

# POLITIQUE INTERNE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

*À l'attention du personnel du Musée National des Beaux-arts du Québec*

*Version de septembre 2023*



Jean-Luc Murray  
Directeur général MNBAQ

Résolution: CA 2023-12-14 9.1

## Table des matières

1.	PRÉAMBULE .....	3
2.	DÉFINITIONS.....	3
3.	BUT ET OBJECTIFS DE LA POLITIQUE.....	4
4.	CHAMP D'APPLICATION .....	4
5.	RÔLES ET RESPONSABILITÉS.....	4
6.	LES EXIGENCES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS.....	4
6.1	Les principes directeurs .....	4
6.2	Les évaluations des facteurs relatifs à la vie privée (ÉFVP) et les clauses contractuelles de protection des Renseignements personnels - gestion des tiers et transferts hors Québec .....	9
6.3	La gestion des Incidents de Confidentialité .....	9
6.4	La formation et la sensibilisation .....	9
7.	LE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS .....	10
8.	CONFORMITÉ .....	10
9.	MISE EN ŒUVRE, SUIVI ET RÉVISION .....	10

## 1. PRÉAMBULE

Le Musée National des Beaux-arts du Québec (le **Musée**) reconnaît l'importance de protéger la vie privée dans le cadre de ses activités, notamment avec l'émergence constante de nouvelles technologies permettant la collecte, l'utilisation et la communication de Renseignements personnels.

## 2. DÉFINITIONS

**Anonymisation** : procédé permettant de faire en sorte qu'un RP ne permette plus de façon irréversible d'identifier directement ou indirectement un Individu.

**Incident de confidentialité (Incident)** : s'entend de la perte, du vol, de l'accès non autorisé intentionnel ou par inadvertance, de l'utilisation ou de la divulgation non autorisée d'un renseignement personnel.

**Individu** : tout le personnel, administrateur ou dirigeant, client, partenaire d'affaires externe au Musée, ou autre personne dont le Musée a été, est ou sera amené à collecter, utiliser, conserver, communiquer, détruire ou anonymiser les RP.

**Profilage** : évaluation de certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou de son comportement.

**Renseignement personnel (RP)** : tout renseignement qui porte sur une personne physique et qui, seul ou combiné à d'autres renseignements, permet de l'identifier directement ou indirectement. Un Renseignement personnel peut être : le nom, l'adresse domiciliaire, l'adresse de courriel, le numéro de téléphone, la date de naissance. Ce peuvent aussi être des identifiants numériques uniques comme l'adresse IP d'ordinateur ou les identifiants uniques d'un appareil mobile ainsi que les préférences personnelles, les données de géolocalisation, les données de sondages, les visites de Sites Web dans la mesure où ces données sont associées aux renseignements personnels d'une personne. Les Renseignements personnels ne comprennent pas : les Renseignements personnels qui ont été anonymisés par la suppression de détails susceptibles de les identifier, de sorte que les données ne puissent pas être associées à une personne en particulier et les coordonnées professionnelles d'une personne.

**Renseignement personnel sensible (RP sensible)** : tout RP qui suscite un haut degré d'attente raisonnable en matière de vie privée, notamment en raison du préjudice potentiel à la personne en cas d'Incident. Ce sont, par exemple, les données biométriques, les RP de santé, les RP financiers, le NAS, le numéro de passeport, etc.

**Traitement ou traiter (de ou un RP)** : tout ou partie des activités suivantes que sont la collecte, l'utilisation, la conservation, la communication, la destruction ou l'anonymisation de RP.

**Traitement automatisé** : processus qui permet d'utiliser les RP d'un Individu en vue d'analyser et de prédire son comportement, par exemple, pour déterminer ses besoins.

### 3. BUT ET OBJECTIFS DE LA POLITIQUE

La Politique de protection des renseignements personnels (la « Politique ») décrit les normes et les pratiques de protection des renseignements personnels (PRP) appliquées par le Musée et vise les objectifs suivants :

- Énoncer les orientations et les principes directeurs destinés à assurer efficacement la protection des Renseignements personnels ;
- Adopter les meilleures pratiques reconnues comme telles en matière de PRP ;
- Protéger les RP qui sont recueillis par le Musée tout au long de leur cycle de vie, c'est-à-dire de leur collecte à leur destruction ou anonymisation, en passant par leurs utilisation, communication, et conservation.

