Règlement Général sur la Protection des Données (RGPD)

Introduction et impacts pour les organisations canadiennes

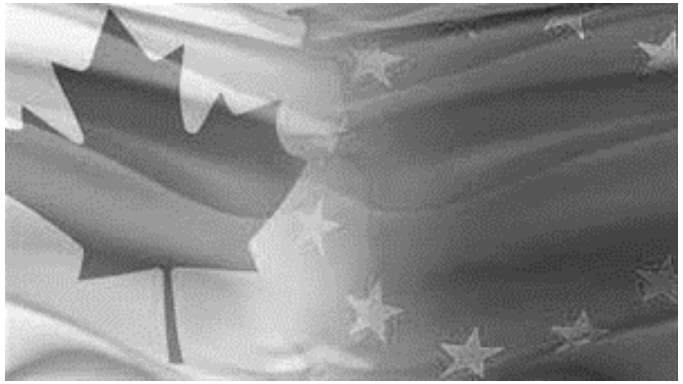
ISACA - Section de Québec
Colloque PRP
1er juin 2017

Mélanie Gagnon, CIPM, CISA

MGSI
www.dataprotection.lu

Agenda

1 **Introduction au RGPD**



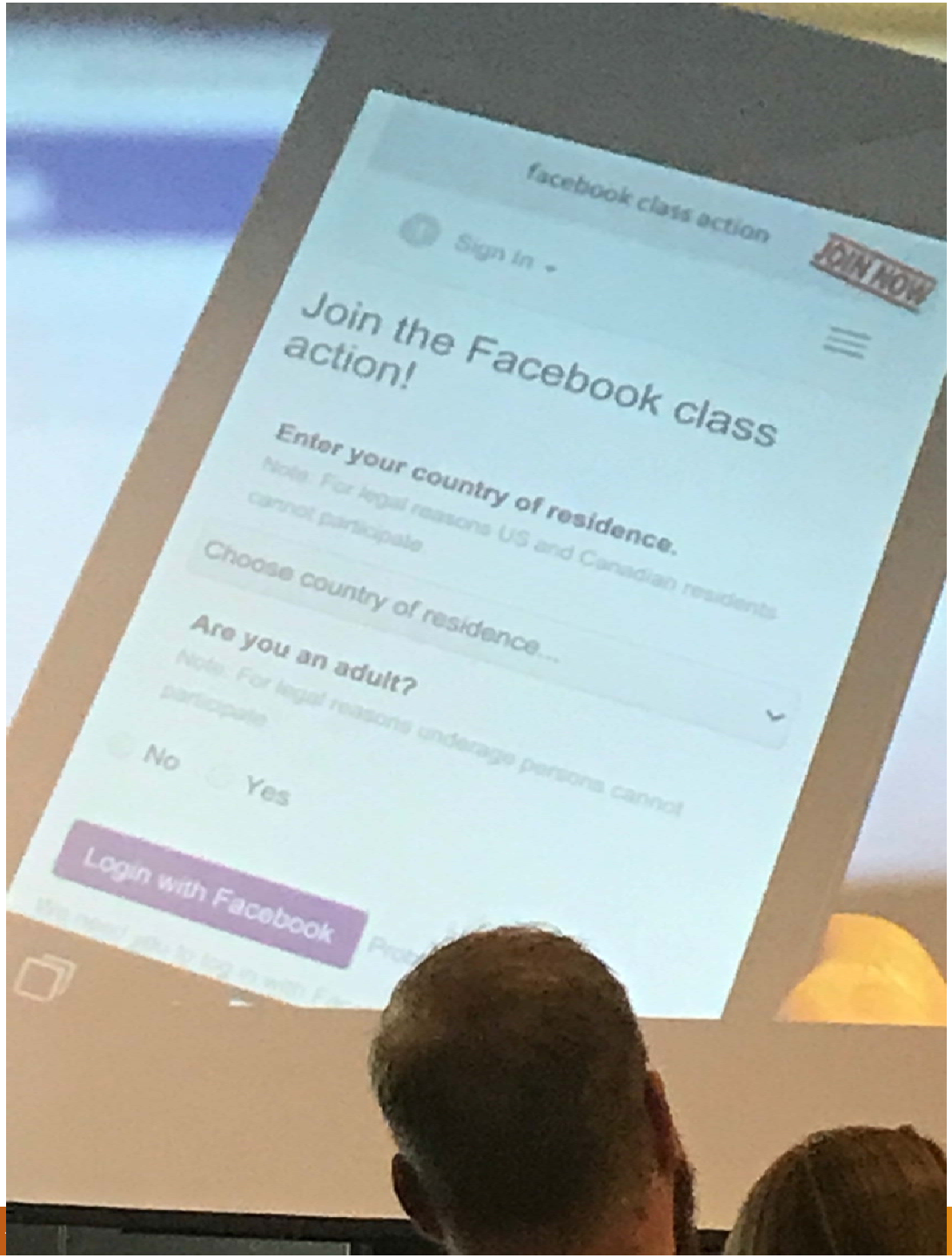
2 **Impacts du RGPD pour les sociétés canadiennes**

