « défini » :

- est un processus « géré » qui est ajusté à partir de l'ensemble des processus standards de l'organisme public selon les orientations d'ajustement de celui-ci ;
- dispose d'une description à jour du processus tel qu'il est utilisé ;
- fournit des produits de travail, des mesures et d'autres informations d'amélioration des actifs liés aux processus de l'organisme.

Un processus « défini » d'un projet fournit une base pour la planification, la réalisation et l'amélioration des tâches et des activités du projet. Un projet peut avoir plus d'un processus « défini » (par exemple : un pour le développement du produit et l'autre pour la mise à l'essai du produit). Un processus « défini » correspond au niveau de capacité 3.

Processus de PRP

Le processus de PRP est un ensemble cohérent de pratiques spécifiques et de pratiques de gestion qui permettent de réaliser et de gérer le processus de PRP selon les choix de gestion de l'organisme public et les principes et obligations légales de la PRP.

Les pratiques spécifiques sont regroupées en huit buts, correspondant aux huit phases du cycle de vie de la PRP. Lorsqu'elles sont réalisées, elles permettent d'atteindre les buts considérés comme étant importants pour respecter les principes et obligations légales de PRP.

Les pratiques de gestion sont regroupées en cinq buts, correspondant aux cinq niveaux de capacité (ou de gestion) les plus avancés. Lorsqu'elles sont réalisées, elles permettent d'atteindre les buts de gestion (ou les niveaux de capacité) visés par l'organisme public.

Processus d'optimisation

Un processus « d'optimisation » est un processus « géré quantitativement » qui est amélioré sur la base d'une compréhension des causes communes de variation inhérente au processus. Un processus qui focalise sur l'amélioration continue de l'étendue de la performance du processus au moyen d'améliorations à la fois incrémentales et innovatrices. (Voir « processus géré quantitativement » et « processus défini »). Un processus « d'optimisation » correspond au niveau de capacité 5.

Processus géré

Un processus « géré » :

- est un processus qui est planifié et réalisé conformément aux politiques et directives et qui emploie des personnes qualifiées disposant de ressources adéquates pour produire des résultats contrôlés ;
- fait participer les parties prenantes au projet qui sont concernées ;
- est suivi, contrôlé et passé en revue ;
- est évalué quant à sa conformité relativement à sa description de processus.

Un processus « géré » correspond au niveau de capacité 2.

Processus géré quantitativement

Un processus « géré quantitativement » est un processus « défini » qui est contrôlé par des techniques statistiques ou d'autres techniques quantitatives. La qualité du produit, la qualité du service et les attributs de performance du processus sont mesurables et contrôlés durant tout le projet (voir « processus d'optimisation » et « processus défini »). Un processus « géré quantitativement » correspond au niveau de capacité 4.

Processus incomplet

Un processus qui n'est pas réalisé ou n'est réalisé que partiellement et qui correspond au niveau de capacité 0. Un ou plusieurs but(s) spécifique(s) du processus n'est pas (ne sont pas) atteint(s).

Processus réalisé

Un processus où sont réalisées les pratiques spécifiques de PRP permettant d'atteindre les buts spécifiques du processus de PRP. Un processus « réalisé » correspond au niveau de capacité 1 lorsque tous les projets de développement de l'organisme public atteignent les buts spécifiques du processus de PRP.

Processus standard de PRP de l'organisme

Une définition opérationnelle du processus de PRP pour le développement des systèmes d'information qui guide l'établissement d'un processus commun à l'échelle de l'organisme public (d'après ISO / CÉI 15504-9). Ce processus standard décrit les éléments de base du processus de PRP à partir desquels sera établi un processus « défini » pour chaque projet de développement. Ce processus standard prend forme au niveau de capacité 3.

Produit

Le terme « produit » signifie tout résultat ou service résultant d'un processus et qui est destiné à être livré à un client ou à un utilisateur. Un produit est un produit de travail livré au client.

Produit de travail (bien livrable)

Le terme « produit de travail » ou « bien livrable » signifie tout objet produit par un processus. Ces objets peuvent inclure des fichiers, des documents, des parties de produit, des services, des processus, des spécifications et des factures. Des exemples de processus pouvant être considérés comme des produits de travail comprennent un processus manufacturier, un processus de formation et un processus de retrait du produit.

Produit de travail type (bien livrable type)

Composant du Modèle qui fournit des exemples de résultats provenant d'une pratique spécifique ou de gestion. Ces exemples sont appelés « produits de travail types » ou « biens livrables types », car il peut exister d'autres produits de travail tout aussi efficaces, mais non répertoriés.

Lorsqu'un article de la loi est rapporté dans la description d'un produit de travail type, cela indique que ce produit de travail type est prévu dans une disposition légale expresse et que sa réalisation se fera de manière à la respecter.

Profil d'accès

Description des catégories de personnes qui ont accès aux renseignements personnels, aux programmes de traitement, à la configuration de production et aux rapports produits par le système, sous forme électronique ou autres, et de leurs privilèges d'accès (lecture, modification, copie, destruction, impression ou autres). Cette description est établie en fonction des processus d'affaires et des unités administratives concernées.

Projet

Ensemble géré de ressources interreliées qui livre un ou plusieurs produit(s) à un client ou à un utilisateur. Cet ensemble de ressources comprend un début et une fin délimités et il fonctionne typiquement selon un plan. Un tel plan, fréquemment documenté, spécifie le produit à être livré ou implanté, les ressources et les fonds utilisés, le travail à réaliser et un calendrier de travail. Un projet peut être composé de projets ou sous-projets.

Protection des renseignements personnels

La protection des renseignements personnels est un droit conféré à toute personne, par le chapitre 3 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.* Ce droit découle du droit au respect de la vie privée consacré dans la *Charte des droits et libertés de la personne* du Québec. Toute personne a un droit de regard sur les renseignements personnels qui la concernent et qui sont détenus par les organismes publics. Pour assurer la PRP, les organismes publics gèrent les renseignements personnels de manière transparente et ils mettent notamment en œuvre les mesures suivantes :

- mesures nécessaires pour permettre aux personnes d'exercer leurs droits d'accès aux renseignements personnels et de rectification ;
- mesures nécessaires pour que les principes et les obligations de PRP de la Loi sur l'accès et des autres lois qu'ils administrent soient respectés et mis en œuvre relativement à leur :
  - collecte ;
  - accès et rectification par la personne concernée ;
  - accès par le personnel de l'organisme ;
  - utilisation à l'intérieur de l'organisme ;
  - communication à des tiers, à l'extérieur de l'organisme ;
  - conservation ;
  - destruction.

Cette responsabilité des organismes publics repose donc sur la gestion et la réalisation d'un ensemble d'activités permettant la mise en application des principes et obligations légales de PRP.

Références

Composants du Modèle qui dirigent l'utilisateur vers des informations complémentaires ou plus détaillées dans des processus associés auxquels il peut se référer. Toutes les références sont clairement indiquées en italique dans le Modèle. Toutes les références à des composants du Modèle commencent avec le terme « Se référer à », tel que *Se référer au processus « Planification de projet » pour obtenir plus d'informations relatives à la planification globale de projet ou le terme « consulter », tel que « consulter le site Web du MRCI :* www.aiprp.gouv.qc.ca/html/communication.html ».

Renseignement anonyme

Renseignement qui concerne une personne mais qui ne permet pas de l'identifier ou de la reconnaître.

Renseignement personnel

Renseignement qui concerne une personne physique et permet de l'identifier.

Répondant de la protection des renseignements personnels dans le projet (répondant de la PRP)

À la différence du responsable de la protection des renseignements personnels de l'organisme (RPRP) ou de la personne qui agit à titre de représentant de la PRP pour tous les projets de développement de l'organisme public, les responsabilités et les activités du répondant de la PRP se limitent à un projet de développement particulier. Il est formellement assigné à la fonction de réalisation du processus de PRP dans un projet. Il a le pouvoir de prendre des décisions à cet égard et il répond de cette responsabilité à l'autorité compétente.

La fonction de répondant de la PRP pourrait également être assumée par le chargé de projet, par le RPRP ou une personne qu'elle désigne, ou toute autre personne qui détient l'autorité et la compétence appropriées.

Représentation continue

Une structure du CMMI où les niveaux de capacité fournissent un ordre recommandé pour aborder l'amélioration du processus de PRP. (Voir « niveau de capacité », « processus de PRP » et « amélioration de processus. »)

Responsable de la protection des renseignements personnels (RPRP)

Selon le *Plan d'action gouvernemental pour la PRP*, dans chaque ministère ou organisme, un membre du personnel de direction relevant directement du sous-ministre ou du président de l'organisme est désigné à titre de responsable de la protection des renseignements personnels pour toute l'organisation. Outre ses responsabilités légales en matière d'accès et de rectification des renseignements personnels, le RPRP agit comme interlocuteur auprès de la Commission d'accès à l'information et représente l'organisation. Il soutient et conseille le personnel d'encadrement et les employés afin que l'ensemble de l'organisation respecte les principes et obligations légales de PRP, et ce, notamment dans les projets de développement des systèmes d'information.

Il arrive fréquemment que la personne désignée comme responsable de l'accès aux documents assume, à la fois, la responsabilité de traiter les demandes d'accès aux documents et d'assurer la protection des renseignements personnels. Lorsqu'elle assume ces deux responsabilités, elle remplit l'ensemble des fonctions décrites dans la Loi sur l'accès.

Responsable de la sécurité de l'information numérique (RSIN)

Personne désignée par le sous-ministre ou le dirigeant d'organisme pour assurer la gestion et la coordination de la sécurité et le représenter en cette matière dans l'organisation.

Service du processus de PRP

Une pratique comprend la réalisation d'un ensemble d'activités permettant de produire les biens livrables et les services attendus. À la différence des biens livrables qui comportent un caractère statique, les services sont des processus utilisables à la suite de la réalisation d'une pratique (par exemple : un programme de formation). Un service exige la participation d'une personne (et quelquefois l'utilisation d'un logiciel) pour qu'il puisse être offert. Il revêt un caractère dynamique, participatif.

Sous-pratique

Descriptions détaillées offrant une orientation pour l'interprétation des pratiques spécifiques ou de gestion. Une sous-pratique peut être formulée comme si elle était normative, mais elle est en fait un composant du Modèle destiné uniquement à fournir des exemples d'activités qui peuvent être utilisées ou non pour réaliser la pratique.

Validation

Bien que la « vérification » et la « validation » apparaissent à prime abord très similaires, elles réfèrent chacune à des préoccupations différentes. La validation confirme que le produit, tel qu'il est fourni, va satisfaire les besoins relativement à l'utilisation prévue. En d'autres mots, la validation s'assure que « vous construisez le bon système ». La validation est réalisée par un client / utilisateur ou par son représentant.

Vérification

La vérification confirme que les produits de travail reflètent adéquatement les exigences. En d'autres mots, la vérification s'assure que « vous construisez le système correctement ».

La vérification consiste à effectuer un examen pour déterminer si tels pratiques, sous-pratiques ou produits de travail ou autres activités de PRP ont été réalisés selon les « règles de l'art » et les principes et obligations légales de PRP, en fonction des critères et des orientations établis. Afin d'assurer l'objectivité ou l'impartialité, la personne qui réalise la vérification ne peut pas réaliser les activités à vérifier.

ANNEXE – D **Buts et pratiques spécifiques**

BS 1 RECUEILLIR DES RENSEIGNEMENTS PERSONNELS

Les renseignements personnels sont recueillis en respectant les principes et les obligations légales de PRP.