### 4. CHAMP D'APPLICATION

La Politique s'applique à tous les employés du Musée, y compris, mais sans s'y limiter, à son personnel, aux tiers avec lesquels le Musée a une relation contractuelle, aux sous-traitants exécutant des fonctions en lien avec le traitement de RP, à toutes les personnes morales ou physiques qui utilisent ou ont accès aux RP recueillis et/ou détenus par le Musée.

Le Musée est responsable de s'assurer que l'ensemble de ces personnes respectent les principes directeurs énoncés dans la Politique.

### 5. RÔLES ET RESPONSABILITÉS

Les rôles et responsabilités des intervenants responsables d'assurer le respect et la mise en œuvre de la Politique sont décrits dans la Matrice RACI, jointe comme Annexe A.

### 6. LES EXIGENCES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Cette Politique soutient l'engagement continu du Musée à respecter et à protéger la confidentialité et la sécurité des RP qu'il recueille des Individus suivants :

- a) Tous les clients du Musée ;
- b) Les représentants des fournisseurs de services passés, actuels et futurs du Musée qui doivent fournir des RP pour établir une relation d'affaires avec lui ;
- c) Le personnel passé, actuel et futur du Musée ;
- d) Toute autre personne physique dont les RP sont traités dans le cadre des activités du Musée.

#### 6.1 Les principes directeurs

Le Musée s'engage à respecter les principes directeurs en matière de PRP mentionnés ci-dessous conformément à la Loi :

1. **Responsabilité.** Le Musée est responsable du traitement des RP qu'il a en sa possession, y compris les renseignements qui sont confiés à des tiers. Le Musée a nommé un chef de la PRP, dont les coordonnées se trouvent ci-dessous, qui s'assure de l'application de cette Politique et s'assure que le Musée se conforme aux lois et règlements relatifs à la P PRP.
2. **Identifier les finalités.** Le Musée doit préalablement déterminer les raisons pour lesquelles il veut collecter, utiliser, communiquer et/ou conserver des RP. Le Musée s'assure de collecter uniquement les RP qui sont nécessaires pour répondre aux finalités prédéterminées.
3. **Consentement.** À moins d'exceptions prévues dans la Loi, pour pouvoir collecter, utiliser et communiquer les RP d'une personne, le Musée s'assure d'obtenir le consentement de cette dernière en l'informant préalablement :
  - Des finalités pour lesquelles ses RP seront recueillis ;
  - Des différents moyens par lesquels ils seront recueillis ;
  - De son droit d'accès à ses RP, de son droit de les rectifier ;
  - Du nom des tiers à qui ils sont communiqués ;
  - De son droit de retirer son consentement à tout moment, sous réserve de restrictions légales ou contractuelles;
  - Le cas échéant, du transfert des RP en dehors du Québec.

Le Musée s'assure également d'obtenir le consentement approprié en fonction de la nature du RP qu'il recueille. Le consentement de l'Individu devra être manifeste et exprimé de manière expresse notamment dans les cas suivants :

- Si le RP sensible qui a été recueilli est utilisé à une fin autre que celle pour laquelle il a été initialement collecté et qu'aucune exception prévue à la Loi ne peut s'appliquer;
  - Si la collecte se fait au moyen d'une solution technologique dont les fonctions permettent d'identifier, localiser ou d'effectuer un Profilage sur elle.
4. **Collecte.** Le Musée recueille les RP directement auprès de l'Individu concerné à moins d'avoir obtenu son consentement à ce que ses RP soient collectés auprès de tiers ou que la Loi l'autorise à les collecter autrement.

Le Musée limite la collecte des RP uniquement à ceux qui sont nécessaires pour les fins de ses activités.

Le Musée recueille des RP pour les fins suivantes:

Catégorie de personne concernée	Fins de collecte
Clients	<ul style="list-style-type: none"> <li>• Déterminer votre admissibilité aux produits ou services du Musée et vérifier le respect de conditions pouvant s'appliquer;</li> <li>• Confirmer l'identité des individus, vérifier l'exactitude des Renseignements personnels et les mettre à jour, à des fins de transactions ainsi que dans le but de réduire la fraude ou les erreurs dans le traitement des transactions;</li> </ul>

