COMPRENDRE LE RGPD

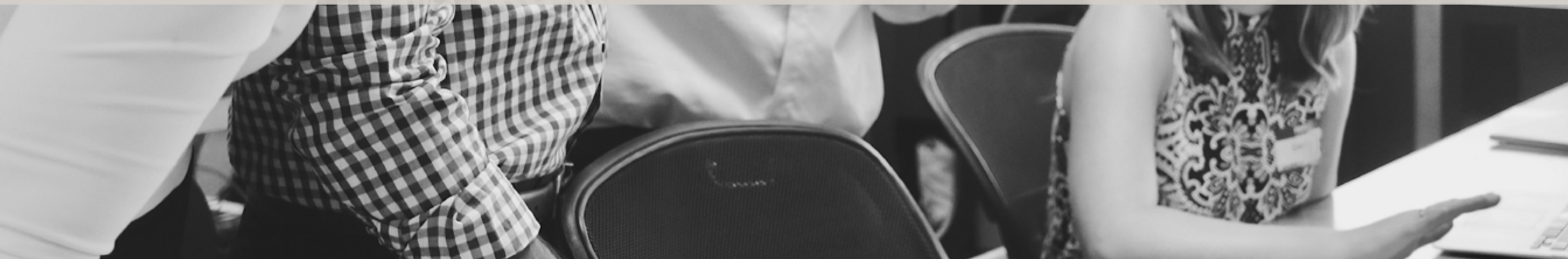
Le rôle des normes dans la conformité

Conseil canadien des normes

Un monde de possibilités à votre portée.

Canada

Le Conseil canadien des normes tient à remercier les membres du Comité consultatif canadien sur le RGPD (CCC RGPD) pour leur expertise et leur contribution au présent document.



OBJET DU DOCUMENT

Le Conseil canadien des normes (CCN) a produit ce document d'orientation pour faire connaître le Règlement général sur la protection des données (RGPD) aux organisations canadiennes et pour recommander à ces dernières des stratégies de normalisation qui en facilitent le respect. Ce règlement mis en place par l'Union européenne (UE) a des répercussions sur le reste du monde, et peut avoir des implications majeures pour les organisations canadiennes.

C'est pourquoi ce document explique l'utilité de la normalisation pour assurer la conformité au RGPD, et fournit de l'information qui aidera dans cette démarche ainsi que dans l'utilisation des normes pertinentes. Il faut toutefois noter que le RGPD est un instrument juridique complexe, et qu'il ne suffit pas de se plier à des normes pour en respecter toutes les dispositions.

CONTENU DU PRÉSENT DOCUMENT :

- Interprétation des principaux articles du RGPD
- Exemples d'application du RGPD
- Exemples de secteurs touchés par le RGPD
- Normes utiles pour comprendre ou respecter le RGPD
- Liste de mesures recommandées
- Annexe contenant un tableau de synthèse pouvant servir d'outil de référence rapide résumant le RGPD

NOTE 1 : Ce document d'orientation s'adresse aux organisations, mais peut aussi être consulté à titre informatif par les membres du grand public.

NOTE 2 : Le texte de ce document se fonde sur celui du RGPD. D'autres interprétations sont possibles.

NOTE 3 : La mise en application et le respect du RGPD peuvent être encadrés par des lois locales et diverses autorités de protection des données.

NOTE 4 : L'adoption de toute norme en particulier n'est pas obligatoire pour le respect du RGPD, mais est généralement préférable.

QU'EST-CE QUE LE RGPD?

En vigueur depuis le 25 mai 2018, le RGPD harmonise les lois sur la protection des données dans l'ensemble de l'UE, où les autorités de protection des données (APD) des États membres veillent à son respect. Le RGPD s'applique à toutes les organisations sur le territoire de l'UE ainsi qu'à toutes celles – où qu'elles soient – qui traitent ou stockent des données à caractère personnel relatives à des personnes concernées résidant dans l'UE. Les organisations canadiennes doivent adhérer au RGPD si elles proposent des biens ou des services à ces personnes ou font un suivi de leur comportement. Qui plus est, si une organisation canadienne traite ou transfère des données à caractère personnel relatives à une personne (quelle que soit sa nationalité, même s'il s'agit d'un citoyen canadien) alors que celle-ci est sur le territoire de l'UE, elle pourrait aussi avoir à se plier au règlement, sous peine de lourdes amendes.

En vertu du RGPD, la Commission européenne est tenue de surveiller les lois sur la protection des données des pays hors UE, dont le Canada, et c'est seulement si elle juge leur protection adéquate que les données à caractère personnel peuvent être transmises vers ces pays sans mesures additionnelles. Le gouvernement du Canada rend régulièrement compte à la Commission européenne pour maintenir le statut d'adéquation. Depuis l'arrêt de juillet 2020 de la Cour de justice de l'Union européenne (CJUE), toute entreprise de l'UE entendant transmettre des données à caractère personnel à un importateur de données en dehors de l'UE doit d'abord vérifier si le régime juridique du pays concerné ne compromet pas la capacité de l'importateur à protéger adéquatement ces données. Le message de la CJUE est clair : il ne peut y avoir libre circulation des données à caractère personnel que si le pays du destinataire est doté de mécanismes adéquats protégeant les droits des citoyens de l'UE sur leurs données; sinon, il est interdit aux organisations de l'UE de permettre l'accès aux données. C'est donc dire que les responsables du traitement des données dans l'UE doivent voir si les renseignements personnels à transmettre hors de l'UE seront suffisamment protégés dans le pays de destination.

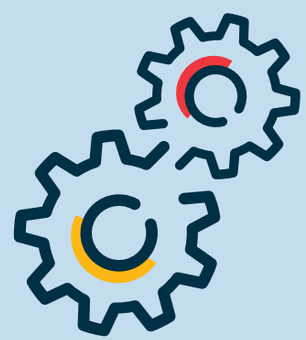
QU'EST-CE QU'UNE NORME?

Les normes sont des spécifications écrites. Appliquées systématiquement, elles encadrent la fiabilité de matériaux, de produits, de processus et de services courants pour assurer qu'ils sont appropriés à leur objet. Elles sont établies par consensus et approuvées par un organisme reconnu, comme le CCN. Les normes reposent sur l'expertise d'un groupe de spécialistes et visent à optimiser les avantages pour la société. Bref, elles établissent une référence pour la conception et le développement d'innovations, et favorisent la conformité aux réglementations nationales et internationales. De plus, les normes publiées peuvent s'accompagner de programmes de certification et d'accréditation qui facilitent l'accès aux marchés étrangers et la conformité réglementaire.

En quoi les normes sont-elles utiles pour la conformité au RGPD?
En général, les normes sont revues régulièrement de façon à suivre les avancées technologiques, ce qui permet aux organisations d'adapter leurs mesures de conformité. En proposant lignes directrices, méthodes et procédures à suivre pour répondre aux exigences du RGPD, la normalisation facilite la conformité des organisations canadiennes au Règlement. Une multitude de normes volontaires est continuellement en cours d'élaboration pour améliorer les pratiques exemplaires en matière de confidentialité des données, de cybersécurité, de protection de l'information et des technologies, etc. Bien qu'elles ne soient pas directement référencées dans le RGPD, ces normes sont un repère stable pour les organisations canadiennes qui doivent se conformer au Règlement.

LE CONSEIL CANADIEN DES NORMES

Constitué en 1970 en tant que société d'État fédérale, le Conseil canadien des normes (CCN) est le chef de file canadien de la normalisation et de l'accréditation sur la scène nationale et internationale. Il collabore étroitement avec un vaste réseau de partenaires pour promouvoir l'élaboration de normes efficaces et efficientes qui protègent la santé, la sécurité et le bien-être de la population canadienne tout en aidant les entreprises à prospérer. Organisme d'accréditation principal au Canada, le CCN renforce la confiance du marché au pays et à l'étranger en veillant à ce que les organismes d'évaluation de la conformité respectent les normes nationales et internationales les plus strictes. Membre de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (IEC), il défend les intérêts du Canada sur la scène internationale et relie des milliers de personnes aux ressources et aux réseaux du monde entier, mettant ainsi à la portée de la population et des entreprises du pays un monde de possibilités.