3 **Exigences du RGPD**

Introduction au RGPD – *En quelques mots*

Nouveau règlement général sur la protection des données

- Adopté le 27 avril 2016 et *applicable à partir du 25 mai 2018*
- Applicable *directement dans toute l'Europe*, il harmonise la législation au niveau européen
- *Renforce les droits des personnes* concernées et les *devoirs des responsables* de traitement et leur sous-traitants
- Des *sanctions importantes* (jusque 2 à 4 % du CA annuel mondial ou 10 M€ à 20 M€)
- Intégration de la possibilité de « class action » par des associations représentant les personnes concernées


facebook class action
Sign In
JOIN NOW
Join the Facebook class action!
Enter your country of residence.
Choose country of residence...
Are you an adult?
No
Yes
Login with Facebook


KEEP
CALM
AND
PREPARE
FOR GDPR


Adoption
Entrée en application
< 12 mois pour se conformer
27 Avril 2016
1er juin 2017
25 Mai 2018

Introduction au RGPD – *En quelques mots*

Renforcement des droits des personnes

- Information claire et compréhensible
- Nouveaux droits
- Maîtrise de ses données personnelles

Renforcement des obligations

- Concept d'« Accountability » - démonstration de la conformité vs. formalité préalable (gouvernance)
- Mesures organisationnelles et techniques appropriées/adéquates selon la nature, la portée, le contexte et les finalités du traitement
- Importance de définir les différents rôles : autorité de contrôle, responsable de traitement, sous-traitant, destinataire, etc.

Introduction au RGPD – *En quelques mots*

Champ d'application

- Le responsable de traitement ou le sous-traitant est **établi sur le territoire de l'UE** (que le traitement ait lieu ou non dans l'Union);
- Le responsable de traitement ou le sous-traitant n'est pas établi sur le territoire de l'UE, mais:
  - **Offre des biens ou des services aux personnes résidant dans l'UE**, qu'un paiement soit exigé ou non desdites personnes;
  - **Surveille le comportement des personnes qui se trouvent sur le territoire de l'UE**, dans la mesure ou il s'agit d'un comportement qui a lieu au sein de l'Union.

Données à caractère personnel

Toute information, quelque soit sa nature et son support se rapportant à :

- Une personne physique identifiée
  nom, prénom, adresse email….

ou

- Une personne physique identifiable
- Données localisation, matricule, identifiant
- Éléments propres à son identité physiologique, culturelle, sociale…

(Art. 4. 1)

Catégories particulières de données à caractère personnel

Origine raciale ou ethnique

Opinions politiques

Convictions religieuses ou philosophiques, appartenance syndicale

Données génétiques

Réf: art 9

Catégories particulières de données à caractère personnel

Données biométriques aux fins d'identifier une personne physique de manière unique

Données concernant la santé

Données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

Réf: art 9

Donnée à caractère personnel – Exemple

Données collectées lors de l'achat d'un billet d'avion (en ligne)

- Nom, adresse, numéro de téléphone, courriel
- Numéro de passeport / carte d'identité
- Carte de crédit
- Allées et venues (pays visité(s), durée du séjour, autre(s) personne(s), etc.)
- Adresse IP (dynamique ou non)
- Cookies

Données cat. particulières

- Allergies
- Maladie
- Besoins particuliers (chaise roulante, handicap, etc.)

Traitement de données

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel.

Collecte, organisation, utilisation, communication, conservation, extraction, rapprochement, diffusion, enregistrement, destruction…

Réf: art 4. 2

Agenda

1 **Introduction RGPD**

2 **Impacts du RGPD pour les sociétés canadiennes**

3 **Se préparer au RGPD**

Sociétés canadiennes – *Impacts*

Est-ce que le RGPD s'applique à vous? Quelques questions, notamment:

- Est-ce que vous faites de la promotion de vos services à des citoyens de l'UE?
- Avez-vous des employés dans l'UE?
- Est-ce que vous collectez / recevez des données de citoyens Européen?
- Est-ce que votre organisation agit pour le compte d'une organisation européenne ?

