POLITIQUE DE GESTION DES RENSEIGNEMENTS PERSONNELS

Version : 2.0

Date de création ou de révision : 2023-09-25

Rédigé par : MS Solutions

Table des matières

1 OBJECTIF DU DOCUMENT

La présente politique énonce les règles de gestion des renseignements personnels chez MS Solutions en respectant les exigences de sécurité de l'information.

Elle définit en outre les dispositions génériques relatives au marquage, à la classification et à la manipulation des données.

2 RÔLES ET RESPONSABILITÉS

2.1 Le propriétaire de l'information :

Le propriétaire de l'information est celui qui décide qui a accès à l'information et quel est son niveau d'accès. Il est chargé d'identifier la sensibilité des informations, de les classer de manière appropriée et d'appliquer les politiques et les procédures pour les protéger.

Le propriétaire de l'information doit également s'assurer que tous les employés qui ont accès aux informations sous sa responsabilité sont correctement formés sur les pratiques de sécurité et comprennent leur rôle dans la protection des informations.

MS Solutions peut nommer des propriétaires de l'information selon le principe de qui est la personne responsable si la sécurité de l'information est touchée?

Les propriétaires de l'information peuvent donc être nommés par type de client, portefeuille de client ou domaine d'affaires. Le plus important c'est que les informations (en particulier les renseignements personnels) aient des propriétaires.

3 CHAMP D'APPLICATION

La présente politique s'adresse à toutes les entités du MS Solutions. Elle couvre l'ensemble des accès logiques aux systèmes d'information.

4 DÉFINITIONS

- **Systèmes d'information (« SI »)** : Un ensemble de composants interconnectés qui fonctionnent ensemble pour collecter, stocker, traiter et distribuer des informations.
- **Renseignement personnel (« RP »)** selon la commission d'accès à l'information du Québec : « Les renseignements personnels sont ceux qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée ». Un renseignement personnel ou « RP » est toute information qui permet, de façon directe ou indirecte, d'identifier de façon unique une personne. Les renseignements personnels n'incluent pas l'information liée à l'exercice d'une fonction au sein d'une entreprise (adresses de courriel, numéro de travail professionnel...). Parmi les renseignements personnels :
    - Nom, prénom, adresse, téléphone, code postal ;
    - Date de naissance ;
    - État civil ;
    - Nationalité ;
    - Informations médicales.
- **Sécurité des données** : Le principe de « sécurité des données » comporte l'obligation de prendre les mesures de sécurité appropriées, de sorte qu'il faut régulièrement revoir et améliorer les mesures pour les adapter aux nouvelles technologies et aux nouveaux risques qui apparaissent au fil du temps. Les entreprises devraient mettre en œuvre des mesures de sécurité adaptées au contexte, ce qui implique que la rigueur de ces mesures dépendrait du niveau de risque et de la nature des renseignements personnels concernée.
- **Principe de responsabilité** : Introduit par la loi 25, le principe vise à responsabiliser les entreprises à adopter de bonnes pratiques en matière de protection des renseignements personnels, notamment par la mise en place de documents encadrant la collecte, l'utilisation, la communication et la conservation des renseignements personnels.

5 RÈGLES DE SÉCURITÉ

5.1 Cycle de vie des renseignements personnels

À l'image de chaque information, un renseignement personnel passe par 5 étapes :

5.1.1 Collecte

Il s'agit de l'étape initiale où l'information est récupérée. Cette récupération peut être sous forme d'une information communiquée par la personne concernée ou transmise par une tierce partie.

Généralement la récupération se fait de trois façons :

- Recueilli : formulaire rempli, information envoyée par un fournisseur… ;
- Créé : un profil avec des renseignements personnels est créé au niveau d'un système d'information ;
- Inféré : information déduite de la corrélation d'autres informations.

Obligation MS Solutions pour la collecte :

- Déterminer les fins de collecte ;
- Limiter la collecte aux besoins déterminés ;
- Utiliser les moyens légaux pour la collecte ;
- Informer la personne concernée et obtenir son consentement.

5.1.2 Utilisation

Après avoir été collectée, l'information doit souvent être traitée d'une manière ou d'une autre. Cela pourrait impliquer de l'analyser, de le catégoriser ou de le transformer en un format différent. Le traitement est souvent nécessaire pour rendre l'information plus utile ou pour la préparer en vue de son stockage ou de sa diffusion.

Obligation de MS Solutions pour l'utilisation :

- Limiter les accès aux seules personnes ayant l'habilitation pour la recevoir ;
- Limiter l'utilisation aux fins déterminées lors de la collecte.

5.1.3 Communication

La communication décrit l'étape où l'information est communiquée en interne ou entre différentes parties concernées.