Pour en savoir plus, consulter le site https://www.ccn.ca

TERMES CLÉS DU RGPD

CHAMP D'APPLICATION TERRITORIAL

Le RGPD concerne les données à caractère personnel des résidents de l'UE traitées et stockées à l'intérieur comme à l'extérieur de l'UE. Il s'applique aux organisations qui : a) ont une présence physique dans l'UE, b) mènent des activités de traitement de données se rapportant à l'offre de biens ou de services aux résidents de l'UE, ou c) surveillent les actions des résidents de l'UE qui se trouvent sur le territoire de l'UE (ex. : surveillance de leur activité sur Internet à des fins publicitaires). Le RGPD s'applique aussi à toutes les organisations hors de l'UE qui traitent des données à caractère personnel se rapportant aux résidents de l'UE, où qu'elles soient.

(RGPD : article 3; considérants 22, 23, 24, 25)

PERSONNE CONCERNÉE

Personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, des données de localisation, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Autrement dit, la personne concernée est un être humain au sujet duquel et auprès duquel une organisation obtient de l'information à caractère personnel.

(RGPD : article 4; considérants 15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37)

DONNÉES À CARACTÈRE PERSONNEL

Aussi appelées « renseignements personnels », « renseignements nominatifs » ou « renseignements permettant d'identifier une personne », les données à caractère personnel constituent toute information qui se rapporte à une personne donnée. Cette information peut avoir été obtenue de la personne en question, ou encore avoir été générée lors de l'utilisation ou du traitement d'autres renseignements la concernant.

(RGPD : article 4; considérants 15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37)

RESPONSABLE DU TRAITEMENT DES DONNÉES

Organisation qui décide quelles données seront recueillies, traitées et stockées, et qui répond des méthodes employées pour la collecte, le traitement et le stockage des données ainsi que de l'accessibilité, de la sécurité et de la conservation des données. Elle est également responsable des décisions concernant la sollicitation des tiers (sous-traitants des données).

(RGPD : article 4; considérants 15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37)

TRAITEMENT DES DONNÉES

Toute opération appliquée à des données ou des ensembles de données à caractère personnel, telles que la manipulation, la catégorisation ou l'utilisation dans des opérations mathématiques.

(RGPD : article 4; considérants 15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37)

SOUS-TRAITANT DES DONNÉES

Personne ou organisation qui traite des données à caractère personnel sur instruction du responsable du traitement. Le sous-traitant des données n'est pas propriétaire des données ni ne contrôle les finalités du traitement. Il est possible pour une organisation d'être à la fois responsable du traitement des données et sous-traitant des données.

(RGPD : article 4; considérants 15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37)

DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Le délégué à la protection des données veille au respect des lois sur la protection de la vie privée en vigueur au sein d'une organisation. Il doit pouvoir exercer ses fonctions sans ingérences, et faire rapport à la plus haute autorité de l'organisation. Il est aussi le point de contact pour les APD, avec lesquelles il collabore en tant que de besoin. Enfin, il est la personne-ressource pour tout ce qui touche la protection de la vie privée; il assure des actions de formation adéquates; et il évalue et communique les risques.

(RGPD : articles 37, 38, 39; considérant 97)

GRANDS PRINCIPES DU RGPD

TRAITEMENT ET RESPONSABILITÉ

Les données recueillies doivent être limitées à ce qui est nécessaire, se rapporter clairement à la personne concernée, et être traitées avec les précautions et la confidentialité que demande leur degré de sensibilité.

(RGPD : article 5; considérant 39)

LICÉITÉ

Le traitement des données est considéré comme licite s'il est effectué avec le consentement de la personne à qui ces données se rapportent, s'il est nécessaire au fonctionnement de l'organisation qui les recueille, ou s'il est justifié par un motif légal valide.

(RGPD : article 6; considérants 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 171)

CONSENTEMENT

Le cas échéant, les données à caractère personnel ne peuvent être recueillies, traitées ou communiquées que si la personne concernée a donné son consentement, et ce, en termes clairs, de plein gré et de manière éclairée. Les données pourront être traitées si cela est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement des données, à moins que ne prévalent les libertés et droits fondamentaux de la personne concernée. La personne concernée peut retirer son consentement à tout moment.

(RGPD : article 7; considérants 32, 33, 42, 43)

CONSENTEMENT D'UN ENFANT

La notion de consentement au sens du RGPD s'applique aux personnes concernées âgées d'au moins 16 ans. Pour les moins de 16 ans, l'organisation doit obtenir le consentement d'un parent ou d'un tuteur de l'enfant avant que les données concernant l'enfant ne soient recueillies, traitées, stockées ou communiquées.

(RGPD : article 8; considérant 38)

CATÉGORIES PARTICULIÈRES

Le traitement de certains types de données hautement sensibles est interdit sauf consentement explicite de la personne concernée ou dans des circonstances exceptionnelles. Entrent dans ces catégories particulières les données concernant la santé, les données biométriques, les données à caractère personnel qui révèlent l'origine raciale ou ethnique, l'orientation sexuelle, les convictions religieuses ou philosophiques, les opinions politiques ou l'appartenance syndicale.

(RGPD : article 9; considérants 46, 51, 52, 53, 54, 55, 56)

NORMES INTERNATIONALES TOUCHANT LE RGPD

ISO/IEC 15944-5:2008 : TECHNOLOGIES DE L'INFORMATION — VUE OPÉRATIONNELLE D'AFFAIRES — PARTIE 5: IDENTIFICATION ET RÉFÉRENCE DES EXIGENCES DE DOMAINES JURIDICTIONNELS EN TANT QUE SOURCES DE CONTRAINTES EXTERNES | Cette norme vise à faciliter l'établissement d'une architecture d'affaires électronique dans le respect de contraintes et exigences externes (ex. domaine de compétence). Elle aide les organisations à mettre le RGPD en application dans leurs pratiques.

ISO/IEC 15944-12:2020 : TECHNOLOGIES DE L'INFORMATION — VUE OPÉRATIONNELLE D'AFFAIRES — PARTIE 12: EXIGENCES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE (PPR) RELATIVES À LA GESTION DU CYCLE DE VIE DE L'INFORMATION (ILCM) ET DE L'EDI DES RENSEIGNEMENTS PERSONNELS (PI) | Cette norme établit un cadre qui permet de repérer les contraintes et exigences externes s'appliquant aux données à caractère personnel parmi les renseignements consignés pour une opération d'affaires. Elle présente des pratiques exemplaires qui peuvent améliorer la mise en place de solutions techniques pour assurer le respect du RGPD.

ISO/IEC 19944-1 : INFORMATIQUE EN NUAGE ET PLATE-FORMES DISTRIBUÉES — FLUX DE DONNÉES, CATÉGORIES DE DONNÉES ET UTILISATION DES DONNÉES — PARTIE 1: PRINCIPES DE BASE (EN COURS D'ÉLABORATION) | Cette norme jette les bases de la catégorisation des données qui sont échangées entre les clients et les fournisseurs de services infonuagiques. Elle définit des catégories, comme les données concernant la santé, auxquelles le RGPD s'applique tout particulièrement.

ISO/IEC WD 19944-2: CLOUD COMPUTING AND DISTRIBUTED PLATFORMS — DATA FLOW, DATA CATEGORIES AND DATA USE — PART 2: GUIDANCE ON APPLICATION AND EXTENSIBILITY (EN COURS D'ÉLABORATION) (TITRE INDISPONIBLE EN FRANÇAIS) | Cette norme donnera des indications sur la mise en application de la norme 19944-1 et donnera des exemples se rapportant à la protection de la vie privée.

EXEMPLES D'APPLICATION

COMMENT LE RGPD S'APPLIQUE-T-IL AUX FOURNISSEURS CANADIENS?

