# QUESTIONS ET RÉPONSES

## LE MODÈLE DE CLASSIFICATION DES DONNÉES NUMÉRIQUES GOUVERNEMENTALES

Votre gouvernement

Québec

# Table des matières

Ce document présente des réponses aux questions posées lors de la séance d'information du ministère de la Cybersécurité et du Numérique (MCN) concernant le Modèle de classification de sécurité des données numériques gouvernementales (ci-après « le Modèle de classification »).

## Questions d'ordre général

**En quoi cette démarche s'articule-t-elle autour de l'application de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25)?**

La Loi 25 impose des obligations strictes en matière de protection des renseignements personnels et le Modèle de classification de sécurité s'inscrit dans cette logique en fournissant une approche standardisée pour classifier les données. La classification de sécurité des données peut notamment être un intrant à l'évaluation des facteurs relatifs à la vie privée (EFVP).

**Le nouveau modèle fait-il une distinction entre les termes « données » et « information »?**

Le Modèle de classification ne fait pas la distinction entre les termes « données » et « information ». Cependant, en vertu du Modèle de classification et selon la granularité choisie, une donnée peut notamment être assimilable à une activité, un service, une opération, un processus, un regroupement d'actifs informationnels ou un actif informationnel.

**Quelle est la différence entre l'analyse des préjudices et l'analyse de risque?**

L'analyse des préjudices permet d'apprécier le niveau de sensibilité des données en évaluant le niveau de préjudice causé par une compromission sur la confidentialité, l'intégrité et la disponibilité. Elle ne tient pas compte des mesures de sécurité en place.

L'analyse de risque, quant à elle, prend en compte la probabilité qu'une menace se concrétise et l'efficacité des mesures de sécurité en place. Selon l'approche préconisée par le Modèle de classification, l'analyse de risque est réalisée au besoin, une fois l'analyse des préjudices terminée.

**Le fait que chaque organisme public (OP) fasse cette analyse séparément ne risque-t-il pas de donner des résultats différents pour une même donnée?**

Pour atténuer ce risque, le Modèle de classification propose une démarche et des grilles d'analyse communes à tous les OP. Une formation en ligne est également disponible.

La page Centre gouvernemental de cyberdéfense : Classification de sécurité des données numériques gouvernementales regroupe l'ensemble de la documentation et des outils disponibles concernant le Modèle de classification.

**N'y a-t-il pas un risque que les personnes classifient par prudence à un niveau de préjudice plus élevé que nécessaire?**

Le risque de surévaluation de la classification de sécurité, c'est-à-dire attribuer à des données un niveau de préjudice plus élevé qu'il ne l'est réellement, souvent par crainte de commettre une erreur, existe. Ce comportement peut entraîner des conséquences indésirables, par exemple :

- Des coûts supplémentaires liés à la mise en place de mesures de sécurité inutiles;
- Des restrictions excessives rendant l'accès aux données plus complexe qu'il ne devrait l'être.

Pour atténuer ce risque, il est essentiel que le personnel suive les formations disponibles et utilise les outils et guides mis à sa disposition. La page Centre gouvernemental de cyberdéfense : Classification de sécurité des données numériques gouvernementales regroupe l'ensemble de la documentation et des outils disponibles concernant le Modèle de classification.

En cas de doute, après réflexion, le personnel ne doit pas hésiter à demander de l'aide. Il est toujours préférable de valider une classification plutôt que de la surévaluer.

**Les documents classifiés (exemples : « diffusion restreinte » ou « confidentiel ») sont-ils à l'abri des demandes d'accès à l'information?**

Quelle que soit la classification de sécurité, toute demande d'accès à l'information doit être transmise au responsable des demandes d'accès, qui est la personne habilitée à déterminer si l'information peut être communiquée, en tout ou en partie. La classification des données constitue un élément clé dans cette analyse, mais ne détermine pas à elle seule la décision finale.

**La classification de sécurité et l'inventaire des données peuvent-ils être réalisés indépendamment?**

Oui, ces deux exercices peuvent être réalisés séparément, mais ils sont complémentaires.

L'inventaire des données permet d'identifier et de répertorier les données détenues par un OP, tandis que la classification de sécurité vise à évaluer leur sensibilité afin d'appliquer des mesures de protection adaptées.

Dans cette optique, le MCN propose une démarche intégrée permettant de concilier l'inventaire et la classification des données. Toutefois, il est également possible de classifier les systèmes d'information sans nécessairement réaliser un inventaire détaillé des données qu'ils stockent ou traitent.