PS 1.1 Déterminer tous les renseignements personnels que l'on projette de gérer dans le système

Déterminer, parmi les renseignements que l'on projette de recueillir et consigner dans le système ou produire par celui-ci, ceux qui correspondent à la définition légale de « renseignement personnel ».

PS 1.2 Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système

Indiquer les critères à respecter pour évaluer la nécessité des renseignements personnels que l'on projette de recueillir et consigner dans le système ou produire par celui-ci, en fonction des principes et des obligations légales de PRP, réaliser le « test de nécessité » et le documenter.

PS 1.3 Déterminer les sources d'obtention des renseignements personnels

Déterminer et documenter la provenance des renseignements personnels.

PS 1.4 Informer la Commission d'accès à l'information (CAI) des situations où des renseignements personnels, déjà colligés par une personne (autre que la personne concernée) ou par une entreprise privée, seront recueillis auprès de celles-ci

Déterminer, documenter et mettre en œuvre les mesures nécessaires pour informer la CAI avant de recueillir auprès d'une personne (autre que la personne concernée) ou d'une entreprise privée, des renseignements personnels qu'elle a déjà recueillis, et informer la CAI.

PS 1.5 Déterminer les modalités de collecte des renseignements personnels

Déterminer, en fonction des principes et des obligations légales de PRP et de respect de la vie privée, les modalités de collecte des renseignements personnels.

PS 1.6 Déterminer les modalités d'information de la personne auprès de qui les renseignements personnels seront recueillis

Déterminer les modalités d'information de la personne auprès de qui les renseignements personnels seront recueillis, en fonction des principes et des obligations légales de PRP.

BS 2 TRAITER LES DEMANDES D'ACCÈS À DES RENSEIGNEMENTS PERSONNELS ET DE RECTIFICATION

L'organisme public traite les demandes d'accès à des renseignements personnels consignés dans le système d'information et de rectification de ceux-ci, en respectant les principes et les obligations légales de PRP.

PS 2.1 Mettre en œuvre les modalités de traitement des demandes d'accès à des renseignements personnels et de rectification de ceux-ci

Élaborer, documenter et mettre en œuvre des mesures pour permettre, à la personne concernée, l'exercice de son droit de consulter et d'obtenir une copie des renseignements qui la concernent ainsi que de demander à ce qu'ils soient rectifiés, en respectant les principes et les obligations légales de PRP.

BS 3 ATTRIBUER AU PERSONNEL, LES DROITS D'ACCÈS AUX RENSEIGNEMENTS PERSONNELS

La protection des renseignements personnels est réalisée, en respectant les principes et les obligations légales de PRP, lorsque les droits d'accès aux renseignements personnels sont accordés au personnel de l'organisme public.

PS 3.1 Déterminer les droits d'accès aux renseignements personnels

Indiquer, documenter et appliquer les critères permettant de déterminer les personnes, parmi le personnel de l'organisme public, qui ont qualité (ou sont « autorisées, qualifiées ou habilitées ») à prendre connaissance des renseignements personnels et les renseignements personnels qui sont nécessaires à la réalisation de leurs tâches, et ce, en fonction des principes et des obligations légales de PRP.

PS 3.2 Concevoir et développer le système de manière à respecter les droits d'accès établis

Les différents éléments du système tels que les sous-systèmes, les programmes, les bases de données, les transactions sous forme électronique ou autres, sont développés selon les droits d'accès établis, en respectant les principes et les obligations légales de PRP.

PS 3.3 Mettre en œuvre des mesures visant à permettre au personnel de l'organisme public l'accès aux renseignements personnels dans les seuls cas où cela est justifié

Élaborer, documenter et mettre en œuvre des mesures pour que les membres du personnel de l'organisme public prennent connaissance des renseignements personnels uniquement dans le cadre de l'exercice de leurs fonctions et lorsque cela est nécessaire pour les accomplir adéquatement.

PS 3.4 Décrire, dans le formulaire de déclaration de fichiers des renseignements personnels, les catégories de personnes qui ont accès à des renseignements personnels

La description des catégories de personnes qui ont accès à des renseignements personnels du système dans l'exercice de leurs fonctions. apparaît dans le formulaire de déclaration de fichiers de l'organisme public, en respectant les obligations légales de PRP.

BS 4 UTILISER DES RENSEIGNEMENTS PERSONNELS À L'INTÉRIEUR DE L'ORGANISME PUBLIC

La protection des renseignements personnels est réalisée lors de leur utilisation par le personnel de l'organisme public, en respectant les principes et les obligations légales de PRP.

PS 4.1 Appliquer, dans tous les éléments du système d'information, les règles d'utilisation des renseignements personnels

Appliquer les règles d'utilisation des renseignements personnels convenues, et qui respectent les principes et obligations légales de PRP, dans chacun des éléments du système d'information et des différentes actions associées à ce système.

PS 4.2 Déterminer et évaluer les utilisations des renseignements personnels projetées lors de la modification des systèmes existants

Déterminer les utilisations des renseignements personnels projetées dans le cadre des modifications des systèmes existants, indiquer et documenter les critères à respecter pour les évaluer et réaliser cette évaluation en fonction des principes et des obligations légales de PRP.

PS 4.3 Utiliser, dans la mesure du possible, des renseignements anonymes

Déterminer et mettre en œuvre les conditions à satisfaire pour que les renseignements personnels soient utilisés de façon anonyme et que les résultats (ou produits) de l'utilisation des renseignements personnels soient présentés de façon anonyme.

PS 4.4 Mettre en œuvre des mesures pour prévenir l'utilisation illicite de renseignements personnels au sein de l'organisme public

Élaborer, documenter et mettre en œuvre des mesures techniques et administratives pour prévenir et contrôler toute forme d'utilisation illicite de renseignements personnels.

BS 5 COMMUNIQUER DES RENSEIGNEMENTS PERSONNELS À DES TIERS, À L'EXTÉRIEUR DE L'ORGANISME PUBLIC

La protection des renseignements personnels est réalisée lorsqu'ils sont communiqués à des tiers, à l'extérieur de l'organisme public, en respectant les principes et les obligations légales de PRP.

PS 5.1 Déterminer les situations où l'organisme public projette de communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public

Décrire et documenter les situations où l'organisme public projette de communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public.

PS 5.2 Évaluer les situations où des renseignements personnels seront communiqués à des tiers, à l'extérieur de l'organisme public

Indiquer et documenter les critères à considérer pour évaluer les situations où des renseignements personnels seront communiqués à des tiers, à l'extérieur de l'organisme public ainsi que les mesures de PRP à respecter et réaliser leur évaluation.

PS 5.3 Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité, lorsque des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public

Déterminer, documenter et mettre en œuvre des mesures d'encadrement, de suivi et de sécurité, lorsque des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public.

PS 5.4 Mettre en œuvre des mesures pour obtenir le consentement des personnes

Indiquer, documenter et mettre en œuvre les conditions à respecter pour que le consentement et les modalités de son obtention auprès de la personne concernée par les renseignements personnels respectent les principes et obligations légales de PRP.

BS 6 CONSERVER DES RENSEIGNEMENTS PERSONNELS

La protection des renseignements personnels est réalisée lorsqu'ils sont conservés, en respectant les principes et les obligations légales de PRP ainsi que le calendrier de conservation et les exigences de sécurité.

PS 6.1 Mettre en œuvre des mesures pour conserver les renseignements personnels en respectant le calendrier de conservation, et ce, tout au long de leur cycle de vie

Élaborer, documenter et mettre en œuvre des mesures pour conserver les renseignements personnels actifs, semi-actifs ou inactifs en fonction des délais prévus au calendrier de conservation, et ce, tout au long de leur cycle de vie.

PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels

Élaborer, documenter et mettre en œuvre des mesures de sécurité pour assurer le respect des facteurs de sécurité suivants : disponibilité, intégrité, confidentialité des renseignements personnels, authentification des utilisateurs et irrévocabilité des documents qu'ils rédigent ou des actions qu'ils posent (facteurs DICAI), et ce, tout au long du cycle de vie des renseignements personnels.

BS 7 DÉTRUIRE DES RENSEIGNEMENTS PERSONNELS

La protection des renseignements personnels est réalisée lorsqu'ils sont détruits, en respectant les principes et les obligations légales de PRP et d'élimination des archives publiques.

PS 7.1 Mettre en œuvre des mesures de destruction des renseignements personnels

Élaborer, documenter et mettre en œuvre des mesures techniques et administratives pour détruire des renseignements personnels en fonction des principes et des obligations légales de PRP et du calendrier de conservation.

BS 8 DIFFUSER L'INFORMATION SUR LA GESTION DES RENSEIGNEMENTS PERSONNELS

L'information relative à l'existence des fichiers de renseignements personnels et à la manière dont l'organisation gère et assure la protection des renseignements personnels consignés dans le système d'information, est rendue disponible à toute personne, dans un langage clair et facilement compréhensible, en respectant les principes et obligations légales de PRP.

PS 8.1 Constituer et maintenir à jour un inventaire des fichiers de renseignements personnels créés ou transférés dans le nouveau système ou modifiés dans le système existant et les déclarer à la Commission d'accès à l'information (CAI).

Constituer un inventaire des « fichiers de renseignements personnels » créés, modifiés ou transférés dans le système d'information, les déclarer à la CAI, effectuer leur mise à jour selon des modalités déterminées et informer la CAI de toute modification ultérieure.

PS 8.2 Diffuser l'information sur les modalités de gestion des renseignements personnels

Déterminer et mettre en place des mécanismes pour rendre accessible l'information relative aux modalités de gestion des renseignements personnels, visant à respecter les principes et obligations légales de PRP, et la diffuser aux personnes au sujet desquelles des renseignements personnels sont consignés et utilisés dans le système d'information.

ANNEXE – E **Buts et pratiques de gestion**

BG 1 ATTEINDRE LES BUTS SPÉCIFIQUES DU PROCESSUS DE PRP

Le processus de PRP soutient et rend possible l'atteinte des buts spécifiques de PRP par la réalisation des produits de travail types (ou biens livrables types) de PRP.

PG 1.1 Réaliser les pratiques spécifiques du processus de PRP

Réaliser les pratiques spécifiques du processus PRP afin de développer les produits de travail et de fournir les services attendus pour atteindre les buts spécifiques de PRP.

BG 2 INSTITUTIONNALISER UN PROCESSUS DE PRP « GÉRÉ »

Le processus de protection des renseignements personnels est institutionnalisé comme un processus « géré ».

PG 2.1 Établir une politique relativement au processus de PRP

Établir et maintenir une politique relativement à la planification et à la réalisation du processus de PRP dans un projet de développement d'un système d'information.

PG 2.2 Planifier le processus de PRP

Établir et maintenir le plan pour réaliser le processus de protection des renseignements personnels.

PG 2.3 Fournir les ressources pour le processus de PRP

Affecter des ressources adéquates pour réaliser le processus de protection des renseignements personnels, développer les produits de travail et fournir les services associés à ce processus.

PG 2.4 Assigner la responsabilité du processus de PRP

Assigner la responsabilité et l'autorité aux personnes pour réaliser le processus de PRP, développer les produits de travail et fournir les services associés au processus de protection des renseignements personnels.

PG 2.5 Former le personnel relativement au processus de PRP

Former, au besoin, le personnel ayant à réaliser ou soutenir le processus de protection des renseignements personnels.

PG 2.6 Gérer les configurations du processus de PRP

Placer les produits de travail désignés du processus de protection des renseignements personnels sous les niveaux appropriés de gestion de configuration.