Le RGPD vise à protéger les droits individuels des résidents de l'UE, et s'applique aux organisations européennes, aux entreprises qui ont des bureaux en Europe, et aux personnes qui résident dans tout pays membre de l'UE. Les organismes canadiens croient parfois, à tort, que le RGPD ne leur concerne que s'ils font du commerce international ou s'ils ont des clients européens. Mais il y a d'autres cas à prendre en considération, notamment celui des fournisseurs.

Le RGPD stipule que les organisations qui se conforment au RGPD doivent choisir des fournisseurs dont les activités de traitement des données sont elles aussi conformes au Règlement. Autrement dit, les fabricants et les prestataires de services interentreprises de l'UE doivent s'assurer que les produits et services de leurs fournisseurs répondent aux exigences du RGPD. Selon le degré de sensibilité des données qui sont traitées, il peut être indiqué de conclure un accord de protection des données afin de garantir la sécurité des renseignements personnels. Dans d'autres cas, on aura plutôt recours à une entente avec le fournisseur prévoyant une vérification de l'adéquation des mesures de sécurité et de confidentialité en place et donnant l'assurance que le fournisseur dispose d'une stratégie d'atténuation qui établit, entre autres, les délais dans lesquels il faudra aviser les clients en cas de violation des données ou de la sécurité, ainsi que les démarches à suivre.

EXEMPLES

1. Un cabinet de comptables accueille un nouveau client : un cabinet d'avocats canadien. Or, le cabinet d'avocats collecte des données à caractère personnel ou sensible (états financiers, renseignements confidentiels, information juridique privilégiée, etc.) de clients de l'UE. Il fait parvenir reçus et factures détaillés au cabinet de comptables pour que celui-ci puisse faire son travail. Dans cette situation, le cabinet d'avocats doit se conformer au RGPD pour ses clients de l'UE, et le cabinet de comptables doit traiter ces données en utilisant un système conforme au RGPD pour respecter les obligations du cabinet d'avocats.

---

2. Une entreprise du secteur technologique a créé une application de réservation en ligne, qui peut servir à un large éventail de fournisseurs de services : entraîneurs personnels, plombiers, coiffeurs, etc. L'application permet de collecter des données à caractère personnel telles que le nom et le numéro de téléphone des clients. L'un de ces clients est un centre de conditionnement physique canadien avec des succursales dans l'UE et qui doit, par conséquent, se conformer au RGPD. Pour traiter les données du centre de conditionnement physique, il faut que le système utilisé par l'entreprise fournissant l'application soit conforme au RGPD.

QUELLES SONT LES INCIDENCES DU RGPD SUR DIFFÉRENTS SECTEURS?

Comme le RGPD protège les données à caractère personnel des citoyens et résidents de l'UE où qu'ils soient, il peut s'appliquer aux organisations canadiennes même si elles ne mènent aucune activité dans l'UE. Il peut être difficile de savoir si une personne est citoyenne ou résidente de l'UE lorsque, par exemple, ces données sont obtenues par l'entremise d'un site Web ou d'un centre d'appels. Les organisations qui collectent des données à caractère personnel, en format papier ou numérique, doivent indiquer le type de données qu'elles souhaitent recueillir ainsi que les raisons de la collecte, et solliciter le consentement de la personne concernée préalablement à la collecte et à l'insertion de témoins sur un site Web.

SOINS DE SANTÉ ET SCIENCES DE LA VIE

Une répercussion importante pour ce secteur est l'obligation de demander un consentement explicite avant la collecte de données génétiques, de données biométriques, de données concernant la santé et de données relatives aux essais cliniques. Le RGPD impose des restrictions sur la collecte de données de catégories particulières qui, par leur nature, peuvent poser un risque pour la personne concernée, par exemple son ethnicité, ses croyances religieuses, des photos ou vidéos d'elle, ses empreintes digitales ou d'autres données biométriques, les données concernant sa santé, etc. Aussi est-il fortement recommandé, pour les données cliniques, de recourir à des mécanismes de protection de la confidentialité comme la pseudonymisation, la dépersonnalisation ou le chiffrement. Les organisations du milieu médical et des sciences de la vie doivent aussi trouver des moyens de protéger adéquatement les données, les résultats d'examen, les images médicales et d'autres données des patients générés et stockés par les appareils connectés à l'Internet des objets.

Exemples d'application : Une multinationale du secteur pharmaceutique qui a son siège au Canada et mène des essais cliniques dans les États membres de l'UE; une entreprise qui conçoit des applications mobiles de suivi des maladies chroniques et de la condition physique; un fabricant d'appareils médicaux qui permettent de suivre en temps réel les signes vitaux du patient.

VENTE AU DÉTAIL

Le RGPD protège le droit des personnes de refuser de consentir à l'utilisation de leurs données, ce qui a des implications majeures pour les détaillants, qui doivent obtenir le consentement des consommateurs pour collecter, traiter ou communiquer leurs données à caractère personnel. Cette protection touche particulièrement les détaillants qui utilisent les données relatives à la clientèle pour leurs activités de vente et de marketing.

Exemples d'application : Un site Web d'entreprise à portée internationale qui utilise des témoins pour collecter des données à caractère personnel; une entreprise qui se sert d'une base de données existante ou commerciale pour faire de la prospection ciblée auprès de résidents de l'UE.

SYSTÈMES D'INFORMATION

Le RGPD impose certaines obligations relativement aux systèmes d'information utilisés par les sous-traitants des données et à la protection des données. Il stipule, par exemple, que le traitement des données doit toujours être effectué conformément aux exigences du RGPD et aux exigences du responsable du traitement. Les sous-traitants ne sont pas autorisés à faire appel à leur tour à un sous-traitant pour traiter les données des clients sans avoir obtenu au préalable et par écrit le consentement du responsable du traitement.

Exemples d'application : Un centre de données canadien qui stocke les données de clients; l'exploitant d'un système infonuagique de gestion de l'apprentissage ou d'un service de gestion des relations-client qui met sa plateforme à la disposition de clients qui pourraient recueillir des données à caractère personnel sur les utilisateurs de la plateforme.

