MODÈLE DE CLASSIFICATION DE SÉCURITÉ DES DONNÉES NUMÉRIQUES GOUVERNEMENTALES

GUIDE D'ACCOMPAGNEMENT

Votre gouvernement

Québec

Note au lecteur

Ce guide d'accompagnement complète le document juridique relatif au Modèle de classification des données numériques gouvernementales (Arrêté 2024-05 du ministre de la Cybersécurité et du Numérique).

Les explications et exemples déjà inclus dans le document juridique ne sont pas répétés ici. Il est donc essentiel de consulter le document juridique au préalable pour tirer pleinement profit de ce guide.

Ce guide a été réalisé par la Direction de l'encadrement et de l'évolution des pratiques en sécurité de l'information gouvernementale du ministère de la Cybersécurité et du Numérique.

12 février 2025

TABLE DES MATIÈRES

MISE EN CONTEXTE

Le modèle de classification des données numériques gouvernementales (ci-après, le « modèle de classification ») remplace le *Guide de catégorisation de l'information*[1], pris par le Conseil du trésor en juillet 2016.

D'application obligatoire en vertu de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI), le modèle de classification apporte plusieurs améliorations :

- Une **classification uniforme** des données numériques gouvernementales de même nature à l'aide d'un modèle de classification commun pour l'ensemble des organismes publics (OP);

> 🔍 Le modèle de classification propose une démarche et des grilles d'analyse communes à tous les OP.

- Une **interopérabilité** et une **portabilité** de l'information en disposant des normes équivalentes aux partenaires fédéraux et autres;

> 🔍 Le modèle de classification s'inspire des méthodes en vigueur au gouvernement du Canada qui prennent appui sur les standards américains développés par le National Institute of Standards and Technology (NIST).

Une réutilisation des efforts déjà déployés

Le Programme de consolidation des centres de traitement informatique (PCCTI) lancé en 2019 a introduit une approche d'analyse de préjudices dans un contexte de virage à l'infonuagique. Les OP ayant effectué ces analyses pourront en tirer profit lors de la transition vers le nouveau modèle de classification. L'annexe 2 présente une procédure de conversion ou de révision des analyses de préjudices.

[1] Voir l'annexe 1 qui explique les différences entre la catégorisation (cote DIC) et le modèle de classification.

PUBLIC CIBLE ET OBJECTIFS

Ce guide est destiné à tous les intervenants impliqués dans la classification de sécurité des données numériques gouvernementales. Il complète le document juridique du modèle de classification des données numériques gouvernementales (Arrêté 2024-05 du ministre de la Cybersécurité et du Numérique).

Les objectifs de ce guide sont les suivants :

- Expliquer certains concepts fondamentaux qui sous-tendent le modèle de classification;
- Mettre en évidence, lorsque cela est pertinent, les différentes options disponibles à chaque étape de la classification;
- Présenter des exemples concrets pour illustrer les principes de classification;
- Fournir des conseils pratiques pour garantir une classification appropriée des données.

GLOSSAIRE

Catégorie d'appartenance
Selon le modèle de classification, les données structurées ou non structurées qui sont détenues par les organismes publics appartiennent à l'une ou l'autre des deux catégories d'appartenance suivantes : « classifié » ou « protégé ».

Développement en milieu utilisateur (DMU)
Le « Développement en milieu utilisateur » (DMU) fait référence à la pratique qui consiste à permettre aux utilisateurs finaux, qui ne sont pas nécessairement des développeurs professionnels, de créer ou de personnaliser des applications afin d'optimiser un processus ou d'automatiser des tâches. Les DMU comportent souvent des données organisées dans un tableur ou une base de données, hébergées sur un poste de travail.

Donnée non structurée
Donnée stockée sans être organisée de manière prédéfinie, ce qui rend son utilisation plus difficile pour un système d'information. Les fichiers de type PDF, Word, Excel, PowerPoint, les fichiers audio, vidéo ou image, ainsi que les courriels sont des exemples de données non structurées.

Donnée structurée
Donnée stockée selon un format prédéfini de façon à permettre son interprétation par un logiciel. Les données semi-structurées dans un format préétabli, afin de permettre leur utilisation par un système d'information (json, xml, csv, etc.), ainsi que les DMU, sont considérées comme des données structurées en vertu du modèle de classification.

Donnée classifiée
Catégorie comprenant les données suivantes :

- Les renseignements visés par une restriction au droit d'accès en vertu de la section II du chapitre II de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1) et identifiés comme étant « classifié » à l'annexe 3 du document juridique du modèle de classification;

- Les données dont une compromission pourrait raisonnablement porter atteinte plus généralement à la sécurité de l'État, incluant la défense et le maintien de la stabilité sociopolitique et socioéconomique.

Donnée protégée
Catégorie comprenant les données suivantes :

- Les renseignements visés par une restriction au droit d'accès en vertu de la section II du chapitre II de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ou en vertu du chapitre III de cette loi et identifiés comme étant « protégé » à l'annexe 3 du document juridique du modèle de classification;

- Les données concernant une personne physique, une entreprise ou une autre entité et dont une compromission pourrait raisonnablement causer un préjudice.

Marquage
Un marquage doit être appliqué à chaque donnée non structurée afin de couvrir l'objectif de confidentialité. Un marquage apporte, pour un organisme public, l'obligation d'appliquer à une telle donnée, les mesures de sécurité adéquates qui y sont liées. Ces mesures de sécurité sont notamment celles prévues aux orientations, standards, stratégies, directives, règles et indications d'application pris en vertu de la Loi. Des mesures de sécurité particulières peuvent également être ajoutées au marquage.

Niveau de préjudice
Le niveau de préjudice a pour objet de refléter le degré de gravité ou d'importance du préjudice qui pourrait vraisemblablement résulter d'un bris de confidentialité, d'intégrité ou de disponibilité au regard d'une donnée.

Objet de classification
Un objet de classification peut être assimilé à un programme, une activité, un service, une opération, un processus, un regroupement d'actifs informationnels ou un actif informationnel, et, par voie de conséquence, en assimilant de tels objets à une donnée.

Objectifs de sécurité
La confidentialité, l'intégrité et la disponibilité (CID) sont les trois objectifs pour assurer le niveau de sécurité attendu au regard des données.

Profil de mesures de sécurité
Un profil de mesures de sécurité doit être attribué à chaque donnée structurée afin de couvrir les trois objectifs de sécurité (confidentialité, intégrité, disponibilité). Un profil de mesures de sécurité apporte, pour un organisme public, l'obligation d'appliquer à une telle donnée les mesures de sécurité adéquates qui y sont liées. Ces mesures de sécurité sont notamment celles prévues aux orientations, standards, stratégies, directives, règles et indications d'application pris en vertu de la Loi. Des mesures de sécurité particulières peuvent également être ajoutées au profil.