Sociétés canadiennes – *Impacts*

En tant que responsable de traitement :

- Sujet à toutes les exigences du RGPD comme toute société établie dans l'UE
- Pas de présence physique nécessaire
- Acte juridique entre co-responsables de traitement

En tant que sous-traitant :

- Sujet à toutes les exigences du RGPD comme toute société agissant en tant que sous-traitant pour le compte d'un responsable de traitement soumis au RGPD
- Contrat écrit obligatoire avec le responsable de traitement

Sociétés canadiennes – *Impacts*

Transfert de données hors UE autorisé sous conditions

- Décision d'adéquation (privacy shield, …)
- Règles d'entreprise contraignantes
- Garanties appropriées :
  - Clauses modèles édictées par la commission européenne
  - Code de conduite &, certification
  - Consentement de la personne concernée
  - Autorisation autorité de contrôle

Réf: art. 44-49

Sociétés canadiennes – *Impacts*

Nomination requise d'un représentant en l'absence de présence au sein de l'UE:

- Dans **un** des pays membre de l'UE dans lesquels résident les personnes concernées
- Par mandat écrit est la personne qui est le point de contact des autorités de contrôle et personnes concernées concernant le traitement réalisé
- La responsabilité reste dans le chef de l'organisation responsable de traitement ou sous-traitant qui l'a désigné

Réf: art. 27

Sociétés canadiennes – *Impacts*

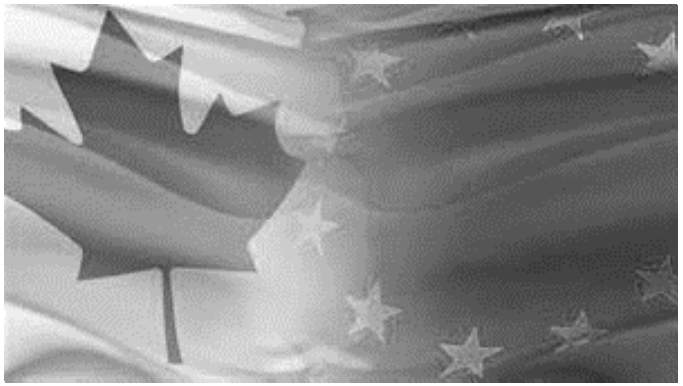
Le RGPD ne s'applique pas à votre organisation/société ?

- Bonnes pratiques à mettre en œuvre dans tous les cas pour pallier aux Lois actuelles (Québec et Canada)
- Permet d'anticiper les changements législatifs à venir (RGPD servira de base pour plusieurs pays)

- **Avantages**
  - Approche basée sur les risques, DPIA et PbD ne sont pas des notions nouvelles
  - Longueur d'avance – plus de temps pour vous préparer
  - Facilite en cas de développement de vos activités / services au marché Européen

Agenda

1 Introduction RGPD



2 Impacts du RGPD pour les sociétés canadiennes

3 Exigences du RGPD

Exigences du RGPD - *Droits des personnes*

Droit d'accès *(art. 15)*	Obtention confirmation et information des données traitées, ou qu'elles ne sont pas traitées
Droit de rectification *(art. 16)*	Rectification des données inexactes ou ajout d'informations pour des données complètes
Droit à l'effacement *(art. 17)*	Suppression des données plus nécessaires, retrait consentement, traitement illicite
Droit de limitation *(art. 18)*	Contestation exactitude, traitement illicite, conservation à des fins de défense des droits en justice
Droit à la portabilité *(art. 20)*	Réception données fournies dans 1 format structuré et lisible par machine pour transmission
Droit d'opposition *(art. 21)*	Opposition aux traitements fondés sur intérêt légitime et mission d'intérêt public, prospection
Décision automatisée *(art. 22)*	Droit de ne pas faire l'objet d'une décision fondée exclusivement sur traitement automatisé

Exigences du RGPD – *Le délégué à la protection des données*

DPO

Obligatoire pour responsable et sous-traitants dans 3 cas dont :

- Suivi régulier et systématique à grande échelle
- Traitement de données sensibles à grande échelle