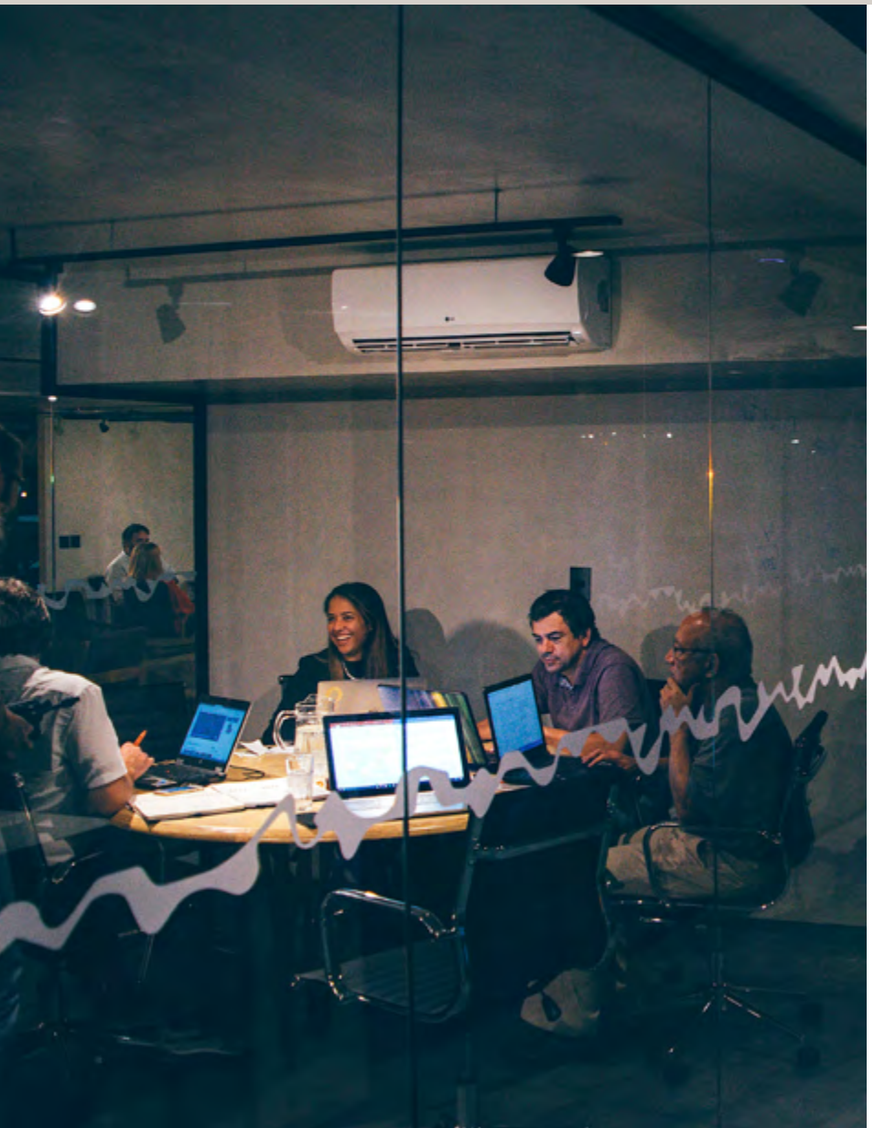
ÉDUCATION

La principale incidence du RGPD sur ce secteur concerne les données de catégories particulières et ceux qui y ont accès. Le règlement impose des restrictions sur ces données puisque, par leur nature même, elles peuvent poser un risque pour les personnes concernées : par exemple, les informations qui permettent de connaître ou d'inférer les restrictions alimentaires sont susceptibles de révéler les croyances religieuses. Qui plus est, la collecte de données à caractère personnel auprès d'un élève de moins de 16 ans nécessite le consentement d'un parent ou d'un tuteur.

Exemples d'application : Une université canadienne à laquelle s'inscrivent des étudiants de l'UE; les membres d'un corps professoral qui collaborent à un projet de recherche avec des collègues de l'UE; une école publique qui recueille de l'information auprès d'élèves provenant de l'UE ou de leurs parents.

DROITS, OBLIGATIONS ET VOIES DE RECOURS

Le RGPD prévoit nombre de droits, d'obligations et de voies de recours. Articulé autour du droit fondamental à la vie privée, il accorde aux personnes concernées des droits robustes, leur assurant un contrôle sur les données les concernant bien supérieur à celui d'autres cadres législatifs, dont celui du Canada. Il prévoit aussi un encadrement serré des organisations pour qu'elles protègent les données personnelles qu'elles collectent.



DROITS FONDAMENTAUX DES PERSONNES CONCERNÉES

DROIT D'ÊTRE INFORMÉ | L'organisation doit informer la personne concernée de ses droits en lui communiquant à ce sujet une information complète, aisément accessible et compréhensible.

(RGPD : articles 13, 14; considérants 60, 61, 62)

DROIT D'ACCÈS | La personne concernée a le droit de consulter toutes les données à caractère personnel la concernant détenue par une organisation, y compris le droit de savoir comment ces données sont traitées.

(RGPD : article 15; considérants 63, 64)

DROIT DE RECTIFICATION | La personne concernée a le droit d'obtenir d'une organisation la rectification des données la concernant.

(RGPD : article 16; considérant 65)

DROIT À L'EFFACEMENT (« DROIT À L'OUBLI ») | La personne concernée a le droit de faire effacer complètement d'un système toutes les données à caractère personnel la concernant. À noter toutefois que ce droit n'est pas absolu et peut faire l'objet d'exceptions.

(RGPD : article 17; considérants 65, 66)

DROIT À LA LIMITATION DU TRAITEMENT | La personne concernée a le droit de demander à une organisation de limiter l'utilisation des données. À la différence du droit à l'effacement, l'organisation peut conserver les données, mais ne doit plus les utiliser d'aucune façon.

(RGPD : article 18; considérant 67)

DROIT À LA PORTABILITÉ DES DONNÉES | La personne concernée a le droit d'obtenir les données la concernant dans un format lisible par machine et facile à transmettre à une autre organisation pour les faire traiter.

(RGPD : article 20; considérant 68)

DROIT D'OPPOSITION | La personne concernée a le droit de s'opposer à ce qu'un tiers traite des données la concernant à des fins de marketing direct (publicité) ou de recherche.

(RGPD : article 21; considérants 69, 70)

DROITS RELATIFS À LA DÉCISION AUTOMATISÉE ET AU PROFILAGE | La personne concernée a le droit d'interdire que des décisions la concernant soient prises par un système automatisé ou une intelligence artificielle sans l'intervention d'un être humain. À noter toutefois que ce droit n'est pas absolu et peut faire l'objet d'exceptions.

(RGPD : article 22; considérants 71, 72, 91)

OBLIGATIONS FONDAMENTALES DES ORGANISATIONS

RESPONSABILITÉS DU RESPONSABLE DU TRAITEMENT | Le responsable du traitement des données est chargé de la mise en place de mesures techniques et organisationnelles appropriées pour protéger la vie privée des personnes concernées et leurs informations en fonction de la sensibilité de celles-ci.

(RGPD : article 24; considérants 74, 75, 76, 77)

PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PROTECTION DES DONNÉES PAR DÉFAUT | Les principes de protection des données dès la conception et par défaut sont appliqués pour garantir que les produits et services répondent intrinsèquement aux critères de sécurité et de confidentialité.

(RGPD : article 25; considérant 78)

RESPONSABLES CONJOINTS DU TRAITEMENT | Si deux entités déterminent les finalités du traitement, elles sont les responsables conjoints du traitement et doivent décider ensemble laquelle d'entre elles veillera au respect des exigences en cas d'exercice par la personne concernée des droits prévus par le RGPD.

(RGPD : article 26; considérant 79)

REPRÉSENTANTS DES RESPONSABLES DU TRAITEMENT OU DES SOUS-TRAITANTS EN DEHORS DE L'UE | Si ni le responsable du traitement ni le sous-traitant ne sont établis dans l'UE, ils doivent désigner un représentant qui l'est. Cette désignation doit être faite par écrit, et les autorités de protection des données compétentes doivent en être avisées.

(RGPD : article 27; considérant 80)

SOUS-TRAITANT | Pour qu'un responsable du traitement soit conforme au RGPD, il faut que tous les sous-traitants qu'il choisit veillent à la conformité de leurs activités de traitement aux exigences du RGPD.

(RGPD : article 28; considérant 81)

TRAITEMENT | Les données ne peuvent faire l'objet d'un traitement de la part d'un sous-traitant que sur instruction du responsable du traitement ou que s'il y est obligé par le droit de l'UE ou le droit d'un État membre.

(RGPD : article 29; aucun considérant)

REGISTRE DES ACTIVITÉS DE TRAITEMENT | Le responsable du traitement doit tenir un registre comportant notamment les informations suivantes : le nom et les coordonnées du délégué à la protection des données et de ses représentants, les traitements de données, les bases juridiques du traitement, les catégories de données traitées. Il doit aussi indiquer si les données sont des renseignements personnels ou non.

(RGPD : article 30; considérants 13, 82)

COOPÉRATION AVEC L'AUTORITÉ DE CONTRÔLE | Le responsable du traitement et le sous-traitant doivent coopérer avec l'autorité de protection des données compétente, à la demande de celle-ci.

(RGPD : article 31; considérant 82)

NORMES INTERNATIONALES TOUCHANT LE RGPD

ISO/IEC 20546:2019 : TECHNOLOGIES DE L'INFORMATION — MÉGADONNÉES — VUE D'ENSEMBLE ET VOCABULAIRE | Cette norme établit un langage clair et commun pour faciliter la compréhension des divers concepts entourant les mégadonnées, ce qui peut faciliter la conformité au RGPD.

ISO/IEC 20889:2018 : TERMINOLOGIE ET CLASSIFICATION DES TECHNIQUES DE DÉ-IDENTIFICATION DE DONNÉES POUR LA PROTECTION DE LA VIE PRIVÉE | Cette norme traite de l'utilisation et de l'importance de la dépersonnalisation (dé-identification) conformément aux principes de protection de la vie privée établis dans ISO/IEC 29100. Elle peut s'avérer utile pour renforcer la protection des données personnelles au regard du RGPD.