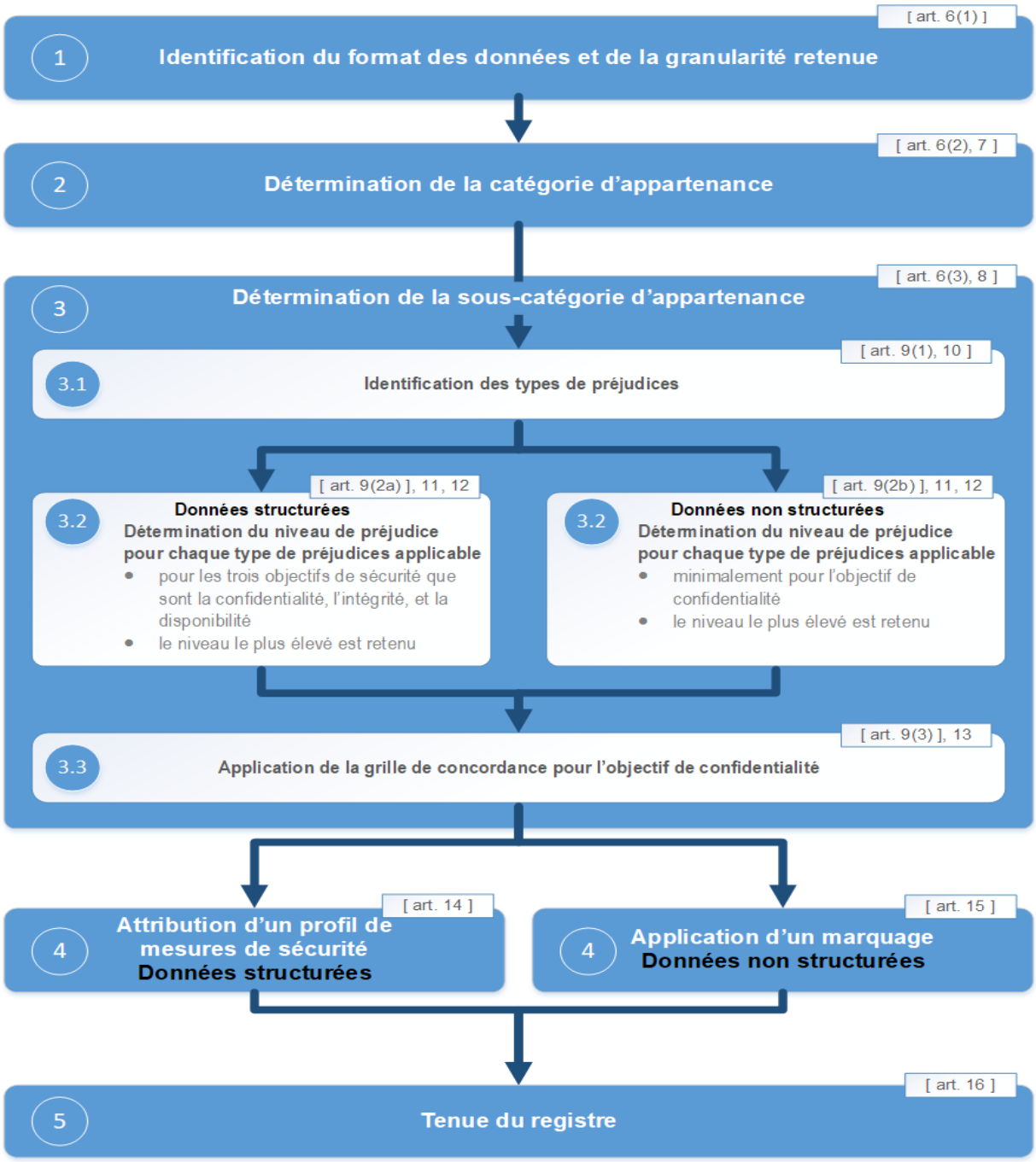
Sous-catégorie d'appartenance
Les sous-catégories d'appartenance possibles, au nombre total de 28, sont réparties parmi les deux catégories existantes (Protégé/Classifié) et par objectif de sécurité (Confidentialité/Intégrité/Disponibilité), en fonction du niveau de préjudice applicable. La figure 2 du document juridique du modèle de classification précise la répartition de ces sous-catégories, avec leurs dénominations respectives. Par exemple : « Très faible », « Faible », « Modéré », « Protégé A », « Protégé B », etc.

Type de préjudices
Un type de préjudices fait référence à un regroupement de préjudices de même nature, par exemple, « T1 - Préjudice physique causé aux personnes physiques » ou « T9 - Préjudice causé à la réputation du Québec ». Le document juridique présente les dix types de préjudices prévus au modèle de classification.

ÉTAPES DE CLASSIFICATION

Les étapes de classification de sécurité des données sont illustrées à la figure suivante. Chaque étape est détaillée par la suite.

Étapes de classification de sécurité des données



1. Identification du format des données et de la granularité retenue

Cette section se réfère à l'article 6 (1) du document juridique du modèle de classification.

1.1 Identification du format des données

Deux formats de données sont prévus au modèle de classification : les données structurées et les données non structurées. Le tableau 1 qui suit en présente quelques exemples.

Les données semi-structurées dans un format préétabli, afin de permettre leur utilisation par un système d'information (json, xml, csv, etc.) ainsi que les développements en milieu utilisateur (DMU), sont considérées comme des données structurées en vertu du modèle de classification.

Tableau 1 : Exemples de formats de données

FORMAT	DÉFINITION	EXEMPLES
DONNÉES STRUCTURÉES	Donnée stockée selon un format prédéfini de façon à permettre son interprétation par un logiciel	• Systèmes d'information, bases de données • Développement en milieu utilisateur (DMU) • Fichiers utilisés par des systèmes d'information : json, xml, csv
DONNÉES NON STRUCTURÉES	Donnée stockée sans être organisée de manière prédéfinie	• Fichiers texte, PDF, Word, Excel, PowerPoint, etc. • Courriels

1.2 Granularité retenue

La granularité représente le niveau de précision souhaité lors de l'identification des objets à classifier, ci-après nommés « objets de classification ». Cette granularité peut avoir un

niveau de détail fin en visant chacune des données ou, au contraire, avoir une plus grande amplitude en visant d'autres objets de classification tels un programme, une activité, un service, une opération, un processus, un regroupement d'actifs ou un actif informationnel.

Le modèle de classification prévoit que l'OP doit déterminer la granularité des objets sur lesquels appliquer la classification. Plus précisément, il doit identifier adéquatement les objets de classification, en faire la description et appliquer le niveau de préjudice le plus élevé qui se rattache à l'une des données se trouvant dans ces objets.

🔍 Pour les OP qui réalisent l'inventaire des données numériques gouvernementales selon l'approche préconisée par le MCN, ce sont les travaux d'inventaire qui conditionnent le choix du niveau de granularité et d'identification des objets de classification. Pour plus de détails, écrire à inventaire.classification@mcn.gouv.qc.ca.

2. Détermination de la catégorie d'appartenance

Cette section se réfère aux articles 6 (2) et 7 du document juridique du modèle de classification.

La détermination de la catégorie d'appartenance consiste à établir si les données sont dites « **données classifiées** » ou « **données protégées** ».

Règle générale, les données de la catégorie « **classifié** » concernent **l'État québécois**, alors que les données de la catégorie « **protégé** » concernent **une personne physique, une entreprise ou une autre entité** (tels un organisme à but non lucratif ou une association).

Le tableau suivant présente quelques exemples de données classifiées et de données protégées.

Tableau 2 : Exemples de catégories d'appartenance

CATÉGORIE D'APPARTENANCE	EXEMPLES
DONNÉES CLASSIFIÉES	• Ébauche de rapport avant publication ou ébauche d'analyse • Procès-verbal d'une réunion • Guide d'utilisation d'un système d'information • Politiques et directives internes d'un organisme • Renseignement portant sur une méthode susceptible d'être utilisée pour commettre un crime ou une infraction à une loi • Ébauche d'un projet de règlement • Analyse relative aux impacts d'un projet de loi non déposé à l'Assemblée nationale • Négociations relatives à une convention collective • Évaluation de la menace et des risques • Plan de continuité des affaires • Avis juridique • Document destiné à un ministre ou au Conseil des ministres • Itinéraire de voyage d'un ministre • Renseignements concernant les modalités de l'aide financière relatifs à des transactions avec des entreprises • Renseignements techniques sur les systèmes d'information • Demande au Conseil du Trésor • Méthode utilisée dans les enquêtes policières • Activités de renseignements • Sujets scientifiques, technologiques ou économiques de sécurité nationale • Vulnérabilités ou capacités des systèmes, installations, infrastructures, projets, plans ou protection des services de sécurité nationale