PG 2.7 Identifier et faire participer les parties prenantes pertinentes au processus de PRP

Identifier et faire participer les parties prenantes pertinentes au processus de protection des renseignements personnels, tel qu'il est planifié dans le projet.

PG 2.8 Suivre et contrôler le processus de PRP

Suivre et contrôler le processus de PRP par rapport au plan de réalisation et entreprendre les actions correctives appropriées.

PG 2.9 Évaluer objectivement la conformité du processus de PRP

Évaluer objectivement la conformité du processus de protection des renseignements personnels réalisé dans le projet, par rapport à la description de ce processus, aux standards et aux procédures et traiter les éléments qui ne sont pas conformes.

PG 2.10 **Passer en revue l'état d'avancement du processus de PRP avec la haute direction**

Passer en revue les activités, l'état d'avancement et les résultats du processus de protection des renseignements personnels avec la haute direction et résoudre les éléments problématiques.

BG 3 INSTITUTIONNALISER UN PROCESSUS DE PRP « DÉFINI »

Le processus de protection des renseignements personnels est institutionnalisé comme un processus « défini ».

PG 3.1 **Établir un processus de PRP « défini »**

Établir et maintenir la description du processus « défini » de protection des renseignements personnels.

PG 3.2 **Recueillir l'information d'amélioration du processus de PRP**

Recueillir l'information sur les produits de travail, les mesures, les résultats des mesures et celle provenant de la planification et de la réalisation du processus de PRP afin de soutenir l'utilisation future et l'amélioration du processus de PRP et de ses actifs au sein de l'organisme public.

BG 4 INSTITUTIONNALISER UN PROCESSUS DE PRP « GÉRÉ QUANTITATIVEMENT »

Le processus de protection des renseignements personnels est institutionnalisé comme un processus « géré quantitativement ».

PG 4.1 **Établir des objectifs quantitatifs pour le processus de PRP**

Établir et maintenir des objectifs quantitatifs pour le processus de protection des renseignements personnels concernant la qualité et la performance du processus en se basant sur les besoins du client et les objectifs d'affaires.

PG 4.2 **Stabiliser la performance des sous-processus du processus de PRP**

Stabiliser la performance d'un ou de plusieurs sous-processus du processus de protection des renseignements personnels afin de déterminer sa capacité à atteindre les objectifs quantitatifs établis de qualité et de performance du processus.

BG 5 INSTITUTIONNALISER UN PROCESSUS DE PRP « D'OPTIMISATION »

Le processus de protection des renseignements personnels est institutionnalisé comme un processus « d'optimisation ».

PG 5.1 **S'assurer de l'amélioration continue du processus de PRP**

S'assurer de l'amélioration continue du processus de protection des renseignements personnels, au regard de l'atteinte des objectifs d'affaires pertinents de l'organisme public.

PG 5.2 **Corriger les principales causes des problèmes du processus de PRP**

Déterminer et corriger les principales causes des défauts et des autres problèmes dans le processus de protection des renseignements personnels.

ANNEXE – F Pratiques spécifiques, sous-pratiques et dispositions légales

Nº	PRATIQUES SPÉCIFIQUES	SOUS-PRATIQUES	DISPOSITIONS LÉGALES
PS 1.1	Déterminer tous les renseignements personnels que l'on projette de gérer dans le système	1. Déterminer les renseignements qui sont de nature personnelle.	Article 54 Loi sur l'accès
PS 1.2	Évaluer la nécessité des renseignements personnels que l'on projette de gérer dans le système	1. Déterminer et documenter l'usage projeté des renseignements personnels qui seront gérés dans le système. 2. Déterminer, pour chaque renseignement personnel, s'il est nécessaire à l'exercice des attributions de l'organisme public ou à la mise en œuvre d'un programme dont il a la gestion. Cette activité est désignée comme étant la réalisation du « test de nécessité ». 3. Déterminer des mesures techniques et administratives pour recueillir et consigner des renseignements de façon anonyme.	Article 64 Loi sur l'accès
PS 1.3	Déterminer les sources d'obtention des renseignements personnels	1. Déterminer les situations où les renseignements personnels peuvent être recueillis auprès de la personne concernée. 2. Déterminer les situations où des renseignements personnels, déjà colligés par une personne (autre que la personne concernée) ou par une entreprise privée, seront obtenus auprès de ceux-ci, et déterminer la nécessité des renseignements, leur usage projeté et les mesures de sécurité. 3. Déterminer les situations où des renseignements personnels seront obtenus auprès d'un autre organisme public.	
PS 1.4	Informer la Commission d'accès à l'information (CAI) des situations où des renseignements personnels, déjà colligés par une personne (autre que la personne concernée) ou par une entreprise privée, seront recueillis auprès de celles-ci		Article 66 Loi sur l'accès
PS 1.5	Déterminer les modalités de collecte des renseignements personnels	1. Déterminer les documents (sous forme papier, électronique ou autres) à produire pour recueillir les renseignements personnels et les modalités entourant la collecte au moyen de ces documents. 2. Déterminer si le système permettra de recueillir des renseignements personnels par des moyens électroniques indirects.	Articles 36 et 37 *Code civil du Québec*
PS 1.6	Déterminer les modalités d'information de la personne auprès de qui les renseignements personnels seront recueillis		Article 65 Loi sur l'accès
PS 2.1	Mettre en œuvre les modalités de traitement des demandes d'accès à des renseignements personnels et de rectification de ceux-ci	1. Déterminer les différentes modalités par lesquelles la personne peut exercer son droit d'accès et de rectification auprès de l'organisme public. 2. Déterminer les mesures à prendre pour répondre aux demandes d'accès et de rectification en respectant les obligations légales de PRP. 3. Déterminer les mesures à prendre pour s'assurer de l'identité de la personne qui adresse une demande d'accès ou de rectification.	Article 84 Loi sur l'accès Articles 86 à 90 Loi sur l'accès Article 94 Loi sur l'accès

Nº	PRATIQUES SPÉCIFIQUES	SOUS-PRATIQUES	DISPOSITIONS LÉGALES
PS 2.1	Mettre en œuvre les modalités de traitement des demandes d'accès à des renseignements personnels et de rectification de ceux-ci (suite)	4. Déterminer, en ce qui concerne la rectification des renseignements, le processus à mettre en place pour que le système permette de consigner qu'il y a contestation de la teneur des renseignements par la personne concernée et, lorsque la personne le demande, pour enregistrer la demande de rectification.	Article 91 Loi sur l'accès
		5. Déterminer la modalité de livraison, sans frais, à la personne concernée, d'une copie de tout renseignement personnel modifié ou ajouté ou, selon le cas, une attestation du retrait d'un renseignement personnel.	Article 92 Loi sur l'accès
		6. Déterminer la modalité pour faire suivre, à la demande de la personne concernée, une copie du renseignement rectifié ou de l'annotation au dossier à l'organisme de qui il a obtenu le renseignement ou à tout organisme à qui le renseignement a pu être communiqué dans le cadre d'une entente conclue suivant la Loi sur l'accès.	Article 93 Loi sur l'accès
		7. Déterminer les modalités pour communiquer des renseignements personnels de manière sécuritaire, afin notamment d'en préserver l'intégrité et la confidentialité.	Article 53 Loi sur l'accès
PS 3.1	Déterminer les droits d'accès aux renseignements personnels	1. Indiquer et documenter les critères à respecter pour déterminer quelles sont les personnes qui « ont qualité » (ou sont « autorisées, qualifiées ou habilitées ») pour prendre connaissance des renseignements personnels et les renseignements personnels nécessaires à la réalisation de leurs tâches.	Article 62 Loi sur l'accès
		2. Déterminer les droits d'accès aux renseignements personnels, aux programmes de traitement, à la configuration de production et aux rapports produits par le système (sous forme électronique ou autres), en fonction des éléments suivants : • les processus d'affaires et les unités administratives concernées ; • les catégories de personnes et les profils de tâches et de responsabilités des personnes qui auront accès aux renseignements personnels consignés dans le système ; • la nécessité d'avoir accès aux renseignements personnels, aux programmes de traitements et aux rapports en fonction des critères établis ; • les privilèges d'accès : lecture, modification, copie, destruction, impression ou autres, pour chaque renseignement personnel.	Article 62 Loi sur l'accès
PS 3.2	Concevoir et développer le système de manière à respecter les droits d'accès établis		
PS 3.3	Mettre en œuvre des mesures visant à permettre au personnel de l'organisme public l'accès aux renseignements personnels dans les seuls cas où cela est justifié	1. Élaborer et diffuser un programme de sensibilisation aux membres du personnel.	Article 62 Loi sur l'accès
		2. Déterminer des mesures administratives et techniques afin de prévenir et de contrôler des accès non autorisés par les membres du personnel.	Article 62 Loi sur l'accès
PS 3.4	Décrire, dans le formulaire de déclaration de fichiers des renseignements personnels, les catégories de personnes qui ont accès à des renseignements personnels	1. Informer la personne responsable de la PRP, des catégories de personnes qui ont accès aux renseignements personnels du système.	Articles 62 et 76 4° Loi sur l'accès

Nº	PRATIQUES SPÉCIFIQUES	SOUS-PRATIQUES	DISPOSITIONS LÉGALES
PS 4.1	Appliquer, dans tous les éléments du système d'information, les règles d'utilisation des renseignements personnels	1. Déterminer les règles d'utilisation des renseignements personnels pour ce système.	Article 37 *Code civil du Québec* Articles 65 2°, 72, 73 et 76 5° Loi sur l'accès
		2. Déterminer les éléments du système d'information qui devront être développés selon les règles d'utilisation des renseignements personnels établies pour ce système.	
		3. Déterminer et documenter les conditions particulières à satisfaire pour l'utilisation des renseignements personnels à des fins d'étude, de recherche et de statistique ou de sondage, et les réaliser.	
PS 4.2	Déterminer et évaluer les utilisations des renseignements personnels projetées lors de la modification des systèmes existants	1. Déterminer les finalités visées par l'utilisation des renseignements personnels dans le contexte des changements apportés au système d'information.	
		2. Indiquer et documenter les critères d'évaluation des types d'utilisations des renseignements personnels ainsi que le seuil d'acceptation de ces utilisations.	Article 37 *Code civil du Québec* Articles 65 2°, 72, 73 et 76 5° Loi sur l'accès
		3. Déterminer : • les mandats, les attributions, les programmes et les dispositions légales pertinentes qui autorisent ce type d'utilisation des renseignements personnels ; • si le consentement des personnes à ce type d'utilisation des renseignements personnels peut (ou devrait) être obtenu.	Article 37 *Code civil du Québec* Articles 53, 65 2°, 72, 73 et 76 5° Loi sur l'accès
		4. Déterminer les modalités selon lesquelles le consentement sera obtenu de la personne concernée et produire un formulaire de consentement.	Article 53 Loi sur l'accès
PS 4.3	Utiliser, dans la mesure du possible, des renseignements anonymes	1. Déterminer les conditions à satisfaire pour que des renseignements soient utilisés de façon anonyme et que les produits (rapports sous forme électronique ou autres) résultant de l'utilisation de renseignements personnels, puissent être présentés, rendus accessibles ou diffusés de façon anonyme.	
PS 4.4	Mettre en œuvre des mesures pour prévenir l'utilisation illicite de renseignements personnels au sein de l'organisme public	1. Élaborer et diffuser un programme de sensibilisation aux membres du personnel.	
		2. Déterminer des mesures administratives et techniques afin de prévenir et de contrôler les utilisations illicites de renseignements personnels par le personnel de l'organisme public.	
PS 5.1	Déterminer les situations où l'organisme public projette de communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public	1. Déterminer les situations où l'organisme public projette de communiquer des renseignements personnels et déterminer celles où des renseignements seront communiqués : • avec le consentement de la personne concernée ; • sans le consentement de la personne concernée.	
PS 5.2	Évaluer les situations où des renseignements personnels seront communiqués à des tiers, à l'extérieur de l'organisme public	1. Indiquer et documenter les critères à considérer lors de l'évaluation des situations où des renseignements personnels sont communiqués à tiers, à l'extérieur de l'organisme public, ainsi que les conditions particulières de PRP à satisfaire.	Articles 53, 59, 59.1, 60, 60.1, 61 67 à 70, 171 3° Loi sur l'accès

