Aide-mémoire

TOUR D'HORIZON SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS – EMPHASE SUR LES NOUVELLES EXIGENCES

C'EST QUOI UN RENSEIGNEMENT PERSONNEL (RP) ?

- Tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier est un RP. (Art. 2 Loi sur le privé).
- Un RP n'est accessible au personnel d'une entreprise que s'il a la qualité pour le connaître et qu'à la condition que ce RP soit nécessaire à l'exercice de ses fonctions. (Art. 20 Loi sur le privé).
- Il est confidentiel. Sauf exception, il ne peut être communiqué sans le consentement de la personne concernée.
- Si une seule information peut paraître anodine, elle peut, quand elle est combinée à d'autres, permettre d'identifier une personne physique. Dans ce contexte, ces informations constituent des RP qu'il faut protéger.
- Exemples de RP (liste non exhaustive) :

Nom et prénom	Numéro de téléphone	Adresse	Adresse courriel personnelle	Date de naissance
Tranche d'âge	No. de carte bancaire ou de carte de crédit	Numéro d'assurance sociale	Numéro de passeport	Niveau d'éducation
Dossier disciplinaire	Noms des parents, conjoints, enfants	Historique des transactions	Adresse IP	Dossier médical
Pièce d'identité	Salaire	Nom bénéficiaire (assurance vie)	CV et notes d'entrevue d'embauche	Renseignements biométriques

INFORMATIONS SUR LE CONSENTEMENT

- Il doit être manifeste, libre, éclairé et être donné à des fins spécifiques déterminées à l'avance. (Art. 4 et 14 Loi sur le privé).
- Il doit être demandé à chacune de ces fins, en termes simples et clairs dans une section distincte de vos demandes de consentement par écrit. (Il faudra ajuster vos documents servant à la collecte de RP ex : formulaires, sondages, correspondances, etc.).
- La personne concernée peut demander qu'on lui prête assistance pour comprendre la portée du consentement demandé. (Sur les documents servant à la collecte de RP, il faudra indiquer les coordonnées d'une personne en mesure de lui prêter assistance.)
- Il ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.
- Un consentement qui n'est pas donné conformément à la Loi est sans effet.
- Lorsqu'un consentement doit être obtenu relativement à un RP sensible (par exemple de nature médical ou financière), il faut obligatoirement obtenir un consentement express, préférablement par écrit.

PRINCIPES À RETENIR

- Avant de collecter des RP, il faut déterminer pourquoi nous en avons besoin (les fins de la collecte).
- Lors de la collecte, on ne peut recueillir que les RP nécessaires aux fins déterminées avant la collecte.
- Les RP doivent être recueillis auprès de la personne concernée directement, à moins d'obtenir son consentement ou qu'une loi autorise la cueillette auprès d'un tiers.
- Lors de la collecte de RP, il faut respecter les obligations d'information et de transparence et informer les personnes concernées des éléments prévus aux articles 7 à 8.1, 12.1 de la Loi sur le privé, soit notamment :
  - Le type de RP collecté, les fins pour lesquels ils sont recueillis, qui peut y avoir accès, etc.;
  - Les droits d'accès et de rectification prévus à la loi;
  - Le droit de retirer son consentement à la communication ou à l'utilisation des RP recueillis.
- Les RP ne peuvent être utilisés que pour les fins déterminées avant la collecte, à moins d'obtenir le consentement de la personne visée ou que la Loi l'autorise. (Art. 12 Loi sur le privé)
- Les RP ne doivent pas être communiqués à un tiers à moins d'obtenir le consentement de la personne visée ou que la Loi l'autorise.
- Sous réserve d'un délai de conservation prévu par une loi, lorsque la finalité de la collecte des RP est accomplie, il faut les détruire ou les anonymiser. (Art. 23 Loi sur le privé)
  - Se référer à votre calendrier de conservation pour les délais de conservation (voir le service du Centre de documentation pour plus de détails).

QU'EST-CE QU'UN INCIDENT DE CONFIDENTIALITÉ ?

Type d'incident	*Exemples*
Accès non autorisé à un RP	*Une personne d'une autre direction, d'une autre organisation, un fournisseur, etc. a accès à des RP auxquels elle ne devrait pas avoir accès. Intrusion d'une base de données en raison d'une sécurité informatique inadéquate ou d'une cyberattaque.*
Utilisation non autorisée d'un RP	*Des RP sont utilisés dans un autre contexte que celui pour lequel ils ont été recueillis sans le consentement de la personne concernée ni autorisation par la Loi.*
Communication non autorisée d'un RP	*Des RP sont communiqués à des tiers sans le consentement de la personne concernée ni autorisation par la Loi. Un RP est transmis par erreur à la mauvaise personne.*
Perte d'un RP ou toute atteinte à la protection d'un tel renseignement	*Un document comprenant un RP est perdu ou volé, mal classé ou détruit alors qu'il devait être conservé.*

QUELLES SONT LES MESURES À PRENDRE EN CAS D'INCIDENT DE CONFIDENTIALITÉ ?

1. Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé aux personnes concernées et éviter que de nouveaux incidents de même nature ne se produisent (rappeler le courriel, communiquer avec le destinataire pour lui demander d'effacer le courriel sans en prendre connaissance, aviser la DTI en cas de tentative d'hameçonnage, etc.).
2. Aviser votre supérieur(e).
3. Évaluer le risque de préjudice sérieux (sensibilité du RP, conséquences appréhendées de son utilisation, probabilité qu'il soit utilisé à des fins préjudiciables) et apporter les correctifs nécessaires pour éviter que la situation se reproduise et aviser la Commission d'accès à l'information si nécessaire (étape à réaliser avec votre Responsable de la protection des renseignements personnels (RPRP)).
4. Compléter le registre d'incident avec votre supérieur(e) et votre RPRP.