DONNÉES PROTÉGÉES

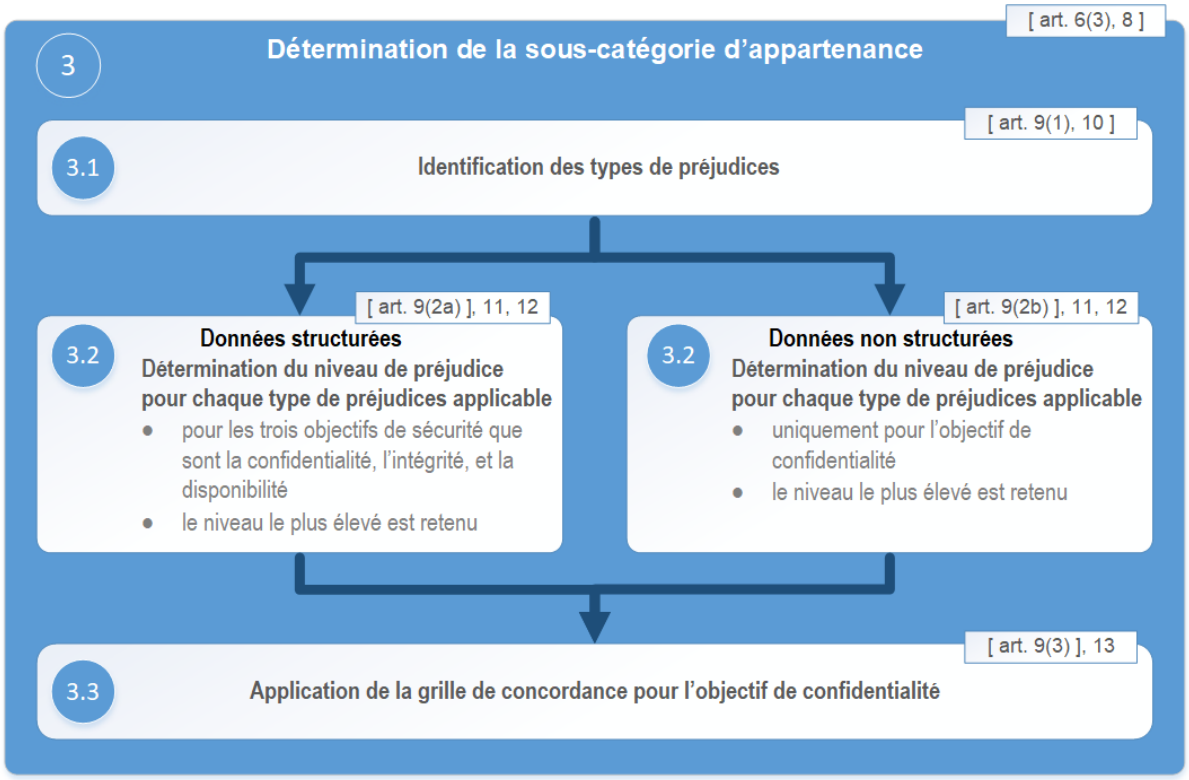
- Coordonnées de contact d'un citoyen
- Renseignements de santé et de services sociaux (résultats de laboratoire, antécédents médicaux, maladies, prestations de soins réalisés, traitements, handicap, évaluation psychosociale, etc.)
- Données fiscales (revenus d'emploi, cotisations, avis de cotisation)
- Numéro permettant d'identifier une personne (Numéros d'assurance sociale, d'assurance maladie, de permis de conduire)
- Origine ethnique, orientation sexuelle, croyances religieuses ou opinions politiques
- Données biométriques (ADN, sang, tracé de la signature, voix, empreintes digitales, reconnaissance oculaire, faciale ou vocale)
- Renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle fourni à un organisme public par un tiers
- Renseignement concernant un témoin repenti inscrit au programme de protection des témoins
- Renseignement d'une enquête policière concernant des personnes

 Si une donnée a, au moment de sa classification, le potentiel d'appartenir à la fois à la catégorie « classifié » et à la catégorie « protégé », la première catégorie prévaut sur la deuxième de sorte que la donnée concernée doit être considérée comme faisant alors partie de la catégorie « classifié ».

L'identification des « données classifiées » revêt une importance particulière pour l'État québécois. La compromission de ces données pourrait, par exemple, avoir une incidence sur les résultats d'un programme gouvernemental, causer un embarras politique, ou encore, avoir une incidence sur la sécurité de l'État ou de la société civile.

3. Détermination de la sous-catégorie d'appartenance

Cette section se réfère aux articles 6 (3), 8, 9 (1), 9 (2a), 9 (2 b), 9 (3), 10, 11, 12 et 13 du document juridique du modèle de classification.



L'étape 3, soit la détermination de la sous-catégorie d'appartenance, se fait à l'aide de l'analyse des préjudices.

Données structurées : cette analyse est généralement réalisée par un comité de classification de sécurité, composée de représentants des données et des systèmes, de la sécurité de l'information, de la protection des renseignements personnels et d'autres expertises jugées pertinentes. L'annexe 4 propose la composition d'un tel comité.

Données non structurées : cette analyse peut être réalisée par toute personne produisant ou manipulant ce type de données dans le cadre de son travail. Elle peut prendre appui sur une évaluation préalable effectuée par le comité de classification de sécurité des données tel que défini à l'annexe 4.

3.1 Identification des types de préjudices

Cette section se réfère aux articles 9 (1) et 10 du document juridique du modèle de classification.

La détermination de la sous-catégorie d'appartenance vise à déterminer les types de préjudices applicables.

- Il est important de bien analyser chacun des dix (10) types de préjudices et de ne retenir que les préjudices qui sont applicables;
- Lorsqu'un préjudice est retenu, ce dernier doit être analysé pour les trois objectifs de sécurité (CID).

Les considérations dans le choix des types de préjudices sont les suivantes :

- Le contexte de l'organisme public : chaque organisme public a une mission à remplir, laquelle peut être considérée d'importance pour l'État. Certains types de préjudices pourront être plus pertinents aux fins de l'analyse des préjudices;
- La catégorie d'appartenance (« classifié » ou « protégé ») de l'objet de classification : certains types de préjudices sont plus adaptés à la catégorie d'appartenance « classifié » alors que d'autres types sont plus adaptés à la catégorie d'appartenance « protégé ». Les types T1 à T4 visent la catégorie d'appartenance « protégé » alors que les types T5 à T10 se rapportent davantage à la catégorie d'appartenance « classifié ». Cette règle n'est cependant pas absolue.

Considérations des préjudices subis par les organismes publics

Alors que l'analyse de l'approche de catégorisation (cote DIC) était davantage orientée vers les conséquences pour l'organisme, le modèle de classification se concentre plutôt sur les préjudices causés aux citoyens, aux entreprises et à l'État.

Par conséquent, lors de l'analyse, l'OP ne doit pas se limiter à évaluer les préjudices qui l'affectent directement, tels que ceux liés à son fonctionnement interne, à la qualité de ses services ou à son image. Il doit avant tout se concentrer sur les préjudices potentiels causés à l'État, en raison de la sensibilité des données traitées et des conséquences plus larges que pourrait entraîner une défaillance en matière de sécurité. Il doit alors se référer aux types de préjudices T5 à T10 du modèle de classification. Ces types de préjudices ne visent pas l'organisme en particulier, mais le bien commun, c'est-à-dire l'administration publique ou le gouvernement dans son ensemble. Il est question de programmes gouvernementaux, de services publics et du bon fonctionnement de l'État québécois.

L'exemple qui suit présente l'identification des types de préjudices applicables aux données de la catégorie « protégé ».

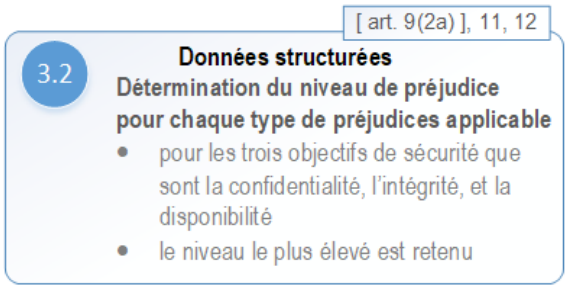
Exemple 1 : Identification des types de préjudices

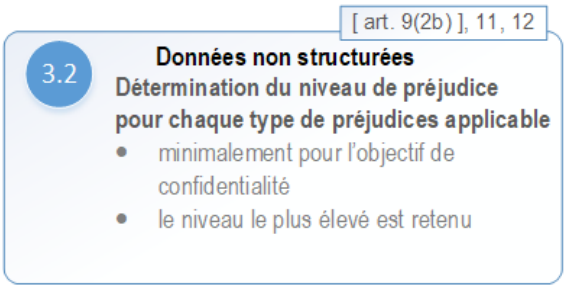
Dans cet exemple, il s'agit de données financières se rapportant à des entreprises. Puisque les types T1, T2 et T3 visent davantage des personnes physiques, ceux-ci sont exclus de l'analyse. Le type T4 se rapporte plus spécifiquement aux entreprises. Pour les types restants, seuls les types T6 et T7 touchent davantage à l'aspect financier de cette analyse.