Nº	PRATIQUES SPÉCIFIQUES	SOUS-PRATIQUES	DISPOSITIONS LÉGALES
		2. Évaluer et documenter les communications de renseignements personnels à des tiers.	Articles 53, 59, 59.1, 60, 60.1, 61, 67 à 70, 171 3° Loi sur l'accès
PS 5.3	Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité, lorsque des renseignements personnels sont communiqués à des tiers, à l'extérieur de l'organisme public	1. Enregistrer ou prévoir l'enregistrement de certaines communications de renseignements personnels.	Articles 59 1° à 4°, 59.1, 60, 60.1 Loi sur l'accès
		2. Constituer, maintenir à jour et rendre disponible un registre des communications des renseignements personnels à des tiers.	Articles 67 à 68.1 de la Loi sur l'accès
		3. Conclure, lorsque cela est requis, une entente écrite avec la tierce partie et la faire approuver par la CAI.	Articles 68 à 70 Loi sur l'accès
		4. Élaborer, dans le cas d'un contrat de services avec un fournisseur de services informatiques, un contrat écrit avec des clauses de PRP et de sécurité	Article 67.2 et 69 Loi sur l'accès
		5. Vérifier, dans le cas des communications de renseignements personnels à un tiers, à des fins d'étude, de recherche ou de statistique, si la CAI a autorisé au préalable la communication, et lorsque cela s'applique, si les exigences relatives au sondage sont respectées.	Article 125 Loi sur l'accès
		6. Déterminer, documenter et mettre en œuvre des mesures de sécurité lors des communications à des tiers, à l'extérieur de l'organisme public.	Articles 67.2, 68, 68.1 et 69 Loi sur l'accès
PS 5.4	Mettre en œuvre des mesures pour obtenir le consentement des personnes	1. Déterminer les modalités selon lesquelles le consentement sera obtenu auprès de la personne concernée.	Article 53 Loi sur l'accès
		2. Produire un formulaire du consentement.	
		3. Faire approuver, par le répondant de la PRP dans le projet ou le responsable de la PRP de l'organisme public, le libellé du consentement et les modalités selon lesquelles il sera obtenu.	
PS 6.1	Mettre en œuvre des mesures pour conserver les renseignements personnels en respectant le calendrier de conservation, et ce, tout au long de leur cycle de vie	1. Élaborer les règles de conservation des renseignements personnels en déterminant, d'une part, les durées de conservation pour les renseignements personnels qui : • sont d'utilité courante (exploitation du système) ; • sont occasionnellement utilisés à des fins administratives ou légales (semi-actifs). En déterminant, d'autre part, le mode de disposition des renseignements personnels qui : • ne sont plus utilisés à des fins administratives ou légales (inactifs) et sont destinés à être détruits ; ou • en ce qui a trait aux renseignements personnels ayant une valeur de recherche ou une valeur historique, sont destinés à être conservés de façon permanente.	Articles 7, 8 et 15 *Loi sur les archives*
		2. Déterminer les mesures techniques et administratives pour conserver (ou « stocker » ou « archiver ») les renseignements personnels identifiés dans la sous-pratique nº 1 en fonction des délais prévus au calendrier de conservation.	
		3. Mettre en œuvre les mesures techniques et administratives décrites dans la sous-pratique nº 2.	
PS 6.2	Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des renseignements personnels	1. Déterminer et documenter des mesures de sécurité techniques et administratives tout au long du cycle de vie des renseignements personnels.	Chapitre 3 Loi sur l'accès

Nº	PRATIQUES SPÉCIFIQUES	SOUS-PRATIQUES	DISPOSITIONS LÉGALES
		2. Déterminer et documenter des mesures techniques et administratives pour que les renseignements personnels soient tenus à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis.	Article 72 Loi sur l'accès
		3. Mettre en œuvre des mesures de sécurité techniques et administratives, tout au long du cycle de vie des renseignements personnels.	Chapitre 3 Loi sur l'accès
PS 7.1	Mettre en œuvre des mesures de destruction des renseignements personnels	1. Déterminer, en respectant les délais de conservation établis par le calendrier de conservation ainsi que leur caractère confidentiel, les mesures techniques et administratives pour détruire des renseignements personnels.	Article 73 Loi sur l'accès Articles 7, 8 et 15 *Loi sur les archives*
		2. Effectuer la destruction des renseignements personnels selon les modalités décrites.	
PS 8.1	Constituer et maintenir à jour un inventaire des fichiers de renseignements personnels créés ou transférés dans le nouveau système ou modifié dans le système existant et les déclarer à la Commission d'accès à l'information (CAI)	1. En référant aux processus d'affaires qu'ils supportent, déterminer parmi les renseignements personnels à recueillir et consigner dans le système et ses sous-systèmes, ceux qui correspondent à la définition légale de « fichiers de renseignements personnels » c'est-à-dire qui répondent à l'une ou l'autre des deux conditions suivantes : 1° sont identifiés ou se présentent de façon à être retrouvés par référence au nom d'une personne ou à un signe ou symbole propre à celle-ci ; ou 2° ont servi ou sont destinés à servir pour une décision concernant une personne.	Article 71 Loi sur l'accès
		2. Déterminer un format d'inventaire des fichiers de renseignements personnels.	Article 76 Loi sur l'accès
		3. Déterminer les modalités de mise à jour des déclarations de fichiers de renseignements personnels et les maintenir à jour.	Article 77 Loi sur l'accès
		4. Informer le responsable de la PRP de l'organisme public des « fichiers de renseignements personnels » créés ou transférés dans le système d'information ou de leur mise à jour.	
		5. Déclarer les fichiers de renseignements personnels à la CAI et l'informer des mises à jour.	Article 77 Loi sur l'accès
PS 8.2	Diffuser l'information sur les modalités de gestion des renseignements personnels	1. Déterminer l'information portant sur les modalités de gestion des renseignements personnels du système d'information, qui sera diffusée aux personnes pour lesquelles des renseignements personnels sont consignés et utilisés dans le système d'information.	
		2. Établir un plan de diffusion de l'information sur les modalités de gestion des renseignements personnels.	
		3. Produire l'information à diffuser sur les modalités de gestion des renseignements personnels.	
		4. Diffuser l'information.	

ANNEXE – G **Produits de travail types (biens livrables types) des buts spécifiques**

Nº	PRODUIT DE TRAVAIL TYPE (BIEN LIVRABLE TYPE)	Nº PRATIQUE ASSOCIÉE
1	Liste des renseignements personnels que l'organisme public projette de recueillir et consigner dans le système de même que ceux produits par celui-ci (sur support électronique ou autre).	PS 1.1
2	Liste des renseignements personnels à recueillir et consigner dans le système ou à produire par celui-ci, description de l'usage auquel ils sont destinés et justification de leur nécessité.	PS 1.2
3	Liste des renseignements rattachés à des personnes physiques, à recueillir et consigner sous forme anonyme dans le système.	PS 1.2
4	Mesures techniques et administratives pour rendre les renseignements anonymes lorsque cela est requis.	PS 1.2
5	Liste des sources auprès desquelles des renseignements personnels seront recueillis : • la personne concernée ; • une entreprise privée ou une personne (autre que la personne concernée) avec indication de la nécessité des renseignements, leur usage projeté et les mesures de sécurité ; • un autre organisme public.	PS 1.3
6	Document d'information à l'intention de la CAI décrivant les renseignements personnels à recueillir auprès d'une personne (autre que la personne concernée) ou d'une entreprise privée, leur usage, leur nécessité et les mesures de protection et de sécurité.	PS 1.4
7	Description des modalités de collecte des renseignements personnels.	PS 1.5
8	Document décrivant les modalités d'information des personnes, auprès de qui les renseignements personnels seront recueillis, comprenant les éléments suivants (article 65, Loi sur l'accès) : 1° le nom et l'adresse de l'organisme public au nom de qui la collecte est faite ; 2° l'usage auquel ce renseignement est destiné ; 3° les catégories de personnes qui auront accès à ces renseignements ; 4° le caractère obligatoire ou facultatif des renseignements personnels ; 5° les conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande de renseignements personnels ; 6° les droits d'accès et de rectification prévus par la loi.	PS 1.6
9	Liste des mécanismes mis en place pour : • traiter les demandes d'accès à des renseignements personnels et de rectification de ceux-ci en respectant les obligations légales de PRP, notamment les délais prescrits par la loi ainsi que ceux énoncés dans la « Déclaration de services aux citoyens » à cet égard ; • vérifier l'identité de la personne concernée avant de lui communiquer les renseignements demandés ; • préserver le caractère confidentiel des renseignements communiqués.	PS 2.1
10	Liste des critères à respecter pour établir les droits d'accès.	PS 3.1
11	Description des catégories de personnes qui ont accès aux renseignements personnels, aux programmes de traitement, à la configuration de production et aux rapports produits par le système, sous forme électronique ou autres, ainsi que de leurs privilèges d'accès (lecture, modification, copie, destruction, impression ou autres). Cette description est faite en fonction des processus d'affaires et des unités administratives (profils d'accès).	PS 3.1
12	Table de référence croisée entre les différents types de profils d'accès et les différents éléments du système tels que les sous-systèmes, les programmes et les transactions sous forme électronique ou autres.	PS 3.2
13	Architecture du système compatible avec les exigences de PRP, notamment des droits d'accès.	PS 3.2
14	Programme de sensibilisation concernant l'accès aux renseignements personnels et destiné à être diffusé aux membres du personnel.	PS 3.3