	<ul style="list-style-type: none"> <li>• Procéder à l'abonnement initial ou au renouvellement de l'abonnement au Musée;</li> <li>• Gérer et maintenir les dossiers et comptes créés lors de l'achat (la consultation de documentation, l'accès à des services) ou la réservation d'activité en ligne;</li> <li>• Gérer des demandes relatives aux produits et services offerts (offrir les produits et services requis ou susceptibles de vous intéresser ; traiter l'information relative à vos achats et demandes de services ainsi qu'au traitement du paiement de ceux-ci ; etc.);</li> <li>• Gérer, administrer ses programmes et s'assurer que les membres reçoivent les services, rabais et avantages appropriés en conformité avec les modalités applicables;</li> <li>• Études, sondages, analyses, ciblage, segmentations, statistiques, notamment afin d'établir des tarifications, de comprendre et d'analyser les intérêts, les besoins et les préférences des abonnés et clients, et pour veiller à la qualité des produits et services, effectuer des vérifications internes ou mener des activités d'amélioration continue;</li> <li>• Communiquer avec vous, répondre aux questions, aux demandes de commentaires ou traiter les plaintes;</li> <li>• Répondre à nos exigences légales et réglementaires.</li> </ul>
<p><b>Candidats à l'emploi pour un poste au sein du Musée</b></p>	<ul style="list-style-type: none"> <li>• Évaluer votre candidature;</li> <li>• Conserver les résultats de l'évaluation de votre candidature à des fins de références futures;</li> <li>• Communiquer avec vous.</li> </ul>
<p><b>Employés et autres ressources externes du Musée</b></p>	<ul style="list-style-type: none"> <li>• Confirmer l'identité, vérifier l'exactitude des Renseignements personnels et les mettre à jour, à des fins de transactions – notamment le paiement des salaires et autres avantages sociaux – ainsi que dans le but de réduire la fraude ou les erreurs dans le traitement des transactions;</li> <li>• Gérer et maintenir les dossiers employés;</li> <li>• Gérer des demandes relatives au salaire, aux avantages sociaux et aux autres composantes de la rémunération;</li> <li>• Études, sondages, statistiques, notamment aux fins de mesure de la satisfaction des employés et d'amélioration continue;</li> <li>• Communiquer avec vous, répondre aux questions, aux demandes de commentaires ou de plaintes;</li> <li>• Répondre à nos exigences légales et réglementaires.</li> </ul>
<p><b>Utilisateur du site Internet et des applications du Musée</b></p>	<ul style="list-style-type: none"> <li>• Gérer les sites Web et services en ligne, établir des tendances et des statistiques relatives à leur utilisation, évaluer leur performance et améliorer les services;</li> <li>• Personnaliser et adapter votre expérience de navigation selon vos besoins;</li> <li>• Répondre à vos demandes soumises via le site web;</li> </ul>

	<ul style="list-style-type: none"> <li>• Effectuer des analyses statistiques afin de vous proposer des publicités et des sondages ciblés.</li> </ul>
<b>Toute autre personne</b>	<ul style="list-style-type: none"> <li>• Répondre à vos demandes transmises par téléphone, par courriel ou par la poste;</li> <li>• Organiser des événements récréatifs ou de réseautage;</li> <li>• Procéder à des appels de courtoisie;</li> <li>• Envoyer du matériel promotionnel.</li> </ul>

- 5. Limitation de l'utilisation, de la communication et de la conservation.** Le Musée s'assure que les RP qu'il collecte soient utilisés ou communiqués uniquement aux seules fins pour lesquelles ils ont été recueillis et pour lesquelles l'Individu concerné a consenti, à moins que ce dernier ne donne son consentement aux nouvelles finalités, ou à moins d'exceptions prévues dans la Loi. Par exemple, le Musée peut, sans le consentement de l'individu concerné, communiquer les RP de celle-ci au directeur des poursuites criminelles et pénales dans le cadre d'une poursuite intentée contre cet Individu pour une infraction commise à l'égard d'une Loi, bien que les RP n'aient pas été collectés initialement pour cette fin.

Le Musée s'assure également de limiter l'accès aux RP aux seuls individus ayant la qualité pour les recevoir lorsque ces RP sont nécessaires à l'exercice de leurs fonctions.

- 6. Conservation.** Le Musée s'assure de ne conserver les RP qu'il recueille que pour la durée raisonnablement nécessaire pour accomplir les fins pour lesquelles ces RP ont été recueillis, et conformément aux délais prévus au calendrier de conservation joint comme Annexe B, et selon la Loi.