Objet de classification	Description de l'objet	Types de préjudices
Base de données du programme de subvention aux restaurateurs	Renseignements financiers de demande d'aide financière, relatifs au financement, aux travaux et au budget de réalisation d'un projet	T4 – Perte financière pour les entreprises et autres entités
		T6 – Perte financière pour l'État
		T7 – Préjudice causé à l'économie québécoise

3.2 Détermination du niveau de préjudice pour chaque type de préjudices applicable

Cette section se réfère aux articles 9 (2a), 9 (2 b), 11 et 12 du document juridique du modèle de classification.





L'étape 3.2 consiste à déterminer le niveau de préjudice pour chaque type de préjudice applicable, en retenant le niveau de préjudice le plus élevé.

L'analyse du contexte d'utilisation des données est cruciale pour déterminer le niveau de préjudice. Voici des exemples démontrant l'importance de ce contexte en regard de l'objectif de confidentialité.

Exemple 2 : Contextes déterminant le niveau de préjudice

Noms et adresses de personnes

Les noms et adresses de personnes peuvent avoir une sensibilité variable selon le contexte. Voici deux situations :

> Situation 1 : une violation de la confidentialité **d'une liste électorale** pourrait avoir comme conséquence des préjudices physiques ou psychologiques faibles tels un inconfort ou un stress aux personnes concernées. Ceci correspond à un **niveau de préjudice faible**.
>
> Situation 2 : une violation de la confidentialité de dossiers de **personnes bénéficiant du programme de protection des témoins** pourrait avoir comme conséquence des préjudices physiques ou psychologiques graves aux personnes concernées tels que mettre leur santé psychologique, ou même leur vie, en danger. Ceci correspond à un **niveau de préjudice élevé.**

Bien que dans les deux cas il s'agisse de noms et d'adresses de personnes, le niveau de préjudice diffère en fonction du contexte.

Compte rendu de rencontre

Un compte rendu de rencontre peut également avoir une sensibilité variable selon le contexte. Voici deux situations :

> Situation 1 : une violation de la confidentialité concernant un **compte rendu du comité social** traitant des activités à venir dans la prochaine année **n'occasionnerait aucun préjudice, ou tout au plus, un préjudice très faible**.
>
> Situation 2 : une violation de la confidentialité concernant un **compte rendu du comité exécutif** comportant des scénarios de réorganisation administrative pourrait avoir comme conséquence une incidence sur le rendement d'un service. Ceci correspond à un **niveau de préjudice faible**.

Bien que dans les deux cas il s'agisse d'un compte rendu, le niveau de préjudice diffère selon le contexte.

En outre, selon l'objectif de confidentialité, le document juridique du modèle de classification des données numériques gouvernementales comporte le **tableau des données visées par une restriction au droit d'accès en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.** La restriction d'accès est déterminée en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LAI) et les niveaux de confidentialité sont déterminés en vertu du modèle de classification. Ce tableau procure de nombreux exemples de données avec des niveaux minimal et maximal de préjudice portant sur la confidentialité. L'annexe 3 décrit le contenu du tableau pour en faciliter la compréhension.

Données structurées : les trois objectifs de sécurité (confidentialité, intégrité, disponibilité) doivent être considérés dans l'analyse de préjudices.

Données non structurées : l'objectif de confidentialité doit être minimalement considéré dans l'analyse de préjudices.

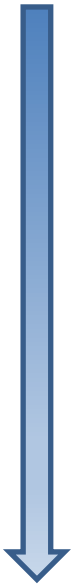
Pour la détermination du niveau de préjudice, il est suggéré de commencer l'analyse à partir du niveau « Très élevé » vers le niveau « Très faible ». Par exemple, pour le type **T1 – Préjudice physique causé aux personnes physiques**, il est suggéré de faire l'analyse selon l'ordre suivant :

🔍 Afin de faciliter l'analyse des préjudices, procéder en questionnant du niveau « Très élevé », jusqu'au niveau « très faible ».

Niveau de préjudice

La compromission de données pourrait-elle correspondre à un niveau de préjudice?

Très élevé



Très faible

Très élevé (ex. : lourdes pertes de vie) :

- Si oui, retenir ce niveau.
- Si non, passez au niveau Élevé pour poursuivre l'analyse.

Élevé (ex. : incapacité physique, décès) :

- Si oui, retenir ce niveau.
- Si non, passez au niveau Modéré pour poursuivre l'analyse.

Modéré (ex. : douleurs physiques, blessures, traumatisme, difficultés, maladie) :

- Si oui, retenir ce niveau.
- Si non, passez au niveau Faible pour poursuivre l'analyse.

Faible (ex. : inconfort physique) :

- Si oui, retenir ce niveau.
- Si non, passez au niveau Très faible pour poursuivre l'analyse.

Très faible (aucun préjudice ou préjudice très faible) :

- Retenir ce niveau.

Lors de la détermination des niveaux de préjudices, il est important de s'en tenir à des situations qui pourraient raisonnablement survenir : le préjudice associé à la compromission de sécurité doit être une conséquence **directe** pour les personnes ou l'État, et non une conséquence **indirecte**.

Exemple 3 : Conséquence directe et indirecte

***Conséquence directe** : la compromission de ce système pourrait créer une violation de la vie privée d'une personne et raisonnablement causer des préjudices psychologiques allant jusqu'à la détresse (T2 – Préjudice psychologique causé aux personnes physiques). Le préjudice qui en découle peut être considéré comme une conséquence directe. Il devrait donc être envisagé dans l'analyse.*

***Conséquence indirecte** : pour la même compromission, une personne pourrait être impliquée dans un grave accident de voiture en raison d'un manque de sommeil ou de concentration causé par le stress d'une violation de sa vie privée. Cela pourrait entraîner des blessures graves, voire la mort (T1 – Préjudice physique causé aux personnes physiques). La situation qui découle de cette extrapolation devrait être considérée comme une conséquence indirecte. Il ne devrait donc pas être envisagé dans l'analyse.*

Il est nécessaire de justifier (documenter) les niveaux de préjudices déterminés comme le démontre l'exemple qui suit. Ces justifications seront consignées au registre de classification des données.

Exemple 4 : Justification de niveau de préjudice

Les niveaux de préjudice sont présentés en rouge dans le tableau.

Objet de classification	Description de l'objet	Types de préjudices	Niveaux de préjudices			Justifications
			Confidentialité	Intégrité	Disponibilité	
Base de données du programme de subvention aux restaurateurs	Renseignements financiers de demande d'aide financière, relatifs au financement, aux travaux et au budget de réalisation d'un projet	T4 – Perte financière pour les entreprises et autres entités	M	M	F	Selon la LAI, les renseignements financiers fournis par des entreprises sont soumis à une restriction des droits d'accès (art.23, LAI)
		T6 – Perte financière pour l'État	M	M	F	Une divulgation ou une violation de l'intégrité pourrait affecter les résultats du programme
		T7 – Préjudice causé à l'économie québécoise	TF	TF.	TF.	Même si le type de préjudices T7 semble s'appliquer à cette évaluation, les niveaux de préjudice sont estimés à TF

Pour conclure, il est important de souligner que l'**analyse de préjudices** se distingue de l'**analyse de risques**. L'objectif principal est de mesurer le niveau de préjudice sans tenir compte des mesures de sécurité actuellement en place advenant une compromission des objectifs de sécurité. Comme le démontre l'exemple qui suit, il est essentiel, à ce stade, de ne pas prendre en considération les mesures de sécurité existantes lors de l'évaluation du niveau de préjudice.

Exemple 5 : Analyse de préjudices qui ne doit pas considérer les mesures de sécurité en place

Plusieurs mesures de sécurité sont déployées pour protéger des données sensibles, dont le chiffrement de la base de données et l'authentification multifacteur (MFA) pour la gestion des accès.