Nº	PRODUIT DE TRAVAIL TYPE (BIEN LIVRABLE TYPE)	Nº PRATIQUE ASSOCIÉE
15	Liste des mesures administratives et techniques, établies *a priori*, afin de prévenir des accès non autorisés par les membres du personnel.	PS 3.3
16	Liste des mesures administratives et techniques, établies *a posteriori*, afin de contrôler des accès non autorisés par les membres du personnel.	PS 3.3
17	Description des catégories de personnes qui ont accès aux renseignements personnels dans l'exercice de leurs fonctions, dans les formulaires de déclarations de fichiers.	PS 3.4
18	Éléments du système d'information développés selon les règles d'utilisation des renseignements personnels établies pour ce système.	PS 4.1
19	Liste des conditions particulières à satisfaire par l'organisme public dans le cas d'utilisations des renseignements personnels à des fins d'étude, de recherche, de statistique ou de sondage.	PS 4.1
20	Liste des types d'utilisations et documentation de leur justification (légale et administrative).	PS 4.2
21	Lorsque cela est requis, formulaire de consentement pour les renseignements personnels pour lesquels une nouvelle utilisation est projetée et, description des modalités selon lesquelles il sera obtenu de la personne concernée.	PS 4.2
22	Documentation, au besoin, des raisons justifiant pourquoi le consentement des personnes à la nouvelle utilisation des renseignements personnels ne sera pas obtenu.	PS 4.2
23	Mesures d'information, au besoin, des personnes concernées par la nouvelle utilisation de renseignements personnels sans leur consentement.	PS 4.2
24	Liste des conditions à satisfaire pour que des renseignements personnels soient utilisés de façon à ce que les produits (rapports sous forme électronique ou autres) résultant de l'utilisation de renseignements personnels, puissent être présentés de façon anonyme.	PS 4.3
25	Liste des types de résultats des traitements des renseignements personnels (principalement les rapports) présentés de façon anonyme.	PS 4.3
26	Programme de sensibilisation des membres du personnel.	PS 4.4
27	Liste des mesures techniques et administratives pour prévenir et contrôler toute forme d'utilisation illicite des renseignements personnels, que l'utilisation soit faite sous forme automatisée, manuelle ou autres.	PS 4.4
28	Liste des situations où l'organisme projette de communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public, avec indication des processus d'affaires concernés, des renseignements personnels communiqués et des personnes, des organismes ou des entreprises privées qui les recevront.	PS 5.1
29	Liste des communications de renseignements personnels à des tiers, qui sont autorisées avec ou sans le consentement de la personne concernée.	PS 5.2
30	Dans le cas où des renseignements personnels seraient communiqués à des tiers sans le consentement, liste des informations suivantes : • processus d'affaires concernés ; • renseignements personnels communiqués ; • personnes, organismes ou entreprises privées qui les recevront ; • conditions particulières de PRP à satisfaire pour effectuer ce type de communication.	PS 5.2
31	Les mesures d'encadrement suivantes, lorsque cela s'applique : • entente écrite avec la tierce partie (personne, organisme ou entreprise privée) et approuvée par la CAI concernant la communication de renseignements personnels à des tiers (articles 68 à 70, Loi sur l'accès) ; • entente écrite, dite « administrative » avec la tierce partie concernant la communication de renseignements personnels à des tiers (articles 67, 67.1 ou autres communications autorisées par la Loi sur l'accès) ; • contrat écrit avec un mandataire spécifiant les mesures de PRP exigées par la loi (article 67.2, Loi sur l'accès) ; • liste des mesures d'encadrement prises lorsque l'organisme public communique des renseignements personnels à des fins d'étude, de recherche et de statistique, à la suite d'une autorisation de recherche de la CAI (article 125, Loi sur l'accès) ; • liste des mesures d'encadrement prises lorsque l'organisme public communique des renseignements personnels à des fins de sondage.	PS 5.3

Nº	PRODUIT DE TRAVAIL TYPE (BIEN LIVRABLE TYPE)	Nº PRATIQUE ASSOCIÉE
32	Liste des mesures administratives et techniques de suivi et de sécurité des renseignements personnels lorsqu'ils sont communiqués à des tiers, à l'extérieur de l'organisme public.	PS 5.3
33	Éléments du système d'information développé ou modifié, qui permettent de consigner des communications de renseignements personnels à des tiers et de maintenir cette consignation à jour. Cette consignation pourra se faire dans un document papier ou électronique.	PS 5.3
34	Description des modalités d'obtention du consentement.	PS 5.4
35	Formulaire de consentement.	PS 5.4
36	Calendrier de conservation ou partie du calendrier de conservation relatifs aux renseignements personnels du système d'information en développement.	PS 6.1
37	Liste des mesures techniques et administratives pour conserver des renseignements personnels, incluant ceux qui sont destinés à être conservés de façon permanente, en respectant les délais prévus au calendrier de conservation.	PS 6.1
38	Éléments du système d'information développé qui implantent les mesures techniques et administratives de conservation définies par le produit de travail type nº 2 (nº 37 de cette annexe).	PS 6.1
39	Liste des mesures de sécurité techniques et administratives mises en œuvre tout au long du cycle de vie des renseignements personnels.	PS 6.2
40	Éléments du système d'information développé ou modifié qui implantent les mesures techniques et administratives de sécurité définies par le produit de travail type nº 2 (nº 39 de cette annexe).	PS 6.2
41	Liste des mesures techniques et administratives pour détruire des renseignements personnels.	PS 7.1
42	Éléments du système d'information développé ou modifié qui implantent les mesures techniques et administratives de destruction définies par le produit de travail type nº 1 (nº 41 de cette annexe).	PS 7.1
43	Inventaire des « fichiers de renseignements personnels » créés ou transférés dans le nouveau système ou modifiés dans le système existant et, comportant pour chaque fichier, les indications suivantes (article 76, Loi sur l'accès) : 1° la désignation de chaque fichier, les types de renseignements personnels qu'il contient, l'usage projeté de ces renseignements et le mode de gestion de chaque fichier ; 2° la provenance des renseignements personnels versés à chaque fichier ; 3° les catégories de personnes concernées par les renseignements personnels versés à chaque fichier ; 4° les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions ; 5° les mesures de sécurité prises pour assurer le caractère confidentiel des renseignements personnels et leur utilisation suivant les fins pour lesquelles ils ont été recueillis ; 6° le titre, l'adresse et le numéro de téléphone de la personne responsable de la protection des renseignements personnels ; 7° les modalités d'accès offertes à la personne concernée.	PS 8.1
44	Formulaires de déclaration de fichiers complétés pour chaque fichier de renseignements personnels, mis à jour et transmis à la CAI (article 76 et 77, Loi sur l'accès).	PS 8.1
45	Information à diffuser sur les modalités de gestion des renseignements personnels.	PS 8.2
46	Plan de diffusion de l'information sur les modalités de gestion des renseignements personnels.	PS 8.2
47	Document de diffusion de l'information sur les modalités de gestion des renseignements personnels. Ce document peut être produit sur différents médias.	PS 8.2

ANNEXE – H Produits de travail types (biens livrables types) des buts de gestion

Nº	PRODUIT DE TRAVAIL TYPE (BIEN LIVRABLE)	Nº PRATIQUE ASSOCIÉE
1	Engagement formel et documenté de la part de la direction du projet relativement à la réalisation du processus de PRP dans le projet de développement.	PG 2.1
2	Plan de communication et de diffusion des orientations, de la politique ou de la directive sur la PRP dans le projet de développement.	PG 2.1
3	Plan de réalisation du processus de PRP intégré dans le manuel d'organisation et de gestion du projet. Le plan de réalisation du processus de PRP inclut typiquement les éléments suivants : • la description du processus de PRP, cette description peut se baser sur les pratiques spécifiques décrites dans la Partie 1 (PS 1.1 à PS 8.2) ; • les standards pour les produits de travail et les services du processus de PRP ; • les exigences pour les produits de travail et les services du processus de PRP ; • les objectifs particuliers de performance du processus de PRP (par exemple : la qualité, la période, la durée et l'utilisation des ressources) ; • les interrelations entre les activités, les produits de travail et les services du processus de PRP ; • les personnes et les ressources (incluant le financement et les outils) nécessaires à la réalisation du processus de PRP ; • l'assignation de la responsabilité et de l'autorité ; • la formation nécessaire pour réaliser et soutenir le processus de PRP ; • les produits de travail à placer sous le contrôle de la gestion de configuration et le niveau de gestion de configuration pour chacun de ces produits ; • les exigences de mesure pour offrir « une vue » sur la performance du processus, ses produits de travail et ses services ; • l'implication des parties prenantes pertinentes ; • les activités pour suivre et contrôler le processus de PRP ; • les activités d'évaluation objective du processus de PRP et de ses produits de travail ; • les activités de revue, par la direction, du processus de PRP et de ses produits de travail.	PG 2.2
4	Description des ressources requises pour réaliser le processus de PRP et indication du moment où elles sont requises : financement, personnes, facilités physiques et outils appropriés.	PG 2.3
5	Désignation d'une personne pour assurer la réalisation des produits de travail types (biens livrables types) relatifs à la PRP dans le cadre du projet et en rendre compte (répondant de la PRP dans le projet).	PG 2.4
6	Description des rôles et des responsabilités des autres parties prenantes pertinentes au processus de PRP.	PG 2.4
7	Description des compétences requises du personnel pour réaliser le processus de PRP.	PG 2.5
8	Plan de sensibilisation et de formation et sa diffusion.	PG 2.5
9	Pour réaliser les produits de travail du processus de PRP reliés à cette pratique se référer aux produits de travail définis dans le processus « Gestion des configurations » où le niveau de gestion de configuration approprié pourra être établi. Cependant, il convient de souligner ces produits de travail types : 1. Liste des éléments de configuration. 2. Historique de révision des éléments de configuration.	PG 2.6
10	Pour réaliser les produits de travail du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans les processus « Planification de projet » et « Suivi et contrôle de projet ». Cependant, il convient de souligner ces produits de travail types : 1. Demandes documentées de participation des parties prenantes. 2. Engagements de participation.	PG 2.7

Nº	PRODUIT DE TRAVAIL TYPE (BIEN LIVRABLE)	Nº PRATIQUE ASSOCIÉE
11	Pour réaliser les produits de travail du processus de PRP reliés à cette pratique se référer aux produits de travail définis dans les processus « Suivi et contrôle de projet » et « Analyse et mesure ». Cependant, il convient de souligner ces produits de travail types : 1. Mesures sur la performance du processus. 2. Liste des actions correctives.	PG 2.8
12	Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Assurance qualité du processus et du produit ». Cependant, il convient de souligner ces produits de travail types : 1. Liste des éléments qui ne sont pas conformes au processus de PRP. 2. Résultats découlant d'actions visant à traiter les éléments non conformes, tel qu'un plan ajusté du processus de PRP.	PG 2.9
13	Compte rendu de la revue, incluant les actions prévues pour résoudre les problèmes soumis à la haute direction.	PG 2.10
14	Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Gestion de projet intégrée ».	PG 3.1
15	Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Gestion de projet intégrée ».	PG 3.2
16	Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Gestion quantitative de projet ».	PG 4.1
17	Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Gestion quantitative de projet ».	PG 4.2
18	Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Innovation organisationnelle et déploiement ».	PG 5.1
19	Pour réaliser les produits de travail types du processus de PRP reliés à cette pratique, se référer aux produits de travail définis dans le processus « Analyse causale et résolution ».	PG 5.2

ANNEXE – I **Aide-mémoire complémentaires**

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 1.1

DÉTERMINER LES BUTS SPÉCIFIQUES DE PRP À ATTEINDRE DANS LE PROJET

UTILITÉ

- Déterminer, dès les études préliminaires du projet, les buts spécifiques de PRP à atteindre dans le système d'information développé. Ils sont déterminés en fonction du cheminement projeté des renseignements personnels. Se référer par la suite aux pratiques, sous-pratiques et biens livrables correspondant à chacun des buts spécifiques pour réaliser le processus de PRP.