Obligation MS Solutions pour la communication :

- Avoir un consentement pour les informations collectées ;
- Respecter les exigences légales lors de la communication de l'information à une tierce partie.

5.1.4 Conservation

Une fois que les informations ont été traitées, elles sont généralement stockées dans un type de référentiel telles qu'une base de données, un serveur de fichiers ou un service de stockage infonuagique. Le support de stockage utilisé peut varier en fonction du type et de la quantité de données stockées, ainsi que d'autres facteurs tels que les exigences de sécurité et d'accessibilité.

Obligation MS Solutions pour la conservation :

- Assurer la qualité des renseignements personnels ;
- Prendre des mesures de sécurité propres pour assurer la sécurité des renseignements personnels.

5.1.5 Destruction

Finalement, les informations peuvent devenir obsolètes ou non pertinentes et devront être éliminées. Cela peut impliquer la suppression de fichiers, le déchiquetage de documents papier ou la destruction d'autres informations pour s'assurer qu'elles ne peuvent pas être consultées ou utilisées de manière inappropriée.

5.2 Classification de l'information

- **Recommandation 1 :** Les informations de MS Solutions doivent être identifiées et classifiées sur trois niveaux de classification (Confidentiel, Interne, Public) en se basant sur l'échelle suivante :

Niveau	Description
Confidentiel	Information qui aurait un impact significatif sur MS Solutions si elle était communiquée en dehors des personnes nommément désignées pour en faire la consultation. Le circuit de validation et de communication de l'information confidentielle obéit à des règles très strictes. Les informations confidentielles sont généralement réservées à un nombre limité de personnes qui ont un besoin légitime d'y accéder.
Interne	Information ayant vocation à demeurer au sein de MS Solutions. Sa communication à l'extérieur de l'entreprise ne peut se faire que sur autorisation d'un responsable habilité.
Public	Information qui peut être rendue publique sans implication pour l'entité ou pour l'organisation.

- **Recommandation 2 :** La classification concerne tout type d'information, quel qu'en soit le support et doit être apparente *(exemple : pied de page pour les fichiers bureautiques, bandeau de classification pour la messagerie électronique …)* sur chacun d'eux à l'exception des documents destinés par nature à la communication au public telle que cartes de visite, informations du site internet, etc.
- **Recommandation 3 :** Par défaut toute information non classifiée par son propriétaire prendra par défaut la classification « Interne ».
- **Recommandation 4 :** L'information reçue d'un organisme tiers fera l'objet de reclassification par le responsable de l'entité destinataire du MS Solutions (*qui devient systématiquement le propriétaire)* afin de garantir, la conformité avec les

directives d'utilisation, d'archivage, de communication, de stockage et de destruction de l'information en interne.

- **Recommandation 5 :** La classification d'une information doit être réexaminée annuellement par son propriétaire qui, à cet effet, prend la responsabilité de sa déclassification.
- **Recommandation 6** : L'information classifiée *« Public »* peut être diffusée à l'extérieur de MS Solutions.

5.3 Marquage et Manipulation de l'information

Les dispositions figurant au tableau ci-après définissent les actions de marquage à entreprendre suivant le niveau de classification des informations et les précautions minimales concernant la manipulation de celles-ci.

Les mesures préconisées peuvent être complétées par chaque entité en fonction des dispositions spécifiques (réglementations, lois, contrats) applicables aux informations traitées (données personnelles, données commerciales …).

	Public	**Interne**	**Confidentiel**
Collecte *(Création /Acquisition)*	• Les en-têtes ou pieds de page des documents électroniques doivent être marqués « public ».	• La liste de diffusion de l'information doit être identifiée. • Les en-têtes ou pieds de page des documents électroniques doivent être marqués « interne ».	• La liste de diffusion de l'information doit être identifiée. • Les en-têtes ou pieds de page des documents électroniques doivent être marqués « Confidentiel ».

	Public	Interne	Confidentiel
Utilisation ***(Accès, traitement et mise à jour)***	• Accès public.	• Seules les personnes internes doivent avoir accès.	• Les accès aux informations confidentielles doivent être tracés. • Les accès aux informations confidentielles se font uniquement via des ressources informatiques maitrisées par MS Solutions. • L'environnement d'accès aux systèmes traitant les informations confidentielles doit être protégé (sans risque d'interception ou de compromission).