En raison des mesures de sécurité en place, certains pourraient être tentés de considérer que le niveau de préjudice pour ces données sensibles est « Faible » tout au plus, car ces mesures devraient théoriquement empêcher toute compromission des données. ***Cependant, cette évaluation est erronée****.*

Dans cet exemple, il est impératif de déterminer le niveau de préjudice en ignorant délibérément les mesures de sécurité en place de chiffrement de la base de données et d'authentification multifacteur (MFA).

Considération des situations de regroupement, d'inférence ou d'interdépendance

Des situations particulières peuvent influencer le niveau de préjudice. Il est question ici de situations de regroupement, d'inférence ou d'interdépendance.

Ces situations varient d'un OP à l'autre en fonction du contexte d'utilisation de l'objet de classification. Il est également important de considérer l'ensemble des parties prenantes concernées dans l'évaluation du niveau de préjudice.

Regroupement

Le regroupement s'applique généralement à la confidentialité, mais peut également s'appliquer à la disponibilité et à l'intégrité comme le démontrent les exemples suivants.

Exemple 6 : Situation de regroupement

Confidentialité *: la divulgation non autorisée d'un dossier contenant des renseignements personnels pouvant causer un préjudice modéré à la personne concernée. Si tous les dossiers des ressources humaines d'un organisme public étaient divulgués, le niveau de préjudice pourrait devenir plus élevé pour l'État.*

Exemple 7 : Situations de regroupement

***Intégrité** : la modification sans autorisation d'un seul dossier peut générer de faibles préjudices alors que la corruption complète d'une base de données comportant des milliers de dossiers peut générer des préjudices élevés.*

***Disponibilité** : la destruction d'un bien, comme un seul serveur, peut générer de faibles préjudices alors que la perte de tout un parc de serveurs serait beaucoup plus préjudiciable.*

Inférence

L'analyse de certaines données peut parfois permettre de tirer des conclusions pouvant compromettre des données encore plus sensibles. Les OP devraient tenir compte de la sensibilité, non seulement des données classifiées, mais aussi de celle d'autres informations associées qui pourraient être inférées et ensuite exploitées par un acteur de menaces.

Exemple 8 : Situation d'inférence

Des dossiers d'employés classifiés de niveau « Modéré » aux fins de confidentialité peuvent contenir de l'information qui donne certaines indications sur le rôle de l'employé et, par le fait même, sur la mission ou la capacité opérationnelle de l'organisation – information qui peut compromettre les intérêts ou la survie de l'organisation.

Interdépendance

Le but de l'analyse des interdépendances est de déterminer s'il est possible qu'un effet de cascade important résultant d'une compromission de données ait une incidence sur d'autres données. Le niveau d'un préjudice, résultant de la compromission en cascade de données, peut être supérieur à celui attribué à la compromission de données prises individuellement, comme dans le cas du regroupement.

Exemple 9 : Situation d'interdépendance

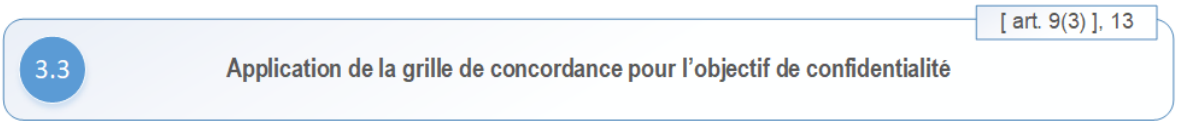
*Pour une compromission de données pouvant affecter la **disponibilité** d'un service offert exclusivement à sa clientèle, un OP détermine que le type « T8 – Préjudice causé aux services rendus à la population » est de niveau « **Faible** ».*

Interdépendance

Si ces données alimentent également la prestation de services d'un partenaire, l'OP pourrait, dans ce cas, déterminer que le type « T8 – Préjudice causé aux services rendus à la population » est de niveau « Modéré » puisque la compromission a une incidence sur les opérations d'autres organismes publics.

3.3 Application de la grille de concordance pour l'objectif de confidentialité

Cette section se réfère aux articles 9 (3) et 13 du document juridique du modèle de classification.



Lors d'une analyse de préjudices, l'exercice permet de déterminer le niveau de préjudice advenant une compromission sur les objectifs de sécurité. Le niveau de préjudice obtenu varie de « Très faible » à « Très élevé ».

Le modèle de classification, en conformité avec celui du gouvernement fédéral, prévoit une nomenclature distincte pour la sous-catégorie d'appartenance d'une donnée au regard de l'objectif de confidentialité, comme indiqué dans la grille de correspondance suivante :

Grille de concordance - confidentialité		
Niveaux de préjudice	**Catégories de données**	
	Données protégées	**Données classifiées**
Très faible	Non classifié	
Faible	Protégé A	Diffusion restreinte
Modéré	Protégé B	Confidentiel
Élevé	Protégé C	Secret
Très élevé		Très secret

Ainsi à titre d'exemple, au lieu de « Modéré » pour la confidentialité, il sera question de :

- « **Protégé B** » lorsqu'il s'agit de données de catégorie d'appartenance « protégé »;
- « **Confidentiel »** lorsqu'il s'agit de données de catégorie d'appartenance « classifié ».

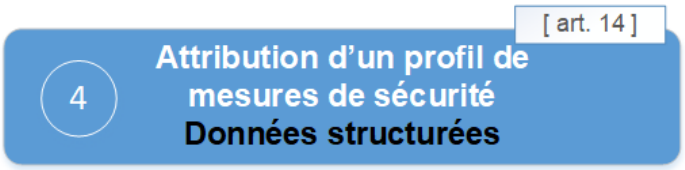
Cette nomenclature permet de distinguer efficacement la catégorie de donnée à la lecture du profil. Par exemple :

- « **Protégé B** » : concerne une personne physique, une entreprise ou une autre entité;
- « **Confidentiel »** : concerne l'État québécois.

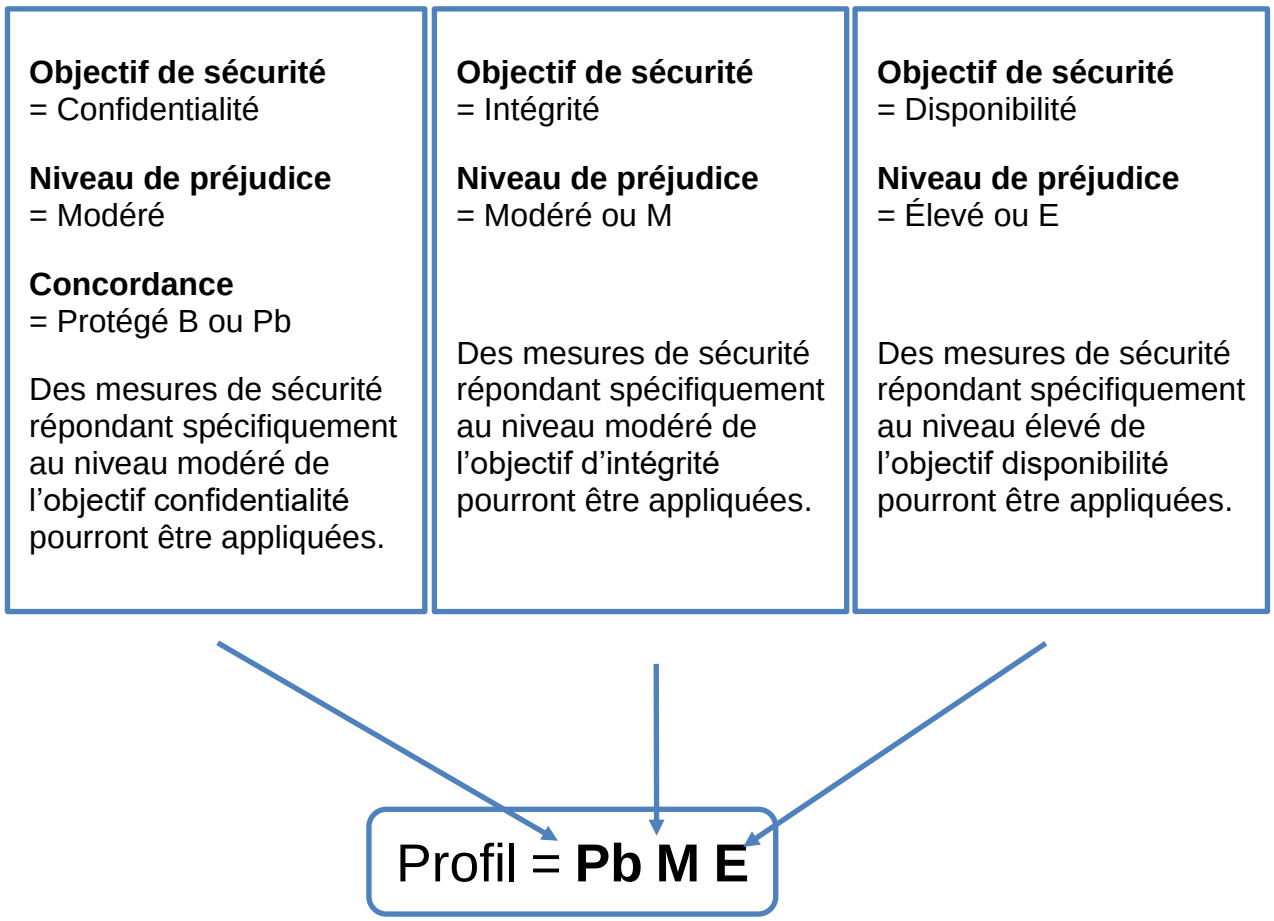
4. Attribution d'un profil de mesures de sécurité ou application d'un marquage