DOCUMENTS COMPLÉMENTAIRES

- aide-mémoire nº 2.1 à 2.8 Déterminer les pratiques spécifiques de PRP à réaliser dans le projet
- annexe D – Buts et pratiques spécifiques
- annexe G – Produits de travail types (biens livrables types) des buts spécifiques
- figure 3 – Schéma du cycle de vie de la PRP

PARTIE 1 – RÉALISER LA PRP	BS 1 À BS 8	LES BUTS SPÉCIFIQUES BS 1 À BS 8 COUVRENT TOUT LE CYCLE DE VIE DE LA PRP

AIDE-MÉMOIRE nº 1.1 DÉTERMINER LES BUTS SPÉCIFIQUES DE PRP À ATTEINDRE DANS LE PROJET

Projet : Sous-projet :

Questions relatives au cheminement des renseignements personnels dans le système d'information	Oui / Non	But spécifique de PRP à atteindre Buts	Commentaires
1. Est-ce que des renseignements personnels seront recueillis, soit auprès de la personne concernée, soit auprès d'autres personnes, d'entreprises privées ou d'autres organismes publics ? *Si vous répondez « oui » à cette question, les buts spécifiques BS 1 à BS 8 seront à réaliser, à l'exception du but spécifique BS 5.*		BS 1 Recueillir des renseignements personnels	
		BS 2 Traiter les demandes d'accès à des renseignements personnels et de rectification	
		BS 3 Attribuer au personnel, les droits d'accès aux renseignements personnels	
		BS 4 Utiliser des renseignements personnels à l'intérieur de l'organisme public	
		BS 6 Conserver des renseignements personnels	
		BS 7 Détruire des renseignements personnels	
		BS 8 Diffuser l'information sur la gestion des renseignements personnels	
2. Les renseignements personnels seront-ils communiqués ou accessibles à des tiers (personnes, organismes publics, entreprises ou fournisseurs) ? *Si vous répondez « oui » à cette question, tous les buts spécifiques seront à réaliser.*		BS 5 Communiquer des renseignements personnels à des tiers, à l'extérieur de l'organisme public	

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 1.2

DÉTERMINER LES RÔLES ET RESPONSABILITÉS DES INTERVENANTS À L'ÉGARD DES BUTS SPÉCIFIQUES DE PRP

UTILITÉ

- déterminer les rôles et responsabilités des intervenants relativement à la réalisation des biens livrables associés aux 8 buts spécifiques de PRP à atteindre dans le système d'information développé

DOCUMENTS COMPLÉMENTAIRES

- annexe G – Produits de travail types (biens livrables types) des buts spécifiques
- schéma de la Partie 1 – Réaliser la PRP dans les projets de développement, présentant un aperçu rapide des pratiques associées à chacun des buts
- tableau 1 – Légende des rôles des parties prenantes dans un projet de développement
- tableau 2 – Légende des responsabilités des parties prenantes dans un projet de développement

LÉGENDE DES SYMBOLES À UTILISER POUR COMPLÉTER L'AIDE-MÉMOIRE

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable de la sécurité de l'information . . . . . .RS
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Pilote de projet . . . . . .PP
Répondant du processus de PRP dans le projet . . . .RPPP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

PARTIE 1 – RÉALISER LA PRP	BS 1 À BS 8	LES BUTS SPÉCIFIQUES BS 1 À BS 8 COUVRENT TOUT LE CYCLE DE VIE DE LA PRP

AIDE-MÉMOIRE nº 1.2 DÉTERMINER LES RÔLES ET RESPONSABILITÉS DES INTERVENANTS À L'ÉGARD DES BUTS SPÉCIFIQUES DE PRP

Projet :

Sous-projet :

Buts spécifiques	Parties prenantes au processus de PRP dans un projet *En vous référant aux biens livrables associés à chaque but, indiquez les responsabilités dans les cases.*									
	Direction et autres					Membres de l'équipe de développement				
	RPRP	Conseiller juridique	Vérificateur interne	Responsable de la sécurité	Responsable des méthodes	Directeur de projet	Chef et chargé de projet	Pilote de projet	Répondant de la PRP	Autres membres
BS 1 Recueillir des renseignements personnels (RP)										
BS 2 Traiter les demandes d'accès et de rectification										
BS 3 Attribuer au personnel, les droits d'accès aux RP										
BS 4 Utiliser des RP à l'intérieur de l'organisme public										
BS 5 Communiquer des RP à des tiers, à l'extérieur de l'organisme public										
BS 6 Conserver des RP										
BS 7 Détruire des RP										
BS 8 Diffuser l'information sur la gestion des RP										

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 3.1

DÉTERMINER LES BUTS DE GESTION DE LA PRP À ATTEINDRE DANS LE PROJET

UTILITÉ

- déterminer à quel niveau de capacité (ou de gestion) l'organisme public désire fonctionner en ce qui concerne la mise en œuvre du processus de PRP. On se référera par la suite aux pratiques, sous-pratiques et biens livrables correspondant à chacun des buts de gestion pour réaliser le processus de PRP

DOCUMENTS COMPLÉMENTAIRES

- schéma de la Partie 2 – Gérer la PRP dans les projets de développement
- aide-mémoire nº 4.1 à 4.5 – Déterminer les pratiques de gestion de la PRP à réaliser dans le projet
- annexe E – Buts et pratiques de gestion
- annexe H – Produits de travail types (biens livrables types) des buts de gestion
- figure 6 – Interrelations entre les niveaux de capacité

LÉGENDE DES SYMBOLES À UTILISER POUR COMPLÉTER L'AIDE-MÉMOIRE

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Haute direction . . . . . .HD
Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Pilote de projet . . . . . .PP
Répondant du processus de PRP dans le projet . . . .RPPP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

PARTIE 2 – GÉRER LA PRP	BG 1 À BG 5	LES BUTS DE GESTION S'ÉCHELONNENT SELON 5 NIVEAUX DE CAPACITÉ

AIDE-MÉMOIRE nº 3.1 DÉTERMINER LES BUTS DE GESTION DE LA PRP À ATTEINDRE DANS LE PROJET

Projet : Sous-projet :

Questions	Oui / Non	Buts de gestion correspondants
Niveau de capacité 1 Désirez-vous réaliser les pratiques des buts spécifiques du processus de PRP pour tous les projets de développement des systèmes d'information, sans toutefois les réaliser de façon planifiée ni effectuer un suivi et un contrôle ?		BG 1 Atteindre les buts spécifiques du processus de PRP
Niveau de capacité 2 Désirez-vous planifier, réaliser, documenter, suivre, contrôler ou passer en revue les pratiques spécifiques du processus de PRP dans tous les projets ?		BG 2 Institutionnaliser un processus de PRP « géré »
Niveau de capacité 3 Désirez-vous établir un cadre organisationnel qui permet de réaliser les pratiques spécifiques de PRP à partir d'une même façon de faire pour tous les projets de développement des systèmes d'information impliquant des renseignements personnels (processus de PRP standardisé) ?		BG 3 Institutionnaliser un processus de PRP « défini »
Niveau de capacité 4 Désirez-vous être en mesure non seulement de reproduire le processus de PRP d'un projet à un autre, mais également de prédire quantitativement son comportement, c'est-à-dire le placer sous contrôle statistique ?		BG 4 Institutionnaliser un processus de PRP « géré quantitativement »
Niveau de capacité 5 Désirez-vous mettre l'accent sur l'amélioration continue du processus de PRP sur la base d'information quantitative pour tous les projets de développement des systèmes d'information ?		BG 5 Institutionnaliser un processus de PRP « d'optimisation »

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 3.2

DÉTERMINER LES RÔLES ET RESPONSABILITÉS DES INTERVENANTS À L'ÉGARD DE LA GESTION DE LA PRP DANS LE PROJET

UTILITÉ

- déterminer les rôles et responsabilités des intervenants à l'égard de la réalisation des pratiques et biens livrables associés au but de gestion BG 2 à atteindre dans le projet

DOCUMENTS COMPLÉMENTAIRES

- schéma de la Partie 2 – Gérer la PRP dans les projets de développement, pour avoir un aperçu des pratiques associées au but BG 2 Institutionnaliser un processus de PRP « géré »
- annexe H – Produits de travail types (biens livrables types) des buts de gestion

LÉGENDE DES SYMBOLES À UTILISER POUR COMPLÉTER L'AIDE-MÉMOIRE

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Haute direction . . . . . .HD
Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Pilote de projet . . . . . .PP
Répondant du processus de PRP dans le projet . . . .RPPP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

PARTIE 2 – GÉRER LA PRP	NIVEAU DE CAPACITÉ 2 BG 2	INSTITUTIONNALISER UN PROCESSUS DE PRP « GÉRÉ »

AIDE-MÉMOIRE nº 3.2 — DÉTERMINER LES RÔLES ET RESPONSABILITÉS DES INTERVENANTS À L'ÉGARD DE LA GESTION DE LA PRP DANS LE PROJET

Projet : Sous-projet :

Pratiques	Nº	Parties prenantes au processus de PRP dans un projet *En vous référant aux biens livrables associés aux pratiques, indiquez les responsabilités dans les cases.*									
		Direction et autres					Membres de l'équipe de développement				
		Haute direction	RPRP	Conseiller juridique	Vérificateur interne	Responsable des méthodes	Directeur de projet	Chef et chargé de projet	Pilote de projet	Répondant de la PRP	Autres membres
Établir une politique relativement au processus de PRP	PG 2.1										
Planifier le processus de PRP	PG 2.2										
Fournir les ressources	PG 2.3										
Assigner la responsabilité	PG 2.4										
Former le personnel relativement au processus de PRP	PG 2.5										
Gérer les configurations du processus de PRP	PG 2.6										
Identifier et faire participer les parties prenantes pertinentes	PG 2.7										
Suivre et contrôler le processus de PRP	PG 2.8										
Évaluer objectivement la conformité du processus de PRP	PG 2.9										
Passer en revue l'état d'avancement du processus de PRP avec la haute direction	PG 2.10										

INFORMATIONS PERTINENTES POUR L'UTILISATION DE L'AIDE-MÉMOIRE Nº 3.3

DÉTERMINER LES RÔLES ET RESPONSABILITÉS DES INTERVENANTS À L'ÉGARD DE LA GESTION DE LA PRP DANS LE PROJET

UTILITÉ

- déterminer les rôles et responsabilités des intervenants à l'égard de la réalisation des pratiques et biens livrables associés aux buts de gestion BG 3, BG 4 et BG 5 à atteindre dans le projet

DOCUMENTS COMPLÉMENTAIRES

- schéma de la Partie 2 – Gérer la PRP dans les projets de développement, pour avoir un aperçu des pratiques associées aux buts *BG 3 Institutionnaliser un processus de PRP « défini »*, *BG 4 Institutionnaliser un processus de PRP « géré quantitativement »* et *BG 5 Institutionnaliser un processus de PRP « d'optimisation »*
- annexe H – Produits de travail types (biens livrables types) des buts de gestion

LÉGENDE DES SYMBOLES À UTILISER POUR COMPLÉTER L'AIDE-MÉMOIRE

RÔLE : réfère à la fonction exercée par la personne

Direction et autres

Haute direction . . . . . .HD
Responsable de la PRP de l'organisme . . . . . .RPRP
Conseiller juridique . . . . . .CJ
Vérificateur interne VI
Responsable des méthodes . . . . . .RM

Membres de l'équipe de développement

Directeur de projet . . . . . .DP
Chef et chargé de projet . . . . . .CP
Pilote de projet . . . . . .PP
Répondant du processus de PRP dans le projet . . . .RPPP
Autres membres . . . . . .A

RESPONSABILITÉ : réfère aux types de tâches dont la personne doit s'acquitter et répondre de leur exécution

Responsable . . . . . .R
Réalise . . . . . .Ré
Offre un soutien et conseille . . . . . .SC
Vérifie . . . . . .Vé
Valide . . . . . .Va
Approuve . . . . . .A
Coordonne C