Utilisation ***(Transmission)***	• En règle générale, pas besoin d'une autorisation pour la transmission en dehors de MS Solutions.	• En règle générale, pas de transmission en dehors de MS Solutions sans autorisation préalable.
		• Les pièces jointes doivent être chiffrées lors de l'envoi par courrier électronique à l'externe.
		• Pour des échanges en format papier à l'externe, il est nécessaire de protéger physiquement les supports servant à ces échanges.
		• Ajout d'un « Disclaimer » pour les courriers électroniques sortants.
			• L'envoi par courrier électronique non chiffré est strictement interdit.
			• Pour des échanges sur supports physiques (papier, clés USB et autres) avec l'extérieur, il est nécessaire d'utiliser des emballages adaptés au transport d'informations confidentielles :
			  ○ Livraison recommandée avec remise à main propre.
			  ○ Possibilité de repérer facilement toute violation de l'emballage .

	Public	Interne	Confidentiel
Utilisation ***(Impression/Duplication)***	• Aucune mesure particulière.	• Obtenir l'autorisation du propriétaire du document avant de le copier.	• Obtenir l'autorisation du propriétaire de l'information avant de faire des copies. • Les copies doivent être marquées « Confidentiel » et la liste des destinataires doit correspondre à la liste de diffusion de l'information.
Conservation ***(Stockage /Archivage/ Sauvegarde)***	• Pas d'exigence spécifique pour les informations publiques concernant leur stockage, leur archivage et leur sauvegarde.	• Les documents doivent être chiffrés lors de leur stockage (disques durs, clés USB et autres), de leur archivage, ou de leur sauvegarde. • Les versions papier sont conservées sous clé.	• Les documents doivent être chiffrés lors de leur stockage (disques durs, clés USB et autres), de leur archivage, ou de leur sauvegarde. • Les versions papier sont conservées dans une armoire forte ou un coffre-fort.
Destruction	• Effacement des supports électroniques. • Déchiquetage des impressions papier.	• Effacement sécurisé des fichiers électroniques via un outil d'effacement électronique agréé par MS Solutions.	• Destruction ou effacement sécurisé le plus rapidement possible pour les supports préparatoires (papier, clés USB et autres) ayant servi à l'élaboration de l'information classifiée « Confidentiel ».

5.4 Inventaire des actifs informationnels

La création d'un inventaire des actifs informationnels est l'exercice de comprendre les types de données possédées ainsi qu'où elles se trouvent. Cet exercice doit être minimalement fait pour les renseignements personnels.

Voici quelques étapes générales effectuées pour créer l'inventaire des données :

- **Identifiez toutes les sources de données** : Élaborer une liste de tous les différents endroits où les données sont stockées. Cela peut inclure les bases de données, les serveurs de fichiers, les applications, le stockage en nuage, les appareils mobiles et tout autre endroit où les données sont collectées ou stockées.
- **Catégoriser les données** : Une fois les sources de données identifiées, catégoriser les données en fonction de leur type, de leur sensibilité et de leur criticité.
- **Spécifier si des renseignements personnels sont présents** : Pour chaque actif informationnel, il faut préciser si des renseignements personnels sont inclus dans cet actif. Si c'est le cas, l'actif informationnel doit être traité comme des renseignements personnels.
- **Mettre à jour l'inventaire** : Il est important de tenir à jour l'inventaire des données à mesure que de nouvelles sources de données sont ajoutées, que les anciennes sources de données sont supprimées et que les attributs de données changent.

En suivant ces étapes, vous pouvez créer un inventaire complet des actifs informationnels qui aidera à préciser les types de données détenues, où elles se trouvent et comment elles sont utilisées.

5.5 Communication des renseignements personnels

Par défaut, un renseignement personnel est classé « Confidentiel » ainsi MS Solutions ne doit pas communiquer ces renseignements sans le consentement de la personne concernée, sauf les exceptions prévues par la loi.

Les exceptions pour la communication sont :

- Transactions commerciales ;
- Tiers autorisés.

5.5.1 Transactions commerciales

MS Solutions peut (lors de la conclusion d'une transaction commerciale dont elle est partie prenante et qui nécessite de communiquer des renseignements personnels) partager les RP et ceci sans consentement de la personne concernée par le renseignement. Néanmoins une entente doit préalablement être conclue avec l'autre partie, stipulant notamment que cette dernière partie s'engage :

- L'autre partie utilise l'information exclusivement pour les fins convenues dans la transaction ;
- À ne pas communiquer l'information sans avoir une autorisation explicite de la part de la personne concernée ;
- À protéger le caractère confidentiel de l'information ;
- À procéder à la destruction de l'information si la transaction n'aboutit plus ou si l'information n'est plus nécessaire à la conclusion de la transaction.

5.5.2 Tierces autorisées

À certaines conditions, la Loi sur le privé autorise l'entreprise à communiquer un renseignement personnel, sans le consentement de la personne concernée, aux tiers autorisés par la loi comme (le procureur, à une personne ou à un organisme ayant pouvoir de contraindre à leur communication et qui les requiert dans l'exercice de ses fonctions, à un service d'archives dans certaines conditions et/ou après un certain délai…).