**L'utilisation du Référentiel de l'information gouvernementale (RIG) est-elle obligatoire?**

L'utilisation du Référentiel de l'information gouvernementale (RIG) n'est pas obligatoire, mais fortement recommandée. Le RIG est une application Web conçue par le MCN pour inventorier les données numériques gouvernementales. En lien avec le Modèle de classification, il permet notamment la classification de sécurité, la conversion des analyses des préjudices du Programme de consolidation des centres de traitement informatique (PCCTI) et la tenue du registre de classification de sécurité conforme aux exigences.

**Pour les OP dont les services sont impartis au ministère de la Cybersécurité et du Numérique (MCN), est-il prévu que des outils soient déployés?**

Les OP doivent soumettre une demande au MCN, en précisant les configurations souhaitées dans l'outil Purview. Le MCN assurera ensuite leur mise en œuvre technique. Toutefois, il appartient à chaque OP de définir sa propre stratégie de déploiement, en intégrant la gestion du changement, la mise en place d'un projet pilote et l'élaboration des processus internes adaptés.

**Si nous ne sommes pas connectés au réseau de télécommunication gouvernemental RITM, est-il possible de convertir nos analyses des préjudices du Programme de consolidation des centres de traitement informatique (PCCTI) à l'aide du Référentiel de l'information gouvernementale (RIG)?**

Des travaux sont en cours (date à préciser) afin de permettre l'accès au RIG pour les OP non connectés au RITM. En attendant, une conversion manuelle reste possible, même sans connexion au RIG, en appliquant la procédure prévue à l'annexe 2 du guide d'accompagnement.

## Questions sur l’application du Modèle de classification

### Qui évaluera les types de préjudices dans notre organisation?

**Données structurées** : cette analyse est généralement réalisée par un comité de classification de sécurité, composée de représentants des lignes d’affaires, des données et des systèmes, de la sécurité de l’information, de la protection des renseignements personnels et d’autres représentants dont l’expertise est jugée pertinente. L’annexe 4 du guide d’accompagnement 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 des gabarits d’utilisation courante, effectuée par le comité de classification de sécurité des données, comme défini à l’annexe 4 du guide d’accompagnement.

### Que recommandez-vous comme revue périodique de la classification des données structurées?

Le Modèle de classification n’impose pas de fréquence de revue périodique. Toutefois, une bonne pratique consisterait à effectuer une réévaluation régulière, particulièrement lors de changements, afin de s’assurer que la classification des données demeure alignée avec l’évolution des risques, des exigences organisationnelles et des obligations réglementaires.

### Est-il obligatoire d'utiliser exactement la grille des niveaux de préjudice de l’Annexe 2 de l’arrêté ministériel ou peut-on l’ajuster selon la mission de l’OP?

La grille des niveaux de préjudice figurant à l’Annexe 2 de l’arrêté ministériel doit être appliquée dans son intégralité afin d’assurer une uniformité dans l’utilisation du Modèle de classification.

### Comment procéder à la classification quand aucun des 10 types de préjudices ne semble s'appliquer à certaines données?

L’OP doit vérifier si les données concernent des citoyens, des entreprises ou l’État. Dans l’affirmative, il doit considérer les types de préjudices correspondants. Il est possible, dans certaines situations, que les niveaux de préjudices soient très faibles pour chacun des types de préjudices retenus. La classification sera donc « non classifié ». Il est nécessaire de justifier les niveaux pour chacun des types de préjudices retenus.

**Comment considère-t-on les préjudices à l'OP dans l'évaluation?**

Lors de l'analyse des préjudices, l'OP doit porter une attention aux impacts potentiels pour l'État, plutôt que de se limiter aux conséquences affectant directement son fonctionnement interne, comme un secteur, une direction ou encore son image (par exemple, une attention médiatique négative). Il doit ainsi se référer aux types de préjudices T5 à T10 du Modèle de classification qui ne concernent pas l'OP en particulier, mais l'administration publique ou le gouvernement dans son ensemble. Le Modèle de classification met l'accent sur les préjudices causés à l'État, plutôt que sur les préjudices limités à un OP.

**Est-il obligatoire de documenter les raisons justifiant les niveaux de préjudice pour tous les préjudices?**

Oui, le Modèle de classification exige de documenter l'analyse des préjudices afin d'assurer une traçabilité. Les personnes ayant réalisé l'analyse pourraient ne plus être en poste ou ne plus se souvenir des justifications.
Pour un préjudice très faible, une simple mention comme « Aucun préjudice significatif identifiable » suffit. Dès qu'un préjudice, même faible, est identifié, il est recommandé de le documenter.