PARTIE 2–GÉRER LA PRP	NIVEAUX DE CAPACITÉ 3, 4, 5 BG 3, BG 4, BG 5	INSTITUTIONNALISER UN PROCESSUS DE PRP « DÉFINI » (BG 3), « GÉRÉ QUANTITATIVEMENT » (BG 4) ET « D'OPTIMISATION » (BG 5)

AIDE-MÉMOIRE nº 3.3 DÉTERMINER LES RÔLES ET RESPONSABILITÉS DES INTERVENANTS À L'ÉGARD DE LA GESTION DE LA PRP DANS LE PROJET

Projet :

Sous-projet :

Pratiques	Nº	Parties prenantes au processus de PRP dans un projet *En vous référant aux biens livrables associés aux pratiques, indiquez les responsabilités dans les cases.*									
		Direction et autres					Membres de l'équipe de développement				
		Haute direction	RPRP	Conseiller juridique	Vérificateur interne	Responsable des méthodes	Directeur de projet	Chef et chargé de projet	Pilote de projet	Répondant de la PRP	Autres membres
Établir un processus de PRP « défini »	PG 3.1										
Recueillir l'information d'amélioration du processus de PRP	PG 3.2										
Établir des objectifs quantitatifs pour le processus de PRP	PG 4.1										
Stabiliser la performance des sous-processus du processus de PRP	PG 4.2										
S'assurer de l'amélioration continue du processus de PRP	PG 5.1										
Corriger les principales causes des problèmes du processus de PRP	PG 5.2										

ANNEXE – J Cadre légal et administratif à l'égard du respect de la vie privée, de la PRP et de la sécurité et directives nationales et internationales

CADRE LÉGAL ET ADMINISTRATIF QUÉBÉCOIS À L'ÉGARD DU RESPECT DE LA VIE PRIVÉE, DE LA PRP ET DE LA SÉCURITÉ DE L'INFORMATION*

Au Québec, le respect de la vie privée, la PRP et la sécurité de l'information sont régis par un cadre légal et administratif qui se retrouve dans les documents suivants :

- la *Charte des droits et libertés de la personne* du Québec (L.R.Q., c.C-12, articles 5 et 44), disponible sur le site de l'Éditeur officiel : www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_12/C12.html
- le *Chapitre 3 du Code civil du Québec « Du respect de la réputation et de la vie privée »* (L.Q. 1991, c.64), disponible sur le site de l'Éditeur officiel : www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/CCQ/CCQ_1.html
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) qui s'applique aux organismes publics, disponible sur le site de l'Éditeur officiel : www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html
- la *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1) qui s'applique aux entreprises privées, disponible sur le site de l'Éditeur officiel : www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1.html
- la *Loi sur l'administration publique* (L.Q. 2000, chapitre 8. R.P.G, 11221), disponible sur le site de l'Éditeur officiel : www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_6_01/A6_01.html
- la *Loi sur les archives* (L.R.Q., c. A-21.1), disponible sur le site de l'Éditeur officiel : http://www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_21_1/A21_1.html
- la *Loi concernant le cadre juridique des technologies de l'information* (L.Q.2001, c. C-1.1), disponible sur le site de l'Éditeur officiel : www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_1_1/C1_1.html

* Le cadre administratif sur la sécurité décrit dans cette annexe n'est pas exhaustif. Il couvre uniquement quelques-unes des mesures d'encadrement de la sécurité qui s'appliquent aux organismes publics. Pour obtenir plus d'information à ce sujet, consultez l'intranet du Conseil du trésor sur la sécurité et l'ICPG : http://www.inforoute-gouvernementale.qc/securite.htm

- le *Règlement sur les frais exigibles pour la transcription, la reproduction et la transmission de documents et de renseignements nominatifs,* disponible sur le site de l'Éditeur officiel : www.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=3&file=/A_2_1/A2_1R1_1.HTM
- les lois sectorielles qui encadrent les activités des organismes publics, disponibles sur le site de l'Éditeur officiel : www.publicationsduquebec.gouv.qc.ca/home.php#
- *la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale,* disponible sur le site du Conseil du trésor : www.tresor.gouv.qc.ca/doc/acrobat/dirsec1.pdf
- *la Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégés par un droit d'auteur, emmagasinés dans un équipement micro-informatique ou un support informatique amovible,* disponible sur le site du Conseil du trésor : www.tresor.gouv.qc.ca/doc/acrobat/directivemicro99.pdf
- le *Rapport du comité de travail sur la gestion des diagnostics médicaux des employés de la fonction publique mandaté par le Comité interministériel sur la protection des renseignements personnels.* Secrétariat du Conseil du trésor. Février 2002. Disponible sur le site : www.tresor.gouv.qc.ca/publications/diagnosticsante-employes.pdf
- *le Plan d'action gouvernemental pour la PRP* du Conseil exécutif, adopté en mai 1999, disponible sur le site Web du MRCI : http://www.aiprp.gouv.qc.ca/protectionpublic/actions/actions.asp?Sect=1
- *le Cadre de gestion des ressources informationnelles en soutien à la modernisation de l'Administration publique* du Conseil du trésor, chapitre 3.2-4 sur la sécurité et la protection des renseignements personnels, disponible sur le site du Conseil du trésor : www.autoroute.gouv.qc.ca/dossiers/cadre_de_gestion_ct197638.pdf
- les politiques et directives sur la PRP déjà établies au sein de l'organisme public.

DIRECTIVES AUX NIVEAUX NATIONAL ET INTERNATIONAL

Directives qui s'appliquent en matière de protection des renseignements personnels et de respect de la vie privée et dont certains des principes ont guidé l'élaboration du présent document.

- Les *Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières des données de caractère personnel* (1980), disponible sur le site de l'OCDE : http://www1.oecd.org/publications/e-book/9302012E.PDF

  Elles sont devenues la norme nationale en matière de protection des données et le fondement des lois à venir. Le Canada a adhéré à ces principes en 1984.

  Elles énoncent les principes fondamentaux suivants qui sont applicables au plan national :

  - principe de limitation en matière de collecte des renseignements personnels ;
  - principe de la qualité des données ;
  - principe de la spécification des finalités ;
  - principe de la limitation de l'utilisation ;
  - principe des garanties de sécurité ;
  - principe de la transparence ;
  - principe de la participation individuelle ;
  - principe de la responsabilité des entités.

- la *Directive sur la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation des données* de l'Union européenne, qui est entrée en vigueur le 26 octobre 1998. Disponible sur le site http://europa.eu.int/scadplus/leg/fr/lvb/l14012.htm

ANNEXE – K Liste des représentants d'organismes publics consultés durant l'élaboration du modèle*

PHASE 1 CONCEPTION ET ÉLABORATION DU MODÈLE DE PRATIQUES DE PRP : VERSION PRÉLIMINAIRE 0,4

Présentation du *Modèle de pratiques de PRP* les 4, 13 et 26 février 2002

Madame Danielle Bélanger
Secrétariat du Conseil du trésor

Monsieur Jean Biron
Ministère des Ressources naturelles, de la Faune et des Parcs

Maître Myriam Bourget
Ministère des Ressources naturelles, de la Faune et des Parcs

Maître Pierrette Brie
Ministère de l'Emploi, de la Solidarité sociale et de la Famille

Monsieur Michel Cadieux
Ministère des Ressources naturelles, de la Faune et des Parcs

Maître Josette Chandonnet
Ministère de la Justice

Maître Danielle Corriveau
Régie des rentes

Maître Lina Desbiens
Commission de la santé et de la sécurité au travail

Monsieur Gilles Deschamps
Ministère des Relations avec les citoyens et de l'Immigration

Monsieur Clausel Dorcena
Ministère des Relations avec les citoyens et de l'Immigration

Monsieur Daniel Dore
Secrétariat du Conseil du trésor

Madame Élise Dufour
Ministère des Ressources naturelles, de la Faune et des Parcs

Madame Carmen Gauthier
Ministère du Revenu

Monsieur Jacques Gilbert
Ministère du Revenu

Madame Carmen Grondin
Secrétariat du Conseil du trésor

Monsieur Pierre Lafond
Ministère des Ressources naturelles, de la Faune et des Parcs

Monsieur René Landry
Ministère des Ressources naturelles, de la Faune et des Parcs

Monsieur Robert Lebel
Ministère du Revenu

Monsieur Michel Lévesque
Ministère de la Culture et des Communications

Monsieur Alain Pedneault
Ministère du Revenu

Maître Marie-France Piché
Ministère des Ressources naturelles, de la Faune et des Parcs

Maître Diane Poitras
Commission de la santé et de la sécurité du travail

Maître Michel Ricard
Ministère de la Justice

Maître Julie Roberge
Ministère du Revenu

Monsieur Pierre Sasseville
Secrétariat du Conseil du trésor

Monsieur Claude Taillon
Ministère des Ressources naturelles, la Faune et des Parcs

Monsieur Luc Tremblay
Ministère du Revenu

Monsieur Luc Tremblay
Ministère des Ressources naturelles, de la Faune et des Parcs

* Le ministère ou organisme de provenance des personnes est celui où elles travaillaient au moment des travaux.

PHASE 2 CONCEPTION ET ÉLABORATION D'UNE NOUVELLE VERSION DU MODÈLE DE PRATIQUES DE PRP : VERSION 0,8

Travaux de septembre 2002 à mars 2003

Monsieur Jean Biron
Ministère des Ressources naturelles, de la Faune et des Parcs

Maître Josette Chandonnet
Ministère de la Justice

Monsieur Max Chassé
Secrétariat du Conseil du trésor

Monsieur René Cléroult
Ministère de la Culture et des Communications

Maître Danielle Corriveau
Régie des rentes

Monsieur Jacques Gilbert
Ministère du Revenu

Madame Nicole Lemay
Ministère de la Culture et des Communications

Monsieur Michel Lévesque
Directeur général des élections

Monsieur Alain Pedneault
Ministère du Revenu

Maître Jeanne Proulx
Ministère de la Justice

Maître Michel Ricard
Ministère de la Justice

Monsieur Luc Tremblay
Ministère du Revenu

Madame Louise Thiboutot
Secrétariat du Conseil du trésor

ANNEXE – L Clause type de protection des renseignements personnels*

Certaines adaptations pourront se révéler nécessaires selon la nature du contrat et le but recherché par les parties.

Considérant que les renseignements personnels sont confidentiels et, afin d'assurer cette confidentialité lorsque des renseignements personnels sont communiqués au contractant pour la réalisation du contrat et, le cas échéant, lorsque des renseignements personnels sont générés à l'occasion de sa réalisation, (ci-après désignés « renseignements personnels »), le « Fournisseur » s'engage à :

1° informer son personnel des obligations stipulées à la présente disposition et diffuser à cet égard toute l'information pertinente ;

2° rendre accessibles les renseignements personnels, au sein des membres de son personnel, uniquement à ceux qui ont qualité pour les recevoir, lorsqu'ils sont nécessaires à l'exercice de leurs fonctions ;

3° faire signer aux membres de son personnel des engagements au respect de la confidentialité des renseignements personnels, selon le formulaire joint en annexe au contrat, et les transmettre au ministre ou à l'organisme ;

4° ne communiquer les renseignements personnels, sans le consentement de la personne concernée, à qui que ce soit, sauf dans le cadre d'un contrat de sous-traitance et selon les modalités prévues au paragraphe 12° ;

5° soumettre à l'approbation du ministre ou de l'organisme le formulaire de consentement à la communication de renseignements personnels de la personne concernée ;

6° utiliser les renseignements personnels uniquement pour la réalisation du contrat ;

7° recueillir un renseignement personnel au nom du ministre ou de l'organisme dans les seuls cas où cela est nécessaire à la réalisation du contrat et informer préalablement toute personne visée par cette cueillette de l'usage auquel ce renseignement est destiné, ainsi que des autres éléments mentionnés à l'article 65 de la *Loi sur l'accès* ;

8° prendre toutes les mesures de sécurité propres à assurer la confidentialité des renseignements personnels à toutes les étapes de la réalisation du contrat et, le cas échéant, les mesures identifiées à l'annexe… jointe au présent contrat pour en faire partie intégrante ;

9° ne conserver à l'expiration du contrat aucun document contenant un renseignement personnel, quel que soit le support, en les retournant au ministre ou à l'organisme ou en procédant, à ses frais, à leur destruction conformément au *Guide pour la destruction des documents renfermant des renseignements personnels – janvier 1995 – CAI* dont le fournisseur déclare avoir reçu copie ;

* Extrait du *Guide de rédaction des contrats de services professionnels* du ministère de la Justice du Québec. Pages 51 à 54.