- 7. Destruction et anonymisation.** Lorsque les RP collectés ne sont plus nécessaires aux fins pour lesquelles ils ont été collectés et que l'échéance de conservation est terminée, le Musée s'assure de les détruire ou de les anonymiser, selon les procédures applicables.

Un RP pourra être anonymisé seulement pour des fins sérieuses et légitimes. La procédure d'anonymisation devra être approuvée par le Responsable de la PRP afin de s'assurer que les meilleures pratiques ont été mises en place.

- 8. Exactitude.** Le Musée s'assure de l'exactitude des RP recueillis et conservés dans le cadre de ses activités. Le principe d'exactitude vise à réduire la possibilité que des informations inappropriées soient utilisées pour prendre une décision concernant un Individu. L'individu concerné par les RP collectés par le Musée aura le droit de les faire rectifier si nécessaire.

- 9. Mesures de sécurité.** Le Musée met en place des mesures de sécurité proportionnelles à la sensibilité des RP qu'il recueille afin de les protéger contre la perte, le vol et contre l'accès, la communication, la copie, l'utilisation ou la modification non autorisés, conformément à ses encadrements en matière de Sécurité de l'information. Ces mesures de sécurité comprennent des mesures organisationnelles, physiques et technologiques telles que la gestion des accès à ses locaux, ses systèmes, ses réseaux informatiques, de même que la sensibilisation et la formation du personnel du Musée.

- 10. Transparence.** Le Musée documente ses pratiques de gestion des RP de façon simple et claire et les rend accessibles.

Lorsque le Musée recueille des RP auprès de l'Individu en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un Profilage, il doit l'informer du recours à une telle technologie et des moyens qui lui sont offerts pour activer ces fonctionnalités. Le recours à ce type de technologie pour collecter des RP nécessite que les paramètres de confidentialité de la solution offrent le plus haut standard de confidentialité.

- 11. Formation et sensibilisation.** Le Musée forme et sensibilise son personnel en matière de PRP, pour s'assurer que le personnel comprend les exigences à respecter et les mets en pratique. Le personnel qui occupe un poste clé au regard des objectifs de protection de la vie privée (ex : personnel qui intervient dans la gestion d'incidents, dans l'attribution des accès, etc.) reçoit en sus des formations dispensées à tous les collaborateurs du Musée, une formation adaptée à son rôle et ses responsabilités.

- 12. Droits des individus concernés.** Le Musée déploie des procédures permettant de traiter les demandes suivantes :

#### **12.1 Accès et rectification des RP**

Une Individu concerné peut faire une demande écrite au Musée afin de consulter les RP collectés le concernant, pour en vérifier l'exactitude, pour en demander la rectification au besoin et pour connaître les catégories de tiers à qui ils ont été communiqués, à moins d'exceptions prévues dans la Loi.

Ces demandes seront transmises au Responsable de la PRP pour traitement conformément à la Loi.

#### **12.2 Traitement automatisé**

Dans la mesure où le Musée met en place un processus de décision exclusivement fondé sur un traitement automatisé, il doit informer l'Individu concerné qu'il fait l'objet d'un tel processus, de la décision qui a été rendue et de son droit de présenter ses observations à l'égard de cette décision. Un Individu concerné peut, sur demande, être informé, notamment :

- des RP utilisés pour rendre cette décision ;
- des raisons ayant mené à cette décision ;
- De son droit de faire rectifier les RP utilisés pour rendre cette décision.

**12.3 [En vigueur à compter du mois de septembre 2024] Portabilité :** Tout Individu concerné doit pouvoir, sur demande, obtenir une copie des RP qui ont été collectés sur lui. Si ces RP sont informatisés, il peut demander qu'ils lui soient communiqués dans un format technologique structuré et couramment utilisé.

**12.4 Préoccupations et plaintes :** Une Individu concerné peut poser des questions et soulever des préoccupations à l'égard de ses RP. Il peut également déposer une plainte à la suite du non-respect des

principes énoncés dans la Politique. Toutes questions, préoccupations ou plaintes devront être acheminées au Responsable de la PRP.

## 6.2 Les évaluations des facteurs relatifs à la vie privée (ÉFVP) et les clauses contractuelles de protection des Renseignements personnels - gestion des tiers et transferts hors Québec

Le Musée est responsable de tous les RP qu'il détient, divulgue ou communique à des tiers. Pour s'assurer que ces RP bénéficient d'une protection adéquate, le Musée déploie des mesures de protection, telles que :

1. La rédaction de clauses contractuelles permettant aux tiers de traiter les RP seulement pour des fins spécifiques et selon les meilleurs standards en matière de PRP.
2. La réalisation d'ÉFVP dans toutes les situations pour lesquelles la Loi exige une telle évaluation.

