La conformité au RGPD

Par Valérie Chavanne
Avocate & lobbyiste dans les secteurs des médias et des nouvelles technologies

LegalUP Consulting

iab canada

AGENDA

- Qu'est-ce que le RGPD / GDPR ?
- Les objectifs du RGPD
- À noter: une explosion des sanctions
- Un nouveau périmètre d'application
- Une définition clé: « le traitement de données »
- Un renforcement du droit des personnes
- Les Bases légales du traitement de données à caractère personnel
- Les grands principes relatifs au traitement de données à caractère personnel
- Des contraintes nouvelles pour les entreprises : la documentation
- Des outils pour responsabiliser les entreprises
- Des contraintes nouvelles sur les failles de sécurité
- L'établissement d'une gouvernance en continue par la désignation d'un DPO
- Les principales missions du DPO
- La question des transferts hors de l'UE
- Conformité : quels reflexes adopter ?
- Les principaux outils à développer

LegalUP Consulting iab.canada

Qu’est-ce que le RGPD / GDPR?

RGPD (Règlement Général sur la Protection des Données en français) ou GDPR (de l’anglais General Data Protection Regulation) ?

Le RGPD est le nouveau cadre légal européen concernant la confidentialité et la protection des données. La protection des données recouvre les systèmes, politiques et procédures utilisés par les entreprises aux fins de garantir la sécurité des données personnelles qu’elles traitent et de protéger la vie privée des personnes concernées.

Le RGPD est applicable à tous les secteurs d’activité, et ce, quelle que soit la taille de l’entreprise.

Les objectifs du RGPD

- Mettre fin aux divergences d'interprétation au sein de l'EU ;
- Renforcer les droits des personnes sur les traitements des données les concernant
- Renforcer la responsabilisation des entreprises (l'Accountability)

MAIS PAS DE REMISE EN CAUSE DU BUSINESS MODELE DE NOTRE INDUSTRIE

Les principaux **axes de travail** :

- Établir une gouvernance de la gestion des données personnelles ;
- Assurer la conformité aux exigences nouvelles du RGPD.

A noter: une explosion des sanctions

L'une des conséquences, en cas de défaut de conformité au RGPD pour les entreprises, est de se voir infliger une amende pouvant s'élever à un montant équivalent à **4% du chiffre d'affaires annuel mondial total de l'entreprise ou d'un maximum de 20 millions**; sans compter les dommages collatéraux comme l'atteinte à l'image de marque, la perte potentielle de chiffre d'affaires et de capitalisation boursière, etc.

Un nouveau périmètre d'application

- Avec de **nouvelles définitions** (les données personnelles englobent pseudonymes).
- Un **périmètre territorial large** (toute entité, implantée ou pas au sein de l'UE traitant des données personnelles de résidents européens) doit se mettre en conformité. Il existe une carte qui affiche le niveau de protection requis par les européens. https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde.

Le Canada est considéré comme un pays disposition d'un niveau d'adéquation partielle. Cela ne signifie pas qu'il faut stopper tout transfert mais les encadrer.

- **Des bases légales** relatives au traitement des données personnelles clarifiées.

Une définition clé « le traitement de données »

Le traitement de données à caractère personnels(art. 4 du RGPD):

« *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, telles que* ***la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, effacement ou la destruction*** ».

Un renforcement du droit des personnes

Deux mots d'ordre : TRANSPARENCE et CONTRÔLE

- **Un droit à l'information, précisé et élargi** : … sur l'identité et les coordonnées du responsable de traitement, les finalités du traitement, la durée de conservation des données à caractère personne, les destinataires et les transferts de données à caractère personnel hors de l'UE
- **Un droit à l'oubli consacré**
- **Un droit à la portabilité**

Les Bases légales du traitement de données à caractère personnel:

- Le **consentement** de la personne concernée pour une ou plusieurs finalités spécifiques;
- Le traitement est **nécessaire aux fins des intérêts légitimes** poursuivis par le responsable de traitement ou par un tiers;
- Le traitement est **nécessaire à l'exécution d'un contrat** auquel la personne concernée est partie;
- Le traitement est nécessaire au **respect d'une obligation légale** pesant sur le responsable de traitement;
- Le traitement est nécessaire à **l'exécution d'une mission d'intérêt public** ou relevant de l'exercice de l'autorité publique;
- Le traitement est nécessaire à la **sauvegarde des intérêts vitaux de la personne** concernée ou d'une autre personne physique.