10° informer dans les plus brefs délais le ministre ou l'organisme de tout manquement aux obligations prévues à la présente disposition ou de tout événement pouvant risquer de porter atteinte à la sécurité ou à la confidentialité des renseignements personnels ;

11° fournir à la demande du ministre ou de l'organisme toute l'information pertinente au sujet de la protection des renseignements personnels et l'autoriser à visiter les lieux où le fournisseur détient les renseignements personnels afin de s'assurer du respect de la présente disposition ;

12° lorsque la réalisation du présent contrat est confiée à un sous-traitant et qu'elle comporte la communication ou la cueillette de renseignements personnels ;

12.1° soumettre à l'approbation du ministre ou de l'organisme la liste des renseignements personnels communiqués au sous-traitant ;

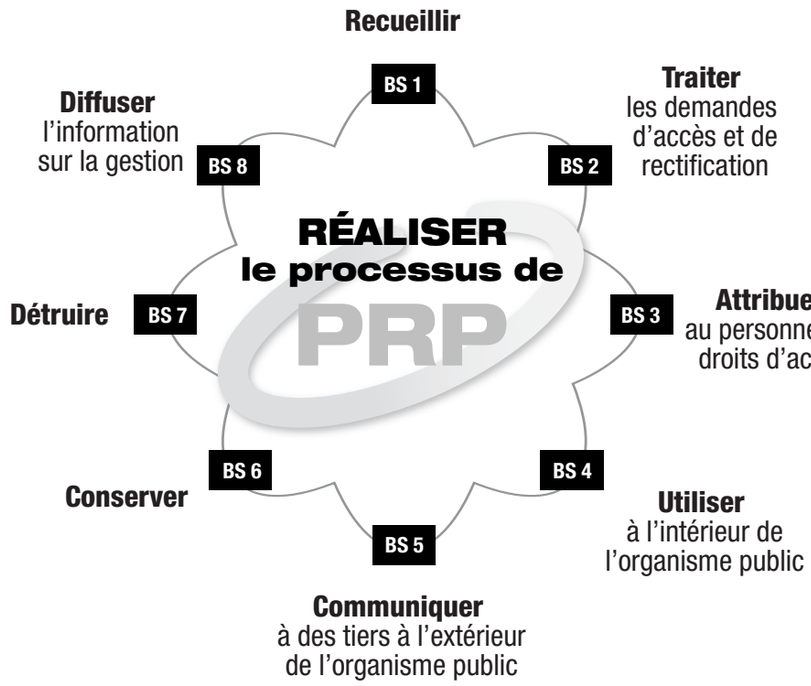
12.2° conclure un contrat avec le sous-traitant stipulant les mêmes obligations que celles prévues à la présente disposition.

Notes

Achevé d'imprimer en mars 2004
sur les presses de l'imprimerie
Héon & Nadeau limitée
à Victoriaville

SCHÉMA DE LA PARTIE 1

Réaliser la protection des renseignements personnels (PRP) dans les projets de développement



BS 1 Recueillir

PS 1.1 Déterminer tous les renseignements personnels (RP) que l'on projette de gérer dans le système

PS 1.2 Évaluer la nécessité des RP que l'on projette de gérer dans le système

PS 1.3 Déterminer les sources d'obtention des RP

PS 1.4 Informer la Commission d'accès à l'information (CAI) des situations où des RP, déjà colligés par une personne (autre que la personne concernée) ou par une entreprise privée, seront recueillis auprès de celles-ci

PS 1.5 Déterminer les modalités de collecte des RP

PS 1.6 Déterminer les modalités d'information de la personne auprès de qui les RP seront recueillis

BS 2 Traiter les demandes d'accès et de rectification

PS 2.1 Mettre en œuvre les modalités de traitement des demandes d'accès à des RP et de rectification de ceux-ci

BS 3 Attribuer au personnel les droits d'accès

PS 3.1 Déterminer les droits d'accès aux RP

PS 3.2 Concevoir et développer le système de manière à respecter les droits d'accès établis

PS 3.3 Mettre en œuvre des mesures visant à permettre au personnel de l'organisme public l'accès aux RP dans les seuls cas où cela est justifié

PS 3.4 Décrire, dans le formulaire de déclaration de fichiers des RP, les catégories de personnes qui ont accès à des RP

BS 4 Utiliser à l'intérieur de l'organisme public

PS 4.1 Appliquer, dans tous les éléments du système d'information, les règles d'utilisation des RP

PS 4.2 Déterminer et évaluer les utilisations des RP projetées lors de la modification des systèmes existants

PS 4.3 Utiliser, dans la mesure du possible, des renseignements anonymes

PS 4.4 Mettre en œuvre des mesures pour prévenir l'utilisation illicite de RP au sein de l'organisme public

BS 5 Communiquer à des tiers à l'extérieur de l'organisme public

PS 5.1 Déterminer les situations où l'organisme public projette de communiquer des RP à des tiers, à l'extérieur de l'organisme public

PS 5.2 Évaluer les situations où des RP seront communiqués à des tiers, à l'extérieur de l'organisme public

PS 5.3 Mettre en œuvre des mesures d'encadrement, de suivi et de sécurité lorsque des RP sont communiqués à des tiers, à l'extérieur de l'organisme public

PS 5.4 Mettre en œuvre des mesures pour obtenir le consentement des personnes

BS 6 Conserver

PS 6.1 Mettre en œuvre des mesures pour conserver les RP en respectant le calendrier de conservation, et ce, tout au long de leur cycle de vie

PS 6.2 Mettre en œuvre des mesures de sécurité, et ce, tout au long du cycle de vie des RP

BS 7 Détruire

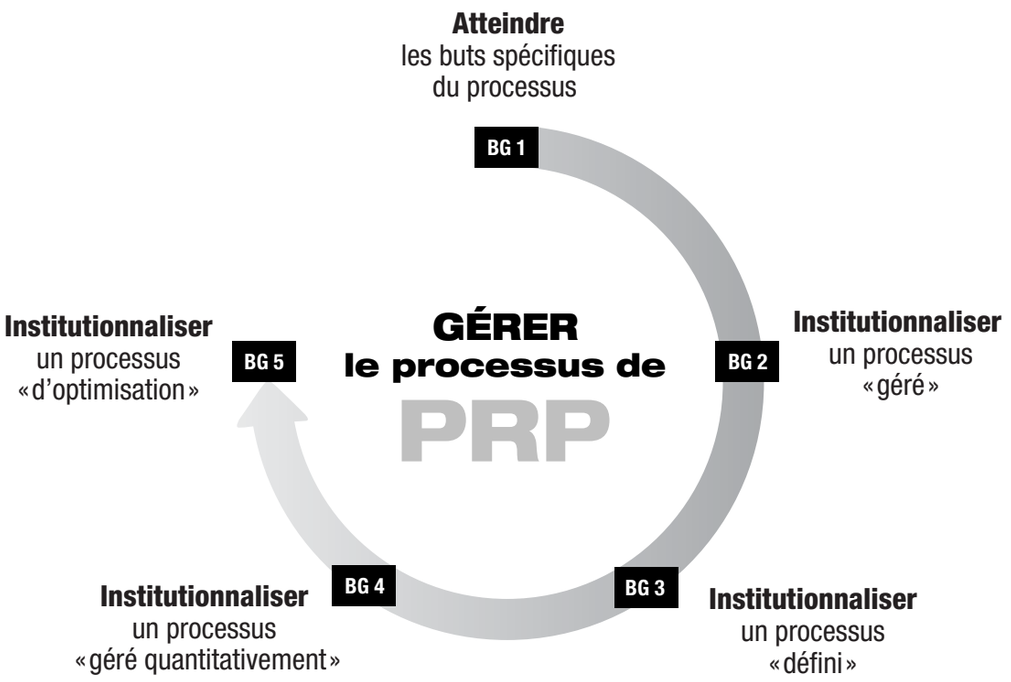
PS 7.1 Mettre en œuvre des mesures de destruction des RP

BS 8 Diffuser l'information sur la gestion

PS 8.1 Constituer et maintenir à jour un inventaire des fichiers de RP créés ou transférés dans le nouveau système ou modifiés dans le système existant et les déclarer à la CAI

PS 8.2 Diffuser l'information sur les modalités de gestion des RP

SCHÉMA DE LA PARTIE 2
Gérer la protection des renseignements personnels (PRP)
dans les projets de développement



BG 1 **Atteindre les buts spécifiques du processus**

Niveau de capacité 1

PG 1.1 Réaliser les pratiques spécifiques

BG 2 **Institutionnaliser un processus « géré »**

Niveau de capacité 2

PG 2.1 Établir une politique

PG 2.2 Planifier le processus

PG 2.3 Fournir les ressources

PG 2.4 Assigner la responsabilité

PG 2.5 Former le personnel

PG 2.6 Gérer les configurations

PG 2.7 Identifier et faire participer les parties prenantes pertinentes

PG 2.8 Suivre et contrôler

PG 2.9 Évaluer objectivement la conformité

PG 2.10 Passer en revue l'état d'avancement avec la haute direction

BG 3 **Institutionnaliser un processus « défini »**

Niveau de capacité 3

PG 3.1 Établir un processus « défini »

PG 3.2 Recueillir l'information d'amélioration

BG 4 **Institutionnaliser un processus « géré quantitativement »**

Niveau de capacité 4

PG 4.1 Établir des objectifs quantitatifs

PG 4.2 Stabiliser la performance des sous-processus

BG 5 **Institutionnaliser un processus « d'optimisation »**

Niveau de capacité 5

PG 5.1 S'assurer de l'amélioration continue

PG 5.2 Corriger les principales causes des problèmes

PRP

Le Modèle de pratiques de protection des renseignements personnels (PRP) a été élaboré à l'intention de tous les organismes publics et principalement pour les membres de l'équipe d'un projet de développement d'un système d'information. Il sera aussi d'une grande utilité pour les gestionnaires, les responsables de la PRP, de la sécurité, de la gestion documentaire, les conseillers juridiques, les responsables des méthodes de développement et de gestion de projets, les vérificateurs et d'autres intervenants d'un organisme public.

Le Modèle offre une base commune de connaissances et de bonnes pratiques pour faciliter le respect des principes et obligations légales de protection des renseignements personnels dans le contexte du développement des systèmes d'information. Le Modèle peut également être utile dans tout programme ou service qui fait appel à des renseignements personnels.

Relations avec les citoyens et Immigration
Québec

ISBN 2-551-19659-0
9 782551 196593
Imprimé au Québec, Canada
19,95 $