L'ÉFVP est un processus d'analyse qui permet aux personnes responsables de la collecte, de l'utilisation ou de la divulgation des RP d'évaluer les risques relatifs à la protection de la vie privée associés à ces activités et déterminer des mesures visant à atténuer les risques identifiés et évalués.

Une ÉFVP devra être réalisée, conformément aux exigences règlementaires, dans les cas suivants :

- Dans le cadre de l'acquisition, du développement, de la refonte d'un système d'information ou d'un projet de prestation de services électroniques impliquant la collecte, l'utilisation, la divulgation, la conservation ou la destruction de RP.
- Lorsque les RP concernés sont transférés à l'extérieur du Québec.
- Lorsque des RP sont recueillis dans le cadre de l'exercice des attributions du Musée ou la mise en œuvre d'un programme d'un organisme public avec lequel le Musée collabore pour une prestation de services ou pour la réalisation d'une mission commune.

De plus, lorsque le Musée communique des RP qu'elle détient à un tiers, elle doit également s'assurer que l'encadrement contractuel stipule les engagements appropriés en matière de PRP.

## 6.3 La gestion des incidents de confidentialité

Le Musée met en place des mesures adéquates afin d'assurer la gestion des Incidents, le tout conformément au Plan de gestion des incidents de Sécurité de l'information et de Confidentialité.

Dès lors qu'un membre du personnel soupçonne ou prend connaissance d'un Incident portant atteinte à la vie privée ou portant atteinte à la confidentialité de RP, il devra immédiatement aviser le Responsable de la PRP.

## 6.4 La formation et la sensibilisation

Le Musée ajoute des formations et des mécanismes de communication destinés à sensibiliser le personnel, ses conseillers, ses partenaires et fournisseurs à l'importance de la PRP dans son programme de formation relatif à la Sécurité de l'information. Le nouveau personnel s'engage par écrit à traiter les RP, conformément aux

principes énoncés dans la Politique, au moment de son embauche. Le cas échéant, cet engagement est consolidé lors de la signature du contrat de travail, de service ou de partenariat.

Une formation sur la PRP est obligatoire à l'embauche. Une formation annuelle (ou selon les besoins) est organisée à titre de rappel et des formations spécifiques sont élaborées si certains employés ou groupes identifiés ont des besoins d'apprentissage plus ciblés et plus approfondis en matière de PRP.

Le programme de formation et de sensibilisation est révisé sur une base annuelle afin de refléter les changements apportés aux réglementations applicables en matière de PRP.

## 7. LE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La fonction de Responsable de la PRP du Musée a été attribuée à :

M<sup>e</sup> Marc Lajoie, LL. B., LL. M.

Secrétaire général et conseiller juridique

Musée national des beaux-arts du Québec

Parc des Champs-de-Bataille

Québec (Québec) G1R 5H3

Canada

[secretariat.general@mnbaq.org](mailto:secretariat.general@mnbaq.org)

Télécopieur : 418 644-1067

## 8. CONFORMITÉ

Le non-respect de cette Politique peut entraîner des manquements ou violations du Code de conduite, d'éthique et des valeurs du Musée. Ainsi le processus de dénonciation doit être effectué rapidement afin de permettre au Musée de prendre en charge la situation. Selon la gravité de la violation, des mesures administratives ou disciplinaires peuvent inclure, sans s'y limiter, un avis verbal, une réprimande, une suspension ou un congédiement. Le Musée pourra mettre fin à une entente qui le lie à un tiers ou à un sous-traitant qui ne se conforme pas à la Politique et qui exécute des fonctions en lien avec le traitement de RP ou qui utilise ou a accès aux RP recueillis par le Musée.

## 9. MISE EN ŒUVRE, SUIVI ET RÉVISION

La Politique entre en vigueur à la date de sa signature par le Responsable de la PRP indiquée ci-dessous. Elle est révisée tous les cinq (5) ans, ou plus tôt si des modifications du cadre juridique ou des évolutions technologiques affectent son application.