ISO/IEC 22624:2020 INFORMATION TECHNOLOGY — CLOUD COMPUTING — TAXONOMY BASED DATA HANDLING FOR CLOUD SERVICES (TITRE INDISPONIBLE EN FRANÇAIS) | Cette norme traite plus en profondeur de la classification des données et de la géolocalisation, en indiquant précisément quand la réglementation, p. ex. le RGPD, entre en ligne de compte.

ISO/IEC TR 22678:2019 INFORMATION TECHNOLOGY — CLOUD COMPUTING — GUIDANCE FOR POLICY DEVELOPMENT (TITRE INDISPONIBLE EN FRANÇAIS) | Cette norme, qui s'adresse aux entreprises et se veut de portée globale, met en lumière les politiques qui pourraient devoir être analysées, et éventuellement modifiées, clarifiées ou interprétées. Ce peut être le cas de certaines politiques et interprétations se rapportant aux RGPD, lesquelles pourraient exiger des positions claires.

OBLIGATIONS FONDAMENTALES DES ORGANISATIONS

SÉCURITÉ DU TRAITEMENT | Le responsable du traitement et le sous-traitant ont l'obligation de mettre en place des mécanismes organisationnels et techniques adéquats pour assurer la sécurité de leurs systèmes afin d'en protéger les données. Ils doivent aussi veiller à ce que des mesures appropriées soient appliquées pour limiter les accès physiques.

(RGPD : article 32; considérants 75, 76, 77, 78, 79, 83)

NOTIFICATION D'UNE VIOLATION DE DONNÉES (AUX AUTORITÉS) | Si la sécurité ou des données font l'objet d'une violation, le responsable du traitement doit en aviser l'autorité de contrôle compétente dans les 72 heures après en avoir pris connaissance. Il n'a toutefois pas à aviser les autorités si le risque de préjudice à la personne concernée est faible ou non-existant. Enfin, si la violation se produit chez le sous-traitant, celui-ci doit en aviser dans les meilleurs délais le responsable du traitement.

(RGPD : article 33; considérants 85, 87, 88)

NOTIFICATION D'UNE VIOLATION DE DONNÉES (À LA PERSONNE CONCERNÉE) | Si la violation de la sécurité ou des données pose un risque de préjudice élevé pour la personne concernée, le responsable du traitement doit l'en aviser. La notification doit porter sur la nature de la violation, décrire les mesures prises pour y remédier et donner des instructions claires sur les démarches à suivre par la personne concernée pour protéger sa vie privée et ses données.

(RGPD : article 34; considérants 86, 87, 88)

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES ET CONSULTATION PRÉALABLE | Le responsable du traitement doit soumettre ses produits et services à une analyse d'impact relative à la protection des données afin de déterminer s'ils impliquent des renseignements personnels et quelles seront les répercussions, le cas échéant, pour la confidentialité de ces renseignements pour les traitements de données à haut risque. L'analyse d'impact est un outil de gestion des risques essentiel pour cartographier les systèmes et les flux de données et pour repérer, analyser, mesurer et atténuer ou éliminer les risques pour la vie privée.

(RGPD : articles 35, 36; considérants 75, 84, 89, 90, 91, 92, 93, 94, 95, 96)

DÉSIGNATION, FONCTION ET MISSIONS DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES | Toute organisation qui traite de l'information se rapportant au suivi de personnes concernées, ou qui fait effectuer ce traitement par un organisme public, doit désigner un délégué à la protection des données, qui se chargera des communications entre le responsable du traitement, le sous-traitant et l'autorité de contrôle compétente. Le délégué à la protection des données surveille également que l'organisation se plie bien au RGPD.

(RGPD : articles 37, 38, 39; considérant 97)

NORMES INTERNATIONALES TOUCHANT LE RGPD

ISO/IEC CD 23751 INFORMATION TECHNOLOGY — CLOUD COMPUTING AND DISTRIBUTED PLATFORMS — DATA SHARING AGREEMENT (DSA) FRAMEWORK (EN COURS D'ÉLABORATION) (TITRE INDISPONIBLE EN FRANÇAIS) | Cette norme porte sur le partage des données. Ce concept de partage sur autorisation peut se répercuter sur la manière dont est appliqué le RGPD.

ISO/IEC 27001:2013 : TECHNOLOGIES DE L'INFORMATION — TECHNIQUES DE SÉCURITÉ — SYSTÈMES DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION — EXIGENCES | Cette norme très utilisée propose un cadre robuste pour la mise en place d'un système de gestion de la sécurité de l'information, ce qui peut aider à prévenir les violations de données et facilité la conformité au RGPD.

ISO/IEC 27002:2013 : TECHNOLOGIES DE L'INFORMATION — TECHNIQUES DE SÉCURITÉ — CODE DE BONNE PRATIQUE POUR LE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION | Cette norme sert de document d'orientation pour l'application de la norme 27001 et pour le choix des bonnes mesures de contrôle pour l'établissement d'un système de gestion de la sécurité de l'information.

ISO/IEC 27018:2019 : TECHNOLOGIES DE L'INFORMATION — TECHNIQUES DE SÉCURITÉ — CODE DE BONNES PRATIQUES POUR LA PROTECTION DES INFORMATIONS PERSONNELLES IDENTIFIABLES (PII) DANS L'INFORMATIQUE EN NUAGE PUBLIC AGISSANT COMME PROCESSEUR DE PII | Cette norme propose un cadre de protection des PII dans les systèmes infonuagiques publics fondé sur ISO/IEC 27002 et conforme à ISO/IEC 29100. Ce mécanisme de protection des PII peut venir renforcer la sécurité des données à caractère personnel, ce qui constitue un volet essentiel du RGPD.

VOIES DE RECOURS DE LA PERSONNE CONCERNÉE

DROIT D'INTRODUIRE UNE RÉCLAMATION | La personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle si elle considère que ses données ont été traitées d'une façon qui viole ses droits au titre du RGPD.

(RGPD : article 77; considérant 141)

DROIT À UN RECOURS EFFECTIF CONTRE UN RESPONSABLE DU TRAITEMENT OU UN SOUS-TRAITANT | La personne concernée a droit à un recours juridictionnel effectif si elle considère que ses renseignements personnels ont été utilisés d'une façon qui viole ses droits.

(RGPD : article 79; considérants 141, 145)

SANCTIONS

AMENDES ADMINISTRATIVES | Les amendes sont déterminées en fonction du préjudice aux personnes concernées, du nombre de personnes concernées touchées et du degré de diligence dont a fait preuve le responsable du traitement ou le sous-traitant. Selon la violation, l'amende peut s'élever à 20 millions d'euros, ou à un montant représentant 2 % à 4 % du chiffre d'affaires annuel mondial brut de l'exercice précédent.

(RGPD : article 83; considérants 148, 149, 150, 151, 152)

SANCTIONS | Il revient aux États membres désirant imposer d'autres sanctions aux responsables du traitement ou aux sous-traitants d'en établir les règles.

(RGPD : article 84; considérants 149, 150, 151, 152)

RESPONSABILITÉ

DROIT À RÉPARATION ET RESPONSABILITÉ
La personne concernée a droit à réparation si elle subit un préjudice matériel (ex. : perte financière) ou moral (ex. : atteinte à la réputation) en raison de la violation par le responsable du traitement (ou dans certains cas précis, par le sous-traitant) de ses obligations au titre du RGPD.

(GDPR: Article 82, Recitals 146, 147)

NORMES INTERNATIONALES TOUCHANT LE RGPD

ISO/IEC 27701:2019 : TECHNIQUES DE SÉCURITÉ — EXTENSION D'ISO/IEC 27001 ET ISO/IEC 27002 AU MANAGEMENT DE LA PROTECTION DE LA VIE PRIVÉE — EXIGENCES ET LIGNES DIRECTRICES | Cette norme constitue une addition d'ISO/IEC 27001 et d'ISO/IEC 27002; elle spécifie les exigences liées au maintien d'un système de gestion de la sécurité de l'information.