4.1 Attribution d'un profil de mesures de sécurité (données structurées)

Cette section se réfère à l'article 14 du document juridique du modèle de classification.

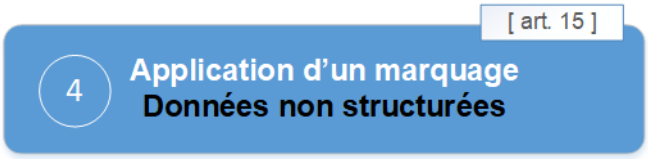


La dénomination d'un profil de mesures de sécurité présente l'ordre suivant pour les objectifs de sécurité : "confidentialité, intégrité, disponibilité" (CID). Le profil reflète le niveau de préjudice le plus élevé ayant été retenu, et ce, pour chaque objectif de sécurité. Des mesures de sécurité pourront conséquemment être appliquées pour chaque objectif de sécurité, selon chaque niveau de préjudice retenu. Voici un exemple de profil :



4.2 Application du marquage (données non structurées)

Cette section se réfère à l'article 15 du document juridique du modèle de classification.



L'objectif de confidentialité doit être minimalement considéré lors du marquage. Des mesures de sécurité pourront conséquemment être appliquées, selon le marquage retenu.

Deux exemples de marquage sont présentés ici.

Exemple 10 : Évaluation du niveau de préjudice pour un courriel

À la demande d'un directeur général, un courriel est transmis, invitant des membres de sa direction à une réunion qui portera sur le développement d'un futur programme de subvention. Si l'invitation ***ne contient aucune information portant sur le contenu du programme****, le courriel pourra être classifié comme «* ***non classifié*** *».*

Si, dans le même courriel, des sujets spécifiques sont inclus, par exemple les ***critères qui permettront de rejeter certaines demandes****, le courriel devra minimalement être classifié comme «* ***Diffusion restreinte*** *». Il est important d'évaluer le niveau de préjudice en fonction des informations complémentaires qui seront ajoutées au courriel.*

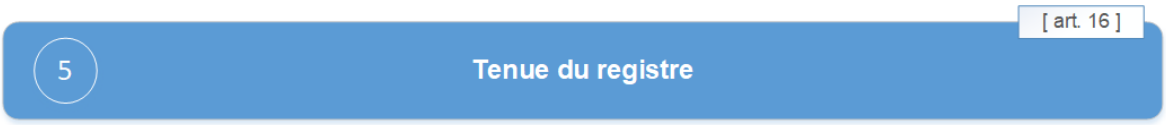
Exemple 11 : Évaluation du niveau de préjudice pour un tableur (Excel)

Un tableur Excel comporte des ***informations fournies par une entreprise*** *concernant une demande de subvention* ***pour le développement d'un nouveau produit****. Les informations recueillies portent sur des détails du produit qu'elle voudrait commercialiser. Les détails recueillis doivent être considérés comme des renseignements confidentiels. Advenant une divulgation de ces détails, il pourrait s'en suivre des préjudices qui pourrait compromettre la viabilité de l'entreprise. Dans ce cas, le niveau de préjudice sera « modéré » pour la confidentialité. À l'aide du tableau de concordance, le niveau de préjudice sera «* ***Protégé B*** *».*

Puisque les mesures pour assurer l'intégrité et la disponibilité des documents ne sont pas sous le contrôle de l'employé qui a produit le tableur, ce dernier n'a pas à se questionner sur les niveaux de préjudice concernant ces deux objectifs de sécurité.

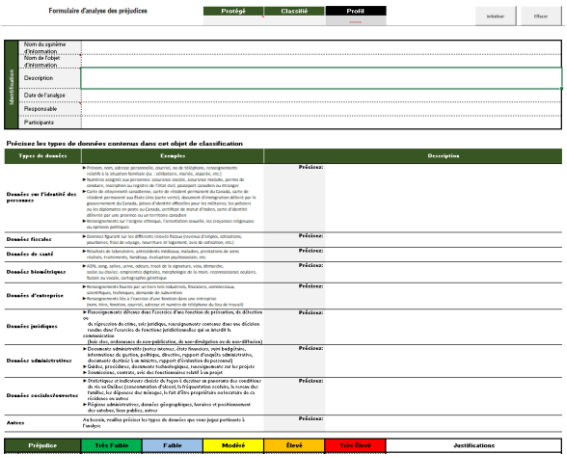
5. Tenue du registre

Cette section se réfère à l'article 16 du document juridique du modèle de classification.

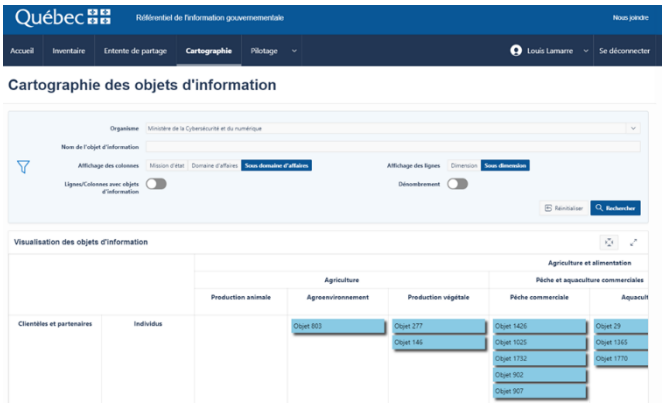


Le registre vise à consigner les informations sur la classification de sécurité des données tels la description des objets de classification, les catégories et sous-catégories d'appartenance, les types et niveaux de préjudices, ainsi les justifications ayant conduit aux résultats obtenus.

L'outil Excel d'**aide à la tâche pour la classification des données structurées** qui est mis à la disposition des OP peut servir de registre, conformément à l'article 16 du modèle de classification.



Également, le ***Référentiel de l'information gouvernementale (RIG)***, un outil gouvernemental mis à la disposition des organismes publics pour l'inventaire et la classification de la sécurité des données peut répondre à l'obligation de tenir un registre, conformément à l'article 16 du modèle de classification.



Enfin, un OP peut développer son propre registre. Dans tous les cas, le registre doit consigner tous les éléments d'information prévus à l'article 16 du modèle de classification.

🔍 L'utilisation du Référentiel de l'information gouvernementale (RIG) est fortement recommandée pour la tenue du registre de classification de sécurité. En effet, l'article 16.4 du document juridique du modèle de classification établit un lien direct entre l'obligation de tenir un registre de classification de sécurité et celle de maintenir un inventaire des données numériques gouvernementales en vertu de la LGGRI.