La Politique a été mise à jour pour la dernière fois le 20 septembre 2023. La Politique remplace toutes les versions antérieures, le cas échéant, et est susceptible d'être modifiée à tout moment à la seule discrétion du Musée.

**Annexe A : Matrice RACI des rôles et responsabilités en matière de Protection des renseignements personnels**

Document séparé.

Matrice des rôles et responsabilités (RACI) du programme de PRP cible (post projets de mise en œuvre de la feuille de route).

**Responsabilités**

**R=Réalisateur**

La personne qui effectue le travail pour accomplir la tâche. Il y a au moins un rôle réalisateur, bien que d'autres puissent être délégués pour aider au travail requis.

**A=Approbateur (Imputable/responsable)**

Il est l'ultime responsable de la réalisation correcte et complète du produit livrable ou de la tâche, et celui qui délègue le travail aux réalisateurs. En d'autres termes, il approuve le travail fourni. Un seul approbateur doit être spécifié pour chaque ligne.

**C=Consulté**

**Légende :**

Rôle	R = Réalisateur
	A = Approbateur
	C = Consulté
	I = Informé

**Définitions acronymes :**

**CPO:** Chief privacy officer / **RPRP:** Responsable de la protection des renseignements personnels

No	RACI PRP	Phase	RPRP/secrétaire général	Comité PRP	Directeur des TI / Responsable Sécurité	Direction des RH	Direction générale adjointe (gestion des risques)	Direction de la communication et du Marketing	Services des Finances	Comité de gestion du changement	archives	Comité de gestion	autre unité
	Nom du responsable		Marc Lajoie	Marc Lajoie	Patrick Lefebvre	Nadia Béland	Patrice Savoie	Sophie Lemelin	Nancy Gagné	Nadia Béland	Nathalie Thibault	Patrice Savoie	

**Stratégie**

1.1	Développer et maintenir une stratégie de PRP	Stratégie	A	R	C	C	I	C	na	C	C	I	na
1.2	Identifier les besoins financiers et en ressources pour soutenir le programme de PRP	Stratégie	R	R	R	R	A	C	C	na	na	I	na
1.3	Développer et maintenir des veilles législatives, réglementaires et de marché sur les enjeux de PRP	Stratégie	A	R	C	na	C	C	C	na	C	I	na

**Organisation et gouvernance**

2.1	Assurer la direction et l'orientation du programme de PRP	Organisation et gouvernance	A	R	C	C	C	C	na	na	na	I	na
2.2	Développer et maintenir le programme de PRP, procéder à allocation du budget/ressources et effectuer les investissements nécessaires	Organisation et gouvernance	A	R	R	na	C	na	R	na	i	I	na
2.3	Définir la stratégie d'implémentation du programme de PRP au sein de l'organisation	Organisation et gouvernance	A	R	R	R	C	R	R	R	na	I	na
2.4	Assurer la gestion du changement	Organisation et gouvernance	C	C	C	I	I	C	na	R/A	C	I	na
2.5	Assurer le conseil et la surveillance en matière de PRP au sein des lignes d'affaires	Organisation et gouvernance	A	R	R	I	C	I	I	I	I	I	na
2.6	Identifier et remédier à la matérialisation des risques en matière de PRP (ex. gestion des incidents et notification, au besoin, aux personnes concernées et aux régulateurs)	Organisation et gouvernance	R/A	C/I	R	C	I	C	na	na	C	I	na
2.7	Exécuter des processus de PRP (ex. collecte, transfert/communication, notification, suppression de données/comptes)	Organisation et gouvernance	A	C	R	R	R	R	R	R	R	na	na

**Politiques, procédures et pratiques**

3.1	Développer et maintenir les politiques de PRP (internes et externes)	Politiques, procédures et pratiques	A	R	R/C	R/C	R/C	C	na	na	C	I	na
-----	--	-------------------------------------	---	---	-----	-----	-----	---	----	----	---	---	----