ISO/IEC 29100:2011 : TECHNOLOGIES DE L'INFORMATION — TECHNIQUES DE SÉCURITÉ — CADRE PRIVÉ | Ce document établit un cadre de sécurité des renseignements nominatifs pour le domaine des technologies de l'information et de la communication. Vu que ce cadre peut améliorer le traitement des données à caractère personnel, il peut s'avérer utile dans les démarches de mise en conformité au RGPD.

ISO/IEC 29151:2017 : TECHNOLOGIES DE L'INFORMATION — TECHNIQUES DE SÉCURITÉ — CODE DE BONNE PRATIQUE POUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL | Fondée sur ISO/IEC 27002, cette norme traite de l'application de mesures de contrôle pour limiter les risques de violation des données, ce qui est l'un des grands objectifs du RGPD.

ISO/IEC 29184:2020 : TECHNOLOGIES DE L'INFORMATION — DÉCLARATIONS DE CONFIDENTIALITÉ EN LIGNE ET LES CONSENTEMENTS | Cette norme jette les bases d'un processus d'obtention du consentement éclairé des clients à l'utilisation de leurs données, le tout d'une manière qui correspond étroitement aux exigences du RGPD.

ISO/AWI 31700 CONSUMER PROTECTION — PRIVACY BY DESIGN FOR CONSUMER GOODS AND SERVICES (EN COURS D'ÉLABORATION) (TITRE INDISPONIBLE EN FRANÇAIS) | Cette norme porte sur le droit à la vie privée des consommateurs et établit une feuille de route que doivent suivre les organisations lorsqu'elles conçoivent et intègrent des mesures de contrôle et mécanismes de protection de la vie privée à leurs produits. Elle traite des questions de vie privée soulevées dans le RGPD.

ISO/IEC 38500:2015 : TECHNOLOGIES DE L'INFORMATION — GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION POUR L'ENTREPRISE | Cette norme fournit un modèle de gouvernance pour l'établissement d'une infrastructure informatique efficace, ce qui peut faciliter la transition vers un modèle conforme au RGPD.

ISO/IEC 38505-1:2017 : TECHNOLOGIES DE L'INFORMATION — GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION — GOUVERNANCE DES DONNÉES — PARTIE 1: APPLICATION DE L'ISO/IEC 38500 À LA GOUVERNANCE DES DONNÉES | Cette norme porte sur l'application d'ISO/IEC 38500 aux gestionnaires d'organisations.

ÉTAPES SUIVANTES

1) ADOPTER UN CADRE DE PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PAR DÉFAUT

La protection des données recoupe les valeurs et les exigences associées à la sécurité et à la gestion de l'information ainsi qu'à la confidentialité et à la gouvernance des données. Il est fortement recommandé d'adopter des pratiques exemplaires et d'améliorer en continu les mesures de protection des données. Les critères de conformité varient en fonction du domaine et de l'autorité compétente ainsi que du type d'information en jeu, mais toute organisation gagne à s'y conformer, que ce soit pour respecter les lois et règlements ou pour répondre aux attentes des clients.

2) EFFECTUER UNE ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

La protection des informations personnelles et des droits individuels est un des fondements du RGPD. Les organisations devraient donc effectuer – avant de concevoir, de développer, d'acquérir ou de mettre en œuvre tout procédé, produit ou système – une analyse d'impact relative à la protection des données afin d'évaluer comment, tout au long de leur cycle de vie, les données à caractère personnel seront collectées, consultées, stockées, transmises et supprimées. Les organisations ont aussi intérêt à tenir compte des bases juridiques, comme la notion de consentement, qui sous-tendent le traitement et le contrôle des données. L'analyse doit aussi passer par la production d'une carte des systèmes et une carte des données faisant le suivi des entrées, consultations et enregistrements de données à l'échelle des systèmes. À noter qu'il faut toujours mener une analyse d'impact lorsque le traitement peut présenter un risque élevé pour la personne concernée.

3) ÉTABLIR UN ACCORD DE TRAITEMENT DES DONNÉES

La plupart des organisations font affaire avec des tiers qui se chargent des données et de leur traitement. L'écosystème de données ainsi créé nécessite la conclusion d'accords de traitement qui établissent à qui, parmi les diverses parties, reviennent les droits et les responsabilités relativement à la protection des données en jeu. Ces accords doivent être rédigés clairement et sans ambiguïté, et leur libellé doit s'accorder avec celui du RGPD. Il est conseillé de consulter un professionnel qualifié bien informé sur la question, ou encore un avocat spécialisé.

4) DÉSIGNER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Le RGPD impose à beaucoup d'organisations d'avoir un délégué à la protection des données, obligation parfois facultative. Le délégué est chargé de conseiller l'organisation et de prendre en charge les questions de confidentialité et de vie privée. Il doit donc être suffisamment qualifié et posséder les compétences, les connaissances et l'expérience nécessaires pour aider son organisation à composer avec les réalités de plus en plus complexes à l'échelle nationale et internationale en matière de confidentialité, de consultation et de protection des données.

5) CONSIDÉRER LES OPTIONS DE MISE EN CONFORMITÉ

Pour protéger les données des consommateurs dans un monde où les frontières commerciales s'estompent, il faut bien se conformer aux mécanismes de confidentialité et de sécurité ainsi qu'aux systèmes de gestion de la qualité. Pour ce faire, il y a diverses démarches à suivre : l'autocertification, la certification privée ou l'obtention d'une certification aux normes internationales. (À noter que le Canada est membre participant d'ISO/PC 317, le comité qui rédige la norme ISO sur les exigences de protection des données en fonction du RGPD.)

6) RESPECTER LES LOIS RÉGISSANT LA COMMUNICATION OUTRE-FRONTIÈRE

Depuis 2001, le Canada jouit d'une situation favorable. L'Union européenne lui a conféré cette année-là le statut d'adéquation, permettant aux données à caractère personnel d'être transmises de l'UE vers le Canada, reconnaissant les protections des données qu'offre la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) comme équivalentes à celles que l'UE accorde à ces citoyens. Selon la LPRPDE, « une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie ». En revanche, la législation canadienne sur la protection de la vie privée et l'accès à l'information n'a pas été modifiée pour répondre aux critères du RGPD, il est donc important de rester vigilant aux changements reliés au statut d'adéquation afin de demeurer conforme.

7) S'AMÉLIORER EN CONTINU

Parmi les pratiques exemplaires de mise en conformité figure l'application d'un modèle d'amélioration continue. Il s'agit d'une belle occasion pour une organisation de peaufiner ses produits et ses pratiques de gouvernance, de renforcer les mécanismes de confidentialité de ses produits et d'améliorer ses relations globales avec les consommateurs et les organismes de réglementation. C'est pourquoi il est recommandé de mettre en place un cycle d'amélioration continue.

NOUS SOMMES PRÊTS À VOUS AIDER

Aider les organisations Canadienne à prospérer grâce à la normalisation est notre spécialité.

L'information partagée dans ce document vise à promouvoir les efforts de votre organisation en lien au RGPD. Pour se renseigner et découvrir les avantages de la normalisation, visiter notre site Web : **www.ccn.ca**.

ENTREZ DANS LE MONDE DE LA NORMALISATION

613 238-3222
innovation@scc.ca
www.ccn.ca

ANNEXE

■ ARTICLES CLÉS DU RGPD ET NORMES POUVANT SOUTENIR LE PROCESSUS DE CONFORMITÉ

Ce tableau résume les informations des sections précédentes. Il est recommandé d'utiliser ce tableau comme un outil de référence rapide pour un accès facile à des informations succinctes sur le RGPD.