LegalUP Consulting iab.canada

Les grands principes relatifs au traitement de données à caractère personnel

- La **minimisation** du traitement des données collectées;
- La **Licéité**, la **loyauté** et la **transparence** du traitement;
- La **finalité** du traitement;
- La **mise à jour;**
- La **durée de conservation** des données.

Des contraintes nouvelles pour les entreprises : la documentation

La fin des « déclarations » MAIS…. Une obligation d'établir et de tenir à jour un **REGISTRE DES ACTIVITÉS DE TRAITEMENT**

Le Registre des activités de Traitement est prévu à l'article 30 du RGPD. Il s'agit d'un document de recensement et d'analyse reflétant la réalité des Traitements et permettant d'identifier les parties prenantes et les principales informations pour chaque catégorie de Données à caractère personnel (finalités, durée de conservation, mesure de sécurité etc).

Des outils pour responsabiliser les entreprises

Il s'agit d'un ensemble de processus nécessaires à assurer une protection optimale des données à caractère personnel.

Les mesures techniques et organisationnelles sont nombreuses et pèsent sur le Responsable de traitement comme sur le Sous-traitant ayant comme objectif le renforcement de la responsabilisation (l'Accountability en anglais) des entreprises.

Il s'agit principalement de :

- "**Privacy by design** c'est à dire dès la conception de vos produits et services.
- "**Privacy by default**" c'est à dire par défaut.
- La réalisation d'Analyse d'impact relative à la protection des données (**PIA**, Privacy Impact Assessment en anglais).

LegalUP Consulting iab.canada

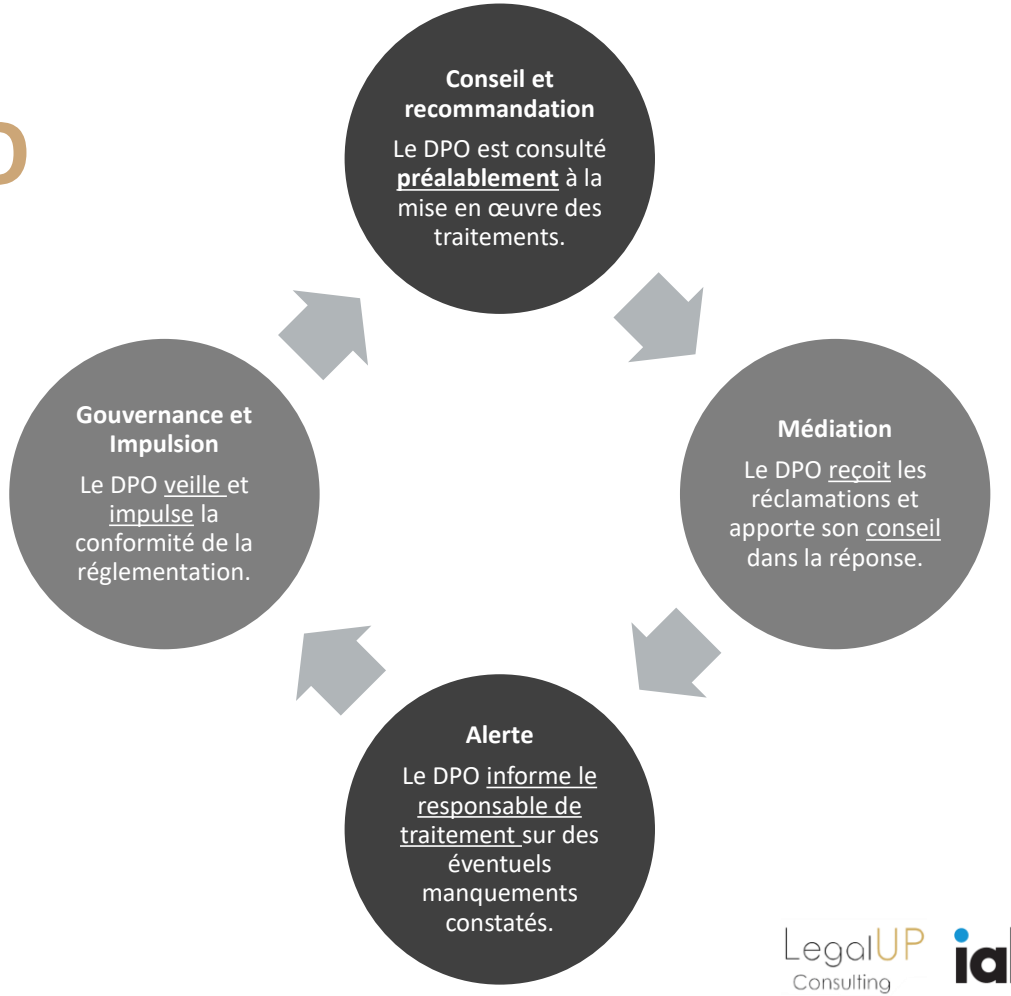
Des contraintes nouvelles sur les failles de sécurité

