

# FEUILLE-INFO

## SUR LA PROTECTION DE LA VIE PRIVÉE

# Règlement général sur la protection des données

## APERÇU

Le Règlement général sur la protection des données (RGPD) de l'Union européenne (UE) est entré en vigueur le 25 mai 2018. Ce règlement relatif à la protection de la vie privée vise à donner aux particuliers de l'UE le pouvoir de contrôler la façon dont les données qui les concernent sont traitées et utilisées.

Bien que le RGPD soit un règlement de l'UE, il peut s'appliquer aux institutions publiques et aux dépositaires de renseignements sur la santé de l'Ontario dans certaines circonstances limitées. Le Commissaire à l'information et à la protection de la vie privée n'est pas responsable de l'application ni de la surveillance du RGPD.

La présente feuille-info donne aux institutions et aux dépositaires de renseignements sur la santé de l'Ontario des renseignements généraux sur l'application possible de ce règlement et de certaines de ses exigences. Celles-ci peuvent être plus contraignantes que les règles énoncées dans la *Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP)*, la *Loi sur l'accès à l'information municipale et la protection de la vie privée (LAIMPVP)* et la *Loi sur la protection des renseignements personnels sur la santé (LPRPS)*.

La présente feuille-info ne constitue pas une interprétation juridique des dispositions du RGPD pas plus qu'elle ne vise à donner des conseils juridiques sur son application en Ontario. Les organismes qui souhaitent obtenir des conseils devraient consulter leur avocat. La portée du règlement et l'interprétation de ses exigences dépendent de décisions et d'avis futurs des tribunaux et des autorités de protection des données de l'UE.



Information and Privacy  
Commissioner of Ontario

Commissaire à l'information et à la  
protection de la vie privée de l'Ontario

## TERMINOLOGIE

Le RGPD s'applique au traitement des **données à caractère personnel** (les renseignements personnels) que le règlement définit comme « toute information se rapportant à une personne physique identifiée ou identifiable » qui est appelée **personne concernée**. Les données à caractère personnel comprennent les adresses IP, les adresses de courriel et les numéros de téléphone.

Le **traitement** s'entend de toute opération appliquée à des données à caractère personnel, telle que la collecte, l'utilisation, le stockage et la divulgation. Les **responsables du traitement** désignent les organismes chargés de déterminer les finalités et les moyens du traitement, c'est-à-dire pourquoi et comment ils entendent recueillir et utiliser les données à caractère personnel. Les organismes qui traitent des données à caractère personnel pour le compte d'un responsable du traitement sont appelés les **sous-traitants**. Si ces termes étaient utilisés en Ontario, les institutions ou les dépositaires de renseignements seraient les responsables du traitement. Si une institution ou un dépositaire de renseignements décidait d'externaliser des activités, comme le stockage des données, pour les confier à un tiers, ce dernier serait le sous-traitant.

Les organismes de réglementation qui surveillent l'application du RGPD dans les États membres sont appelés **autorités de contrôle** ou, plus communément, **autorités de protection des données**.

## APPLICATION DU RGPD

Le RGPD s'applique au traitement des données à caractère personnel effectué par un responsable du traitement ou un sous-traitant établi sur le territoire de l'UE, même si le traitement se fait à l'extérieur de l'UE. Il s'applique également au traitement des données à caractère personnel par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'UE, si le traitement est lié :

- à l'offre de biens ou de services à des personnes dans l'Union;
- au suivi du comportement de ces personnes.

Le simple fait d'avoir un site Web auquel des personnes de l'UE peuvent accéder n'est pas suffisant pour qu'un organisme soit assujéti au RGPD. Cependant, la présence de facteurs supplémentaires, comme l'utilisation d'une langue ou d'une devise utilisée dans l'UE ou la simple mention de clients de l'UE, peut démontrer une intention d'offrir des biens ou des services à des personnes de l'UE.

Bien que la majorité des activités des institutions et des dépositaires de renseignements de l'Ontario ne soient pas assujétiées au RGPD, le règlement peut s'appliquer à certaines activités. Par exemple, les collèges et les universités de l'Ontario qui recrutent activement des étudiants étrangers de l'UE **peuvent** être assujétiés au RGPD en ce qui concerne le traitement des données à caractère personnel de ces étudiants dans l'UE.

Les organismes assujettis au règlement qui ne s'y conforment pas sont passibles de lourdes amendes.

## PRINCIPALES DISPOSITIONS DU RGPD

La section qui suit présente une brève description de quelques dispositions clés du RGPD. Il ne s'agit pas d'un guide exhaustif, mais plutôt de points saillants concernant certaines dispositions importantes du RGPD, qui peuvent différer des dispositions de la *LAIPVP*, de la *LAIMPVP* et de la *LPRPS*, ou être plus contraignantes que celles-ci. Veuillez noter que des dispositions peuvent comporter des exceptions qui ne sont pas abordées dans le présent document d'information.

### Traitement licite des données à caractère personnel

Le règlement énonce les circonstances dans lesquelles les données à caractère personnel peuvent être légalement traitées (traitement licite). En voici quelques exemples :

Les données à caractère personnel peuvent être traitées si la personne concernée a donné son consentement. Le consentement doit être donné de façon libre, spécifique, éclairée et univoque. Il doit être explicite et présenté séparément de toute autre information. Cela signifie que la demande de consentement ne doit pas se trouver dans les conditions générales d'utilisation d'un service. La personne concernée doit également avoir le droit de retirer son consentement en tout temps.