ANNEXES

Annexe 1 – Différences entre la catégorisation (cote DIC) et le modèle de classification

Les approches d'analyse de la catégorisation (cote DIC) et du modèle de classification sont très différentes. Le tableau ci-dessous en présente un résumé.

1. La grille de niveau d'impact de la catégorisation est **davantage dirigée vers les conséquences à l'organisme plutôt que sur les préjudices aux citoyens, aux entreprises et à l'État**. L'extrait de l'annexe 3 du guide de catégorisation démontre cette différence fondamentale :

   Niveau 1 – Bas
   Événement ayant des incidences d'ordre administratif plutôt négligeables qui sont traitées localement, sans affecter l'organisme sur le plan global ou les autres organismes.

   Niveau 2 – Moyen
   Événement ayant des incidences sur plusieurs secteurs d'activités de l'organisme, mais pas sur son image de marque.

   Niveau 3 – Élevé
   Événement ayant des incidences sérieuses pouvant causer des dommages à l'organisme ou à sa clientèle. L'événement pourrait également nuire aux activités critiques de l'organisme ou à son image de marque, mais sans affecter l'image de marque du gouvernement.

   Niveau 4 – Très élevé
   Événement ayant des incidences extrêmement sérieuses sur l'organisme, les citoyens et les autres organismes. L'événement peut affecter l'image de marque du gouvernement.

2. La grille de niveau d'impact de la catégorisation présente **quatre niveaux, au lieu de cinq pour le modèle de classification**. De plus, **les niveaux des deux méthodes ne correspondent pas** en matière de gravité.

Catégorisation : **4 niveaux**	Modèle de classification : **5 niveaux**
1 - Bas (négligeable)	Très faible (ou aucun)
2 - Moyen (modéré)	Faible (limité)
3 - Élevé (grave)	Modéré (grave)
4 -Très élevé (très grave)	Élevé (très grave)
	Très élevé (extrêmement grave)

3. La grille de niveaux d'impact de la catégorisation **ne tient pas compte des différents types de préjudices à l'État**. Il n'est question que d**'«** image de marque du gouvernement » dans le guide de catégorisation.

   Les types de préjudices suivants du nouveau modèle de classification ne sont pas prévus à la catégorisation :

   T6 – Perte financière pour l'État
   T7 – Préjudice causé à l'économie québécoise
   T9 – Préjudice causé à la réputation du Québec
   T10 – Perte de l'autonomie du Québec

4. La grille de niveau d'impact de la catégorisation est variable d'un OP à l'autre. Il n'y a pas d'uniformité entre les OP. En effet, l'étape de préparation de l'exercice de catégorisation prévoyait de **« définir une grille de niveaux d'impact, sur le plan de la DIC, propre à l'organisme ».**

Le modèle de classification prévoit pour sa part une classification uniforme des données numériques gouvernementales de même nature à l'aide d'un modèle commun pour l'ensemble des organismes publics. Conséquemment, il prévoit une grille de niveaux de préjudices commune à tous les OP. Cette approche assure une interopérabilité avec les partenaires, ainsi que la portabilité de l'information en disposant de normes équivalentes.

5. **Concernant l'objectif de disponibilité, l'analyse d'impact de la catégorisation est basée sur la tolérance au manque de disponibilité, plutôt que sur une analyse de préjudices**. Selon les instructions du guide de catégorisation, chaque OP peut développer sa propre échelle personnalisée de tolérance au délai de récupération. L'ancienne méthode de catégorisation propose les tolérances suivantes :

    Niveau 1 – Bas : la tolérance au délai de récupération est de quelques semaines.
    Niveau 2 – Moyen : la tolérance au délai de récupération est de quelques jours.
    Niveau 3 – Élevé : la tolérance au délai de récupération est de quelques heures.
    Niveau 4 – Très élevé : aucune tolérance au délai de récupération.

Le modèle de classification ne recommande pas une telle approche. Il propose plutôt une analyse de préjudices pour l'objectif de disponibilité.

En conclusion, les différences soulevées sont telles qu'une adaptation de la catégorisation des données au nouveau modèle de classification n'est pas possible.

Annexe 2 – Conversion ou révision des profils de sécurité du PCCTI

Les OP ayant réalisé l'analyse de préjudices du PCCTI peuvent se baser sur ces travaux pour convertir ou réviser leurs profils de sécurité au nouveau modèle de classification. Cette transition est possible, car les deux approches partagent, à quelques exceptions près, la même grille de niveaux de préjudices.

> La conversion ou la révision n'est possible que pour les analyses de préjudices déjà réalisées. Toutes les analyses de préjudices à compléter devront être réalisées en respectant toutes les étapes du modèle de classification.

> Bien que les grilles d'analyse de préjudices du PCCTI et du modèle de classification soient similaires, le modèle de classification ajoute un type de préjudices supplémentaire soit *T8 – Préjudice causé aux services rendus à la population*. Il existe donc une possibilité que cet ajout puisse avoir un impact sur l'analyse de préjudices du PCCTI.

Conversion ou révision?

Par « **conversion** », on entend la possibilité de convertir le profil retenu lors de l'analyse des préjudices du PCCTI en un profil prédéfini jugé équivalent dans le modèle de classification. La conversion procure une économie de temps et d'efforts. Cette conversion se veut une étape intermédiaire permettant une adaptation rapide au modèle de classification. Ultérieurement, il faudra prévoir une analyse de préjudices complète afin qu'elle soit parfaitement conforme au modèle de classification. À noter que la démarche intégrée d'inventaire et de classification de sécurité des données numériques gouvernementales sera une bonne occasion de revoir en détail la classification des données.

Pour simplifier la conversion, les niveaux de préjudices « Très faible/Faible » et « Élevé/Très élevé » sont combinés pour les trois objectifs de sécurité. Le tableau suivant présente les équivalences de profils à appliquer :

Niveau de préjudice	Profils du PCCTI	Profils du modèle de classification	
		Protégé	Classifié
Très faible/Faible	Profil A	PaFF	DrFF
Modéré	Profil B	PbMM	CMM
Élevé/Très élevé	Profil C	PcEE	SEE

Tableau 1 - Conversion des profils du PCCTI en profil du modèle de classification

Par « **révision** », on entend la possibilité de réviser le profil obtenu lors de l'analyse de préjudices du PCCTI en un profil dont au moins un des objectifs de sécurité est de même niveau de préjudice selon le modèle de classification. La révision permet de définir les profils plus précisément selon les niveaux de préjudices retenus pour chacun des objectifs

de sécurité. Cependant, sa fiabilité dépend largement de la qualité des analyses de préjudices du PCCTI et du niveau de documentation de ces dernières. Si les informations du PCCTI sont incorrectes, incomplètes ou inexactes, une analyse complète du système devra être réalisée.

Pour des raisons d'efficacité liées à la révision des analyses de préjudices, les niveaux « Très faible/Faible » et « Élevé/Très élevé » sont combinés et deviendront respectivement les niveaux « Faible » et « Élevé » pour les objectifs de sécurité portant sur l'intégrité et la disponibilité uniquement. Les cinq niveaux de préjudices sont maintenus pour l'objectif de sécurité portant sur la confidentialité.

Le tableau suivant présente les choix de profils comparables provenant du modèle de classification selon le profil obtenu lors de l'analyse de préjudices du PCCTI.

Profils PCCTI	Profils comparables du modèle de classification	
	Protégé	Classifié
Profil A (Les objectifs de sécurité ne dépassent pas le niveau Faible)	NcFF	
	PaFF	DrFF
Profil B (Les objectifs de sécurité ne dépassent pas le niveau Modéré)	NcFM, NcMF, NcMM	
	PaFM, PaMF, PaMM PbFF, PbFM, PbMF, PbMM	DrFM, DrMF, DrMM CFF, CFM, CMF, CMM
Profil C (Au moins un des objectifs de sécurité a atteint le niveau Élevé)	NcFE, NcME, NcEF, NcEM, NcEE	
	PaFE, PaME, PaEF, PaEM, PaEE PbFE, PbME, PbEF, PbEM, PbEE PcFF, PcFM, PcFE, PcMF, PcMM, PcME, PcEF, PcEM, PcEE	DrFE, DrME, DrEF, DrEM, DrEE CFE, CME, CEF, CEM, CEE SFF, SFM, SFE, SMF, SMM, SME, SEF, SEM, SEE

Tableau 2 - Profils comparables du modèle de classification

Procédure de conversion/révision

Afin de réaliser une conversion ou une révision des profils du PCCTI vers le modèle de classification, une procédure en deux étapes est proposée. Avant de commencer, il est nécessaire de récupérer les résultats obtenus (profil et niveaux de préjudices par objectif de sécurité) des analyses de préjudices réalisées dans le cadre de la revue diligente du PCCTI.