3.2	Développer et maintenir les processus et procédures de PRP à l'échelle de l'organisation	Politiques, procédures et pratiques	A	R	R	R	C	C	na	R	C	I	na
3.3	Aligner les processus et procédures de PRP de l'organisation avec les requis des lignes d'affaires	Politiques, procédures et pratiques	A	R	R	R	R	R	R	R	R	R	na
3.4	Répondre aux demandes d'exercice des droits des individus en matière de PRP (plaintes, accès, rectification, etc) au moyens d'outils appropriés (scripts, documentation, escalade, etc)	Politiques, procédures et pratiques	R/A	C	C	C	C	C	C	na	C	na	na
3.5	Obtenir et gérer les consentements (identification des requis et vérification des libellés de consentement)	Politiques, procédures et pratiques	A	I	R	C	I	R	na	na	I	I	na
3.6	Encadrer la communication à des tiers et les transferts de RP transfrontaliers	Politiques, procédures et pratiques	A/R	I	R	na	I	R	na	na	I	I	na
3.7	Encadrer la conservation et la disposition des RP	Politiques, procédures et pratiques	R	I	R	C	C	C	na	R	A	I	na
3.8	Opérationnaliser la disposition des RP	Politiques, procédures et pratiques	C	I	A	C	C	I	na	R	R	na	na
3.9	Communiquer avec les autorités (ex. Commission accès à information)	Politiques, procédures et pratiques	R/A	C	R	I	I	C	na	na	na	I	na

#### Communication, formation et sensibilisation

4.1	Développer une stratégie de communication (interne et externe)	Communication, formation et sensibilisation	C	C	C	C	C	A/R	na	C	na	I	na
4.2	Développer une formation PRP à l'échelle de l'organisation	Communication, formation et sensibilisation	R/A	C	R	R	I	C	na	C	R	na	na
4.3	Implémenter des formations et de la sensibilisation à l'échelle de l'organisation	Communication, formation et sensibilisation	R/A	C	R	R	I	C	na	I	R	na	na
4.4	Surveiller l'accomplissement et la mise à jour des formations au sein des lignes d'affaires	Communication, formation et sensibilisation	R/A	R	R	R	I	na	na	I	na	na	na

#### Audit et conformité, évaluation des risques et surveillance

5.1	Développer et maintenir un outil EFVP et fournir des recommandations	Audit et conformité, évaluation des risques et surveillance	A	R	R	na	I	na	na	na	na	na	R approv.
5.2	Initier une EFVP (déclencheur/identifier le besoin pour une EFVP)	Audit et conformité, évaluation des risques et surveillance	R/A	C	R	na	I	na	na	na	na	na	R approv.
5.3	Réaliser une EFVP	Audit et conformité, évaluation des risques et surveillance	R/A	C	I	na	I	na	na	na	na	na	R approv.
5.4	Réaliser la reddition de compte PRP	Audit et conformité, évaluation des risques et surveillance	R/A	I	I	na	I	na	na	na	na	I	R approv.

5.5	Définir et tester les contrôles de PRP	Audit et conformité, évaluation des risques et surveillance	R/A	I	R	na		na	na	na	na	na	na
5.6	Revoir la conformité du programme de PRP	Audit et conformité, évaluation des risques et surveillance	R/A	R	C	C	C	C	C	na	C	I	na
5.7	Auditer la conformité du programme de PRP	Audit et conformité, évaluation des risques et surveillance	R/A	R	C	C	C	C	C	na	C	I	na

**Métriques et reddition**

6.1	Développer des indicateurs/métriques de performance et de risques	Métriques et reddition	R/A	R	C	C	C	C	na	C	C	C	na
6.2	Suivre, surveiller et rapporter la performance sur la base des indicateurs/métriques de PRP	Métriques et reddition	R/A	R	C	C	C	C	na	na	na	I	na
6.3	Faire rapport au comité d'audit du conseil d'administration	Métriques et reddition	R/A	I	C	na	R	I	na	na	na	I	na

#### Avis de non responsabilité

Le présent document a été préparé par KPMG s.r.l./S.E.N.C.R.L.(«KPMG») et est destiné à l'usage interne de MNBAQ («le client»), conformément aux conditions du contrat de mission (le « contrat de mission») daté du 7 juin 2023 conclu avec le client. Le présent document est fourni au client sur une base confidentielle, et il ne peut être fourni à aucune autre personne ou entité sans l'autorisation expresse écrite de KPMG et du client. KPMG ne garantit pas et ne déclare pas que les informations contenues dans le présent document sont exactes, complètes, suffisantes ou adéquates pour leur usage par toute personne ou entité autre que le client, ou pour toute autre fin que celle énoncée dans le contrat de mission. Toute personne ou entité autre que le client ne devra pas s'y appuyer, et KPMG décline expressément dans la présente toute responsabilité ou obligation à l'égard de toute personne ou entité autre que le client pouvant découler de l'usage du présent document.