Les données à caractère personnel peuvent être traitées lorsqu'il est nécessaire de le faire en raison des intérêts légitimes du responsable du traitement pourvu que le traitement ne porte pas préjudice aux libertés et droits fondamentaux de la personne concernée. Cela s'applique aux situations où la personne concernée pourrait raisonnablement s'attendre à ce que le traitement se produise. Par exemple, une personne de l'UE qui présenterait une demande d'admission à une université ou à un collège de l'Ontario pourrait raisonnablement s'attendre à ce que l'institution lui demande des données à caractère personnel pour traiter sa demande.

Les données à caractère personnel peuvent également être traitées si le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

### Catégories spéciales de données à caractère personnel

La façon et le moment de traiter les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques ou biométriques, les données concernant la santé, ou encore les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne font l'objet de restrictions accrues.

## Avis de collecte

Le RGPD exige que les personnes concernées soient avisées avant que des données à caractère personnel les concernant ne soient recueillies. Le responsable du traitement doit leur fournir les renseignements suivants :

- l'identité et les coordonnées du responsable du traitement
- les fins visées par le traitement
- la base juridique du traitement
- les destinataires des données
- la durée de conservation des données

Les personnes concernées doivent également être informées des droits que leur donne le RGPD, qui sont examinés plus en détail ci-dessous. Un avis semblable doit être donné lorsque le responsable du traitement reçoit des données à caractère personnel d'une source autre que la personne concernée, sauf en cas d'exception.

## Analyse d'impact relative à la protection des données

Une analyse d'impact relative à la protection des données, qu'on appelle « évaluation de l'incidence sur la vie privée » en Ontario, est requise lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne concernée. Le RGPD contient des exemples d'activités à risque élevé. Le responsable du traitement doit procéder à l'analyse d'impact relative à la protection des données avant que le traitement ne débute.

## Communication obligatoire d'une violation de données à caractère personnel

Les responsables du traitement sont tenus d'aviser l'**autorité de protection des données** d'une violation de données à caractère confidentiel (atteinte à la vie privée) dans les meilleurs délais, ou au plus tard 72 heures après en avoir pris connaissance. Un tel avis est requis sauf s'il est peu probable que la violation engendre un risque pour les droits et libertés de la personne concernée.

Le responsable du traitement doit communiquer une violation de données à caractère personnel à la **personne concernée** dans les meilleurs délais lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne.

## Droits des particuliers

**Droit d'être informés** : Comme nous l'avons mentionné précédemment, les particuliers ont le droit d'être informés de la façon dont un responsable du traitement traitera les données à caractère personnel qui les concernent.

**Droit d'accès et de rectification** : En général, les particuliers ont le droit de demander une copie des données à caractère personnel qu'elles ont

fournies à un responsable du traitement et la rectification de ces données.

**Droit à la portabilité des données** : Les particuliers ont le droit de recevoir les données dans un format structuré, couramment utilisé et lisible par machine.

**Droit d'opposition au traitement** : Dans certaines circonstances, les particuliers ont le droit de s'opposer au traitement des données à caractère personnel qui les concernent, par exemple, lorsque les données sont traitées à des fins de marketing.

**Droit à la limitation du traitement** : Les particuliers ont le droit d'obtenir la limitation du traitement de données à caractère personnel qui les concernent dans des situations précises, par exemple, lorsque la personne conteste l'exactitude des données ou qu'elle s'oppose au traitement des données qui la concernent et attend une décision.

**Droit de porter plainte** : Les particuliers ont le droit de porter plainte à l'autorité de protection des données si elles croient que le traitement des données qui les concernent viole le RGPD.

**Droit à l'effacement** : En vertu du RGPD, les particuliers ont le droit de demander que les données à caractère personnel les concernant soient effacées. Ce droit, parfois appelé **droit à l'oubli**, s'applique dans certaines circonstances, par exemple, lorsque les données ne sont plus nécessaires pour les fins auxquelles elles avaient été recueillies ou traitées. Les particuliers ont également le droit de demander que les données à caractère personnel les concernant soient supprimées ou déréférencées d'un moteur de recherche.

Il existe des exceptions à ce droit. C'est le cas notamment lorsque le traitement des données à caractère personnel est nécessaire à l'exercice du droit à la liberté d'expression, pour respecter une obligation légale, à l'exercice ou à la défense de droits en justice ou encore pour des motifs d'intérêt public dans le domaine de la santé publique.

## RESSOURCES SUPPLÉMENTAIRES

- **Règlement général sur la protection des données de l'UE**
- Groupe de travail « Article 29 » : **EU General Data Protection Regulation: General Information Document**
- Commission européenne : **Réforme des règles de l'UE en matière de protection des données 2018**
- Information Commissioner's Office of the United Kingdom : **Guide to the General Data Protection Regulation**
- Office of the Information and Privacy Commissioner of British Columbia : **Competitive Advantage: Compliance with PIPA and the GDPR**
- Information and Privacy Commissioner of New South Wales : **NSW Public Sector Agencies and the GDPR**