**Comment déterminer la catégorie d'un document contenant à la fois des données protégées et classifiées?**

Selon le Modèle de classification, si un objet à classifier (système, document, etc.) contient des données classifiées et protégées, il sera considéré comme « classifié ». Cela dit, il est recommandé que la catégorie « protégé » prévale lorsque le niveau de préjudice est inférieur ou égal à « modéré ». Au-delà de ce seuil, la catégorie « classifié » s'applique.

Par exemple, si un objet contient des renseignements personnels avec un niveau de préjudice modéré, il devrait être de catégorie « protégé », même s'il inclut également certaines données « classifié » avec un niveau de préjudice modéré ou inférieur. En revanche, si ce même objet contient des données « classifié » avec un niveau de préjudice élevé ou très élevé, il devrait se voir attribuer la catégorie « classifié ».

**Comment gérer les données des employés de l'État – « protégé » ou « classifié »?**

Puisque les employés de l'État sont des personnes, les données sont généralement de catégorie « protégé ».

**La volumétrie des données est-elle prise en compte pour évaluer un préjudice?**

Oui, le volume de données concernées est pris en compte dans l'analyse des préjudices. Le modèle de classification propose une appréciation qualitative du volume en utilisant des expressions telles que « lourdes », « beaucoup » ou « généralisé » pour identifier certains préjudices.

De plus, des situations de regroupement peuvent également être envisagées. Par exemple, la divulgation non autorisée d'un dossier contenant des renseignements personnels peut causer un préjudice modéré à la personne concernée. Cependant, si tous les dossiers des ressources humaines d'une organisation publique étaient divulgués, le niveau de préjudice pourrait être beaucoup plus élevé pour l'État. Le regroupement s'applique généralement à la confidentialité, mais peut également concerner l'intégrité et la disponibilité des données.

## Questions spécifiques au marquage des données

**Les documents conservés dans les systèmes avec données structurées doivent-ils aussi être marqués?**

Oui, tous les documents doivent être marqués.

**Est-il obligatoire de marquer chacun des 1,5 million de documents PDF dans notre voûte documentaire?**

Non, le marquage systématique de tous les documents n'est pas requis. La priorité de marquage doit être accordée aux documents nouvellement créés, modifiés ou réutilisés, en appliquant un marquage progressif.

**Jusqu'à quelle date antérieure devons-nous marquer les documents existants?**

Il n'y a pas d'obligation de marquer les documents existants de manière systématique. Seuls les documents réutilisés ou modifiés doivent être considérés.

**Le marquage doit-il s'appliquer sur chaque document ou peut-il être fait à un niveau supérieur (exemple : rubriques du plan de classification)?**

Le marquage doit s’appliquer sur chaque document.

**Peut-on appliquer un marquage au niveau des paragraphes dans un document textuel ?**

Oui, c’est possible, bien que le Modèle de classification propose un marquage au niveau du document. Toutefois, chaque OP peut adapter le niveau de granularité de la classification en fonction de ses besoins. Dans certains cas, cette granularité pourrait être affinée jusqu’au niveau des paragraphes d’un document.

**Quelle classification par défaut devrait-on attribuer aux données nouvellement créées?**

Les outils de classification des environnements bureautiques peuvent attribuer des étiquettes par défaut, comme « non classifié » pour un courriel. Toutefois, il appartient à chaque OP de définir et d’appliquer les étiquettes par défaut en fonction de ses besoins et de sa politique de sécurité.

**Comment gérer les données dont la classification change avec le temps (exemple : un rapport financier confidentiel qui devient public à sa publication)?**

La classification d'un document doit être mise à jour systématiquement lorsqu'un changement de statut survient. Cela inclut l'ajustement du marquage.

Par exemple, un rapport financier initialement classé « confidentiel » devra être reclassifié comme « non classifié » au moment de sa publication officielle. Ce processus contribue à une gestion efficace de l'accès à l'information tout en maintenant la protection des données sensibles durant leur cycle de vie.

**Sera-t-il obligatoire d'appliquer un chiffrement avec Purview?**

Non, le chiffrement n'est pas systématiquement obligatoire. Afin de faciliter le déploiement du marquage et d'assurer une cohérence entre les OP, des configurations minimales adaptées aux technologies disponibles dans Microsoft 365 sont proposées. Ces configurations sont dites minimales, car elles permettent d'apposer une étiquette de confidentialité sur les documents sans appliquer immédiatement de mesures de sécurité restrictives, comme le chiffrement. Il revient à chaque OP de définir et d'appliquer les mesures de sécurité appropriées en fonction de ses besoins spécifiques.

Québec