Étape 1 : Déterminer la catégorie d'appartenance « Protégé »/« Classifié » des données.

- Selon le modèle de classification, les données appartiennent à l'une ou l'autre des catégories suivantes :
  - Protégé : données qui concernent une personne physique, une entreprise ou une autre entité;
  - Classifié : données qui concernent l'État.

La section 2 présente la détermination de la catégorie d'appartenance.

Étape 2 : En fonction du profil (A, B ou C) à traiter, déterminer s'il s'agit d'une conversion ou d'une révision.

- Dans le cas d'une **conversion :** il s'agit de convertir le profil à traiter en un profil prédéterminé du modèle de classification. En fonction de la catégorie d'appartenance des données et du profil à traiter, choisir le profil du modèle de classification à l'aide du *Tableau 1 – Conversion des profils du PCCTI en profil du modèle de classification*.

Exemple : Conversion d'un Profil C

Une analyse de préjudices d'un système, contenant des renseignements personnels qui pourraient mettre en danger la vie d'une personne, indique qu'il possède le ***« Profil C »****.*

Afin d'effectuer une conversion de cette analyse, il est nécessaire de déterminer la catégorie d'appartenance des données du système. Puisque le système contient des renseignements personnels, il appartient à la catégorie « Protégé ».

Selon le tableau 1, le profil du modèle de classification serait PcEE.

Dans cet exemple, la conversion du profil C deviendrait PcEE.

- Dans le cas d'une **révision :** il s'agit de réviser le profil à traiter en un profil de mêmes niveaux de préjudices du modèle de classification. En fonction de la catégorie d'appartenance des données et des niveaux de préjudices identifiés pour chacun des objectifs de sécurité, choisir le profil du modèle de classification à l'aide du *Tableau 2 – Profils comparables du modèle de classification*.

Exemple : Révision d'un Profil C

Une analyse de préjudices d'un système, contenant des renseignements personnels qui pourraient mettre en danger la vie d'une personne, fournit les niveaux de préjudices suivants pour les trois objectifs de sécurité :

- ***Élevé** pour l'objectif de confidentialité;*
- ***Modéré** pour l'objectif d'intégrité;*
- ***Faible** pour l'objectif de disponibilité.*

*Comme l'objectif de confidentialité possède le niveau de préjudice le plus élevé, c'est ce dernier qui détermine le profil PCCTI, soit **Élevé** ou **« Profil C »**.*

Afin d'effectuer une révision de cette analyse, il est nécessaire de déterminer la catégorie d'appartenance des données du système. Puisque le système contient des renseignements personnels, il appartient à la catégorie « Protégé ».

Contrairement au PCCTI, le profil du modèle de classification est déterminé par les trois objectifs de sécurité. En reprenant cet exemple, le profil retenu est : « PcMF » où :

- *Pc= **Élevé** pour l'objectif de confidentialité;*
- *M= **Modéré** pour l'objectif d'intégrité;*
- *F= **Faible** pour l'objectif de disponibilité.*

Dans cet exemple, la révision du profil C deviendrait PcMF.

Si la procédure de conversion/révision soulève des enjeux nécessitant une réévaluation d'un ou plusieurs objectifs de sécurité, l'OP devra procéder à une nouvelle analyse de préjudices en respectant toutes les étapes du modèle de classification.

Annexe 3 – Description du tableau des données visées par une restriction au droit d'accès

Cette figure présente un extrait du tableau des données visées par une restriction au droit d'accès et en décrit le contenu pour faciliter sa compréhension.

Renseignements visés par une restriction au droit d'accès en vertu de la section II du chapitre II de la LAI

Des niveaux minimal et maximal de préjudices applicables en vertu du modèle de classification sont suggérés, pouvant aller de « Très faible » à « Très élevé »

En vertu de la LAI			En vertu du Modèle de classification			
Catégorie de données	Types de données	Restriction facultative ou impérative	Catégorie d'appartenance	Confidentialité niveau MINIMAL	Confidentialité niveau MAXIMAL	Exemples
Renseignements personnels	Renseignements personnels sensibles	Impérative	Protégé	Modéré	Élevé[2]	**Modéré :** Renseignements médicaux et numéro d'assurance maladie **Modéré :** Renseignements financiers ou fiscaux (salaire, actif, passif, déclaration de revenus, etc.) **Élevé :** Renseignements en lien avec des enquêtes policières (ex. : délateurs, infiltrations policières, etc.).

Exemples de niveau de préjudice modéré

Exemple de niveau de préjudice élevé

La LAI prévoit deux restrictions au droit d'accès :

- **Restriction facultative :** la confidentialité **peut** être assurée (une demande d'accès à l'information peut être autorisée);
- **Restriction impérative :** la confidentialité **doit** être assurée (une demande d'accès à l'information ne peut être autorisée).

Les catégories d'appartenance sont :

- « données classifiées » ou « classifié »;
- « données protégées » ou « protégé ».

Notons que certains types de données peuvent se retrouver dans l'une ou l'autre des catégories d'appartenance.

Annexe 4 – Formation d'un comité de classification de sécurité des données

Un comité spécialisé devrait être constitué pour favoriser une classification adéquate des données.

La composition des membres de ce comité peut varier selon les besoins. Les rôles et responsabilités qui sont proposés ici peuvent être adaptés en fonction du contexte de l'OP. Ce dernier devrait également mettre en place les mécanismes d'approbation des travaux du comité.

Ce comité est chargé, notamment :

- de procéder à la collecte de l'information requise pour la classification;
- de définir l'étendue de la classification;
- de planifier les activités et les échéanciers de réalisation;
- d'organiser et d'animer les entrevues et les ateliers de travail;
- de produire les documents de travail nécessaires à l'exercice de classification;
- de consolider et de présenter les résultats de la classification.

Rôles et responsabilités proposés :

Chargé de projet
Le chargé de projet coordonne les activités du comité. Il identifie les ressources requises et planifie les exercices de classification.

Conseiller en sécurité de l'information
Le conseiller en sécurité possède une maîtrise des concepts de sécurité de l'information et du modèle de classification des données. Il est le gardien de la pratique de classification de sécurité. Il présente le modèle de classification et les outils afférents aux autres membres du comité et les guide dans leur utilisation. Il anime les séances d'analyse de préjudices et consigne les résultats.

Détenteur ou propriétaire des données
Cet intervenant peut également être désigné sous différents termes tels que propriétaire du système, responsable du processus d'affaires, analyste ou pilote d'affaires. Il joue un rôle clé dans la classification de sécurité. Il fournit les informations pertinentes sur les processus d'affaires, la sensibilité des données (préjudice en regard d'une violation de CID), ainsi que sur les systèmes d'information qui les sous-tendent. Il participe activement à l'analyse de préjudices et recommande les résultats de la classification pour le comité.

Responsable de l’accès aux documents et de la protection des renseignements personnels (RADPRP)
Le RADPRP joue un rôle-conseil auprès du comité dans l’analyse de préjudice, eu égard aux restrictions à l’accès aux documents et à la protection des renseignements personnels formulées en vertu de la *Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels*.

Autres intervenants
Le comité peut s’adjoindre toute personne qui est en mesure de l’appuyer dans ses travaux. Citons, à titre d’exemple, toute personne clé ayant une bonne connaissance de son unité administrative, de ses processus d’affaires et de leurs interrelations ou, encore, les conseillers en architecture technologique, les conseillers en architectures de données, les conseillers juridiques, les spécialistes en gestion documentaire, les vérificateurs internes ou les répondants de l’OP pour les données ouvertes.

Québec