- Indépendant
  Absence de conflit d'intérêt
- Rattaché à la direction
  Position transversale
- Contrôle de la conformité
- Point de contact pour les individus et l'autorité de contrôle
- Informer et conseiller sur les obligations

Réf: art. 37 à 39

Exigences du RGPD – *Notification des violations 1/2*

Qui	Auprès de	Délais à compter de la prise de connaissance
Responsable de traitement	Autorité de contrôle (Ex: CNPD au Luxembourg)	72 heures
Responsable de traitement	Personnes concernées	Dans les meilleurs délais
Sous-traitant	Responsable de traitement	Dans les meilleurs délais

Dérogation: lorsque la violation n'engendre pas de risque, ou risque élevé sur les droits et libertés de la personne au regard des mesures de sécurité prises.

Réf: art. 33 et 34

Exigences du RGPD – *Notification des violations 2/2*

Qui	Auprès de	Contenu
Responsable de traitement	Autorité de contrôle (CNPD)	• Nature de la violation • Identification DPO, point de contact • Conséquences probables • Mesures de remédiation
Responsable de traitement	Personnes concernées	• Nature de la violation • Identification DPO, point de contact • Conséquences probables • Mesures de remédiation
Sous-traitant	Responsable de traitement	• Nature de la violation • Identification point de contact

Réf: art. 33 et 34

Exigences du RGPD – *Data protection by design*

Prendre en compte les principes de la protection des données dès les 1ères phases d'un projet

Assurer la sécurité des données tout au long de leur cycle de vie, et de celui de l'organisation

Mettre en œuvre la **pseudonymisation et chiffrement des données**

Limiter techniquement par défaut **la collecte des données**

Faciliter l'exercice des droits de **l'utilisateur de l'application par des fonctionnalités** en ligne

Réf: art. 25

Exigences du RGPD - *Analyse d'Impact relative à la Protection des Données*

Objectif: Identifier et traiter les risques

- Sur les droits et libertés des personnes physiques
- Engendrés par les opérations de traitement de données

Obligation: Tous traitements susceptibles d'engendrer un risque élevé pour les personnes, dont

- Évaluation d'aspects personnels à grande échelle pour la prise de décision (ex : profilage)
- Traitement de catégories particulières de données à grande échelle (ex : biométrie)
- Surveillance systématique à grande échelle de zone publique

Réf: art. 35

Exigences du RGPD – *La sécurité des données*

Mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque pour protéger contre:

- Le traitement illicite ou non autorisé
- La divulgation
- La perte, la destruction ou dégâts accidentels

Intégrité et confidentialité & disponibilité

Atteinte à la personne possible suite à une divulgation des données mais aussi à la non-disponibilité de la donnée ou son défaut d'intégrité

Codes de conduite
Certification

Réf: art. 32

Exigences du RGPD – *Contrats de sous-traitance*

- Le sous-traitant doit apporter les garanties de respect du GDPR avant la contractualisation (due diligence)
- Le sous-traitant doit tenir un registre des traitements qu'il réalise pour le compte du responsable
- Vérifier l'existence d'un contrat incluant notamment :
  - La description du traitement de données concerné, les catégories de données à caractère personnel et des personnes concernées
  - Les engagements relatifs à l'obligation de mise en place des mesures de sécurité appropriées, de notification d'incident, d'assistance, de confidentialité et suppression des données
  - L'engagement de sous-traitant ultérieur uniquement sur autorisation du responsable

Réf: art. 28

MGSI - Accompagner la mise en conformité au RGPD

- **Une équipe d'experts de 7 personnes dont:**
  - 3 juristes en protection des données
  - 2 experts sécurité de l'information (IT, ISO 27001, 27005)

- Clients et activités:
  - POST Group, POST Telecom
  - Ministère
  - Editus Luxembourg
  - Formation, événements, conférences


MGSI
DPO
GAP ANALYSIS
AUDIT
DPIA
PRIVACY BY DESIGN/ DEFAULT
TRAINING

Accompagner la mise en conformité au RGPD

Nos services

MGSI est la première société au Luxembourg ayant obtenu la qualité d'experte « légal » et « technique » pour l'évaluation des produits et services IT au regard du RGPD des fournisseurs cherchant à obtenir la certification Europrise.

www.european-privacy-seal.eu

Merci pour votre attention

Mélanie Gagnon, CIPM, CISA
CEO & Founder
MGSI sàrl
Melanie.gagnon@mgsi.lu

www.mgsi.lu
www.dataprotection.lu