ARTICLES CLÉS DU RGPD	ARTICLES	CONSIDÉRANTS	DESCRIPTIONS *Le texte de ce document se fonde sur celui du RGPD. D'autres interprétations sont possibles.	NORMES INTERNATIONALES POUVANT FACILITER LE PROCESSUS DE CONFORMITÉ AU RGPD
TERMES CLÉS DU RGPD				
1. Champ d'application territorial	3	22, 23, 24, 25	Le RGPD concerne les données à caractère personnel des résidents de l'UE traitées et stockées à l'intérieur comme à l'extérieur de l'UE. Il s'applique aux organisations qui : a) ont une présence physique dans l'UE, b) mènent des activités de traitement de données se rapportant à l'offre de biens ou de services aux résidents de l'UE, ou c) surveillent les actions des résidents de l'UE qui se trouvent sur le territoire de l'UE (ex. : surveillance de leur activité sur Internet à des fins publicitaires). Le RGPD s'applique aussi à toutes les organisations hors de l'UE qui traitent des données à caractère personnel se rapportant aux résidents de l'UE, où qu'elles soient.	**ISO/IEC 15944-5:2008 :** Technologies de l'information — Vue opérationnelle d'affaires — Partie 5: Identification et référence des exigences de domaines juridictionnels en tant que sources de contraintes externes **ISO/IEC 15944-12:2020 :** Technologies de l'information — Vue opérationnelle d'affaires — Partie 12: Exigences en matière de protection de la vie privée (PPR) relatives à la gestion du cycle de vie de l'information (ILCM) et de l'EDI des renseignements personnels (PI) **ISO/IEC 19944-1 :** Informatique en nuage et plate-formes distribuées — Flux de données, catégories de données et utilisation des données — Partie 1: Principes de base (en cours d'élaboration)
2. Définitions	4	15, 24, 26, 28, 29, 30, 31, 34, 35, 36, 37		
a. Données à caractère personnel			Aussi appelées « renseignements personnels », « renseignements nominatifs » ou « renseignements permettant d'identifier une personne », les données à caractère personnel constituent toute information qui se rapporte à une personne donnée. Cette information peut avoir été obtenue de la personne en question, ou encore avoir été générée lors de l'utilisation ou du traitement d'autres renseignements la concernant.	
b. Traitement des données			Toute opération appliquée à des données ou des ensembles de données à caractère personnel, telles que la manipulation, la catégorisation ou l'utilisation dans des opérations mathématiques.	
c. Personne concernée			Personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, des données de localisation, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Autrement dit, la personne concernée est un être humain au sujet duquel et auprès duquel une organisation obtient de l'information à caractère personnel.	

ARTICLES CLÉS DU RGPD	ARTICLES	CONSIDÉRANTS	DESCRIPTIONS *Le texte de ce document se fonde sur celui du RGPD. D'autres interprétations sont possibles.	NORMES INTERNATIONALES POUVANT FACILITER LE PROCESSUS DE CONFORMITÉ AU RGPD
d. Responsable du traitement des données			Organisation qui décide quelles données seront recueillies, traitées et stockées, et qui répond des méthodes employées pour la collecte, le traitement et le stockage des données ainsi que de l'accessibilité, de la sécurité et de la conservation des données. Elle est également responsable des décisions concernant la sollicitation des tiers (sous-traitants des données).	**ISO/IEC WD 19944-2 :** Cloud computing and distributed platforms — Data flow, data categories and data use — Part 2: Guidance on application and extensibility (en cours d'élaboration) (titre indisponible en français) **ISO/IEC 20546:2019 :** Technologies de l'information — Mégadonnées — Vue d'ensemble et vocabulaire **ISO/IEC 20889:2018 :** Terminologie et classification des techniques de dé-identification de données pour la protection de la vie privée **ISO/IEC 22624:2020 :** Information technology — Cloud computing — Taxonomy based data handling for cloud services (titre indisponible en français) **ISO/IEC TR 22678:2019 :** Information technology — Cloud computing — Guidance for policy development (titre indisponible en français)
e. Sous-traitant des données			Personne ou organisation qui traite des données à caractère personnel sur instruction du responsable du traitement. Le sous-traitant des données n'est pas propriétaire des données ni ne contrôle les finalités du traitement. Il est possible pour une organisation d'être à la fois responsable du traitement des données et sous-traitant des données.	
f. Délégué à la protection des données	37, 38, 39	97	Le délégué à la protection des données veille au respect des lois sur la protection de la vie privée en vigueur au sein d'une organisation. Il doit pouvoir exercer ses fonctions sans ingérences, et faire rapport à la plus haute autorité de l'organisation. Il est aussi le point de contact pour les APD, avec lesquelles il collabore en tant que de besoin. Enfin, il est la personne-ressource pour tout ce qui touche la protection de la vie privée; il assure des actions de formation adéquates; et il évalue et communique les risques.	
GRANDS PRINCIPES DU RGPD				
1. Traitement et responsabilité	5	39	Les données recueillies doivent être limitées à ce qui est nécessaire, se rapporter clairement à la personne concernée, et être traitées avec les précautions et la confidentialité que demande leur degré de sensibilité.	
2. Licéité	6	39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 171	Le traitement des données est considéré comme licite s'il est effectué avec le consentement de la personne à qui ces données se rapportent, s'il est nécessaire au fonctionnement de l'organisation qui les recueille, ou s'il est justifié par un motif légal valide.	
3. Consentement	7	32, 33, 42, 43	Le cas échéant, les données à caractère personnel ne peuvent être recueillies, traitées ou communiquées que si la personne concernée a donné son consentement, et ce, en termes clairs, de plein gré et de manière éclairée. Les données pourront être traitées si cela est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement des données, à moins que ne prévalent les libertés et droits fondamentaux de la personne concernée. La personne concernée peut retirer son consentement à tout moment.	
4. Consentement d'un enfant	8	38	La notion de consentement au sens du RGPD s'applique aux personnes concernées âgées d'au moins 16 ans. Pour les moins de 16 ans, l'organisation doit obtenir le consentement d'un parent ou d'un tuteur de l'enfant avant que les données concernant l'enfant ne soient recueillies, traitées, stockées ou communiquées.	

ARTICLES CLÉS DU RGPD	ARTICLES	CONSIDÉRANTS	DESCRIPTIONS *Le texte de ce document se fonde sur celui du RGPD. D'autres interprétations sont possibles.	NORMES INTERNATIONALES POUVANT FACILITER LE PROCESSUS DE CONFORMITÉ AU RGPD
5. Catégories particulières	9	46, 51, 52, 53, 54, 55, 56	Le traitement de certains types de données hautement sensibles est interdit sauf consentement explicite de la personne concernée ou dans des circonstances exceptionnelles. Entrent dans ces catégories particulières les données concernant la santé, les données biométriques, les données à caractère personnel qui révèlent l'origine raciale ou ethnique, l'orientation sexuelle, les convictions religieuses ou philosophiques, les opinions politiques ou l'appartenance syndicale.	**ISO/IEC CD 23751 :** Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework (en cours d'élaboration) (titre indisponible en français) **ISO/IEC 27001:2013 :** Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences **ISO/IEC 27002:2013 :** Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information **ISO/IEC 27018:2019 :** Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII **ISO/IEC 27701:2019 :** Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices
DROITS FONDAMENTAUX DES PERSONNES CONCERNÉES				
1. Droit d'être informé	13, 14	60, 61, 62	L'organisation doit informer la personne concernée de ses droits en lui communiquant à ce sujet une information complète, aisément accessible et compréhensible.	
2. Droit d'accès	15	63, 64	La personne concernée a le droit de consulter toutes les données à caractère personnel la concernant détenue par une organisation, y compris le droit de savoir comment ces données sont traitées.	
3. Droit de rectification	16	65	La personne concernée a le droit d'obtenir d'une organisation la rectification des données la concernant.	
4. Droit à l'effacement (« droit à l'oubli »)	17	65, 66	La personne concernée a le droit de faire effacer complètement d'un système toutes les données à caractère personnel la concernant. À noter toutefois que ce droit n'est pas absolu et peut faire l'objet d'exceptions.	
5. Droit à la limitation du traitement	18	67	La personne concernée a le droit de demander à une organisation de limiter l'utilisation des données. À la différence du droit à l'effacement, l'organisation peut conserver les données, mais ne doit plus les utiliser d'aucune façon.	
6. Droit à la portabilité des données	20	68	La personne concernée a le droit d'obtenir les données la concernant dans un format lisible par machine et facile à transmettre à une autre organisation pour les faire traiter.	
7. Droit d'opposition	21	69, 70	La personne concernée a le droit de s'opposer à ce qu'un tiers traite des données la concernant à des fins de marketing direct (publicité) ou de recherche.	