- La notification des « failles de sécurité » étendue à toutes les organisations dans un délai de 72 heures à l'autorité de contrôle compétente pour le responsible de traitement.
- Une notification aux personnes concernées est également visée

L’établissement d’une gouvernance en continue par la désignation d’un DPO

- Nomination d’un DPO « Data Protection Officer »
    - Elle est obligatoire lorsque : « *Les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un* ***suivi régulier et systématique à grande échelle des personnes concernées*** » (Article 37 du RGPD)
    - Le DPO peut être interne ou externalisé

Les principales missions du DPO



LegalUP Consulting

iab.canada

La question des transferts hors de l'UE

En quoi consiste un transfert de données hors UE ?

- Ce n'est pas uniquement un déplacement de données d'un point A situé à un point B situé hors de l'UE .
- L'accès distant par un destinataire situé hors de l'UE à des données stockées sur le territoire de l'UE est également.
- Les transferts de données ne sont possibles que sous réserve du respect de certaines conditions strictement encadrées comme par des BCR (Binding Corporate Rules ou des Codes de conduite validé par les autorité de contrôle EU.

Conformité : quels reflexes adopter ?

- **Inciter les équipes à travailler en « mode projet » :**
  - Autodiagnostic sur les risques associés à chaque projet (via une « check-list »)
  - Réflexe de consultation quasi-systématique du DPO.
- **Élargir la culture de la sécurité :**
  - Assurer une bonne compréhension de ces enjeux auprès des collaborateurs, notamment en contact avec les clients/ partenaires
  - Mettre en place des mécanismes et processus de gestion de crise.

LegalUP Consulting iab.canada

Les principaux outils à développer

- La désignation d'un **DPO** et la **Formation** de vos effectifs et de vos cocontractants;
- Le renforcement des mesures assortissants la désignation d'un sous-traitant;
- La mise en place de **Fiche d'inventaires** des traitements pour chaque nouveau produit/service;
- La tenue d'un **Registre des activités de Traitement** (document de recensement et d'analyse reflétant la réalité des Traitements et permettant d'identifier les parties prenantes et les principales informations pour chaque catégorie de Données à caractère personnel (finalités, durée de conservation, mesures de sécurité, etc).
- Le respect des règles d'or de **l'Accountability** (Privacy by design et by default, PIA pour les traitements les plus risqués ou même en case de simple doute);
- L'encadrement des **transferts** de données personnelles vers l'UE;
- **L'engagement dans les Bonnes pratiques comme celles portées par l'IAB.**

LegalUP Consulting iab.canada

Merci pour votre attention

Valérie Chavanne

LegalUP consulting

www.legalupconsulting.com