ARTICLES CLÉS DU RGPD	ARTICLES	CONSIDÉRANTS	DESCRIPTIONS *Le texte de ce document se fonde sur celui du RGPD. D'autres interprétations sont possibles.	NORMES INTERNATIONALES POUVANT FACILITER LE PROCESSUS DE CONFORMITÉ AU RGPD
8. Droits relatifs à la décision automatisée et au profilage	22	71, 72, 91	La personne concernée a le droit d'interdire que des décisions la concernant soient prises par un système automatisé ou une intelligence artificielle sans l'intervention d'un être humain. À noter toutefois que ce droit n'est pas absolu et peut faire l'objet d'exceptions.	**ISO/IEC 29100:2011 :** Technologies de l'information — Techniques de sécurité — Cadre privé **ISO/IEC 29151:2017 :** Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la protection des données à caractère personnel **ISO/IEC 29184:2020 :** Technologies de l'information — Déclarations de confidentialité en ligne et les consentements **ISO/AWI 31700 :** Consumer protection — Privacy by design for consumer goods and services (en cours d'élaboration) (titre indisponible en français) **ISO/IEC 38500:2015 :** Technologies de l'information — Gouvernance des technologies de l'information pour l'entreprise **ISO/IEC 38505-1:2017 :** Technologies de l'information — Gouvernance des technologies de l'information — Gouvernance des données — Partie 1: Application de l'ISO/IEC 38500 à la gouvernance des données
OBLIGATIONS FONDAMENTALES DES ORGANISATIONS				
1. Responsabilités du responsable du traitement	24	74, 75, 76, 77	Le responsable du traitement des données est chargé de la mise en place de mesures techniques et organisationnelles appropriées pour protéger la vie privée des personnes concernées et leurs informations en fonction de la sensibilité de celles-ci.	
2. Protection des données dès la conception et protection des données par défaut	25	78	Les principes de protection des données dès la conception et par défaut sont appliqués pour garantir que les produits et services répondent intrinsèquement aux critères de sécurité et de confidentialité.	
3. Responsables conjoints du traitement	26	79	Si deux entités déterminent les finalités du traitement, elles sont les responsables conjoints du traitement et doivent décider ensemble laquelle d'entre elles veillera au respect des exigences en cas d'exercice par la personne concernée des droits prévus par le RGPD.	
4. Représentants des responsables du traitement ou des sous-traitants en dehors de l'UE	27	80	Si ni le responsable du traitement ni le sous-traitant ne sont établis dans l'UE, ils doivent désigner un représentant qui l'est. Cette désignation doit être faite par écrit, et les autorités de protection des données compétentes doivent en être avisées.	
5. Sous-traitant	28	81	Pour qu'un responsable du traitement soit conforme au RGPD, il faut que tous les sous-traitants qu'il choisit veillent à la conformité de leurs activités de traitement aux exigences du RGPD.	

ARTICLES CLÉS DU RGPD	ARTICLES	CONSIDÉRANTS	DESCRIPTIONS *Le texte de ce document se fonde sur celui du RGPD. D'autres interprétations sont possibles.	NORMES INTERNATIONALES POUVANT FACILITER LE PROCESSUS DE CONFORMITÉ AU RGPD
6. Traitement	29	Aucun	Les données ne peuvent faire l'objet d'un traitement de la part d'un sous-traitant que sur instruction du responsable du traitement ou que s'il y est obligé par le droit de l'UE ou le droit d'un État membre.	
7. Registre des activités de traitement	30	13, 82	Le responsable du traitement doit tenir un registre comportant notamment les informations suivantes : le nom et les coordonnées du délégué à la protection des données et de ses représentants, les traitements de données, les bases juridiques du traitement, les catégories de données traitées. Il doit aussi indiquer si les données sont des renseignements personnels ou non.	
8. Coopération avec l'autorité de contrôle	31	82	Le responsable du traitement et le sous-traitant doivent coopérer avec l'autorité de protection des données compétente, à la demande de celle-ci.	
9. Sécurité du traitement	32	75, 76, 77, 78, 79, 83	Le responsable du traitement et le sous-traitant ont l'obligation de mettre en place des mécanismes organisationnels et techniques adéquats pour assurer la sécurité de leurs systèmes afin d'en protéger les données. Ils doivent aussi veiller à ce que des mesures appropriées soient appliquées pour limiter les accès physiques.	
10. Notification d'une violation de données (aux autorités)	33	85, 87, 88	Si la sécurité ou des données font l'objet d'une violation, le responsable du traitement doit en aviser l'autorité de contrôle compétente dans les 72 heures après en avoir pris connaissance. Il n'a toutefois pas à aviser les autorités si le risque de préjudice à la personne concernée est faible ou non-existant. Enfin, si la violation se produit chez le sous-traitant, celui-ci doit en aviser dans les meilleurs délais le responsable du traitement.	
11. Notification d'une violation de données (à la personne concernée)	34	86, 87, 88	Si la violation de la sécurité ou des données pose un risque de préjudice élevé pour la personne concernée, le responsable du traitement doit l'en aviser. La notification doit porter sur la nature de la violation, décrire les mesures prises pour y remédier et donner des instructions claires sur les démarches à suivre par la personne concernée pour protéger sa vie privée et ses données.	
12. Analyse d'impact relative à la protection des données et consultation préalable	35, 36	75, 84, 89, 90, 91, 92, 93, 94, 95, 96	Le responsable du traitement doit soumettre ses produits et services à une analyse d'impact relative à la protection des données afin de déterminer s'ils impliquent des renseignements personnels et quelles seront les répercussions, le cas échéant, pour la confidentialité de ces renseignements pour les traitements de données à haut risque. L'analyse d'impact est un outil de gestion des risques essentiel pour cartographier les systèmes et les flux de données et pour repérer, analyser, mesurer et atténuer ou éliminer les risques pour la vie privée.	

ARTICLES CLÉS DU RGPD	ARTICLES	CONSIDÉRANTS	DESCRIPTIONS *Le texte de ce document se fonde sur celui du RGPD. D'autres interprétations sont possibles.	NORMES INTERNATIONALES POUVANT FACILITER LE PROCESSUS DE CONFORMITÉ AU RGPD
13. Désignation, fonction et missions du délégué à la protection des données	37, 38, 39	97	Toute organisation qui traite de l'information se rapportant au suivi de personnes concernées, ou qui fait effectuer ce traitement par un organisme public, doit désigner un délégué à la protection des données, qui se chargera des communications entre le responsable du traitement, le sous-traitant et l'autorité de contrôle compétente. Le délégué à la protection des données surveille également que l'organisation se plie bien au RGPD.	
RECOURS, RESPONSABILITÉ, SANCTIONS				
1. VOIES DE RECOURS DE LA PERSONNE CONCERNÉE				
a. Droit d'introduire une réclamation	77	141	La personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle si elle considère que ses données ont été traitées d'une façon qui viole ses droits au titre du RGPD.	
b. Droit à un recours effectif contre un responsable du traitement ou un sous-traitant	79	141, 145	La personne concernée a droit à un recours juridictionnel effectif si elle considère que ses renseignements personnels ont été utilisés d'une façon qui viole ses droits.	
2. RESPONSABILITÉ				
a. Droit à réparation et responsabilité	82	146, 147	La personne concernée a droit à réparation si elle subit un préjudice matériel (ex. : perte financière) ou moral (ex. : atteinte à la réputation) en raison de la violation par le responsable du traitement (ou dans certains cas précis, par le sous-traitant) de ses obligations au titre du RGPD.	
3. SANCTIONS				
a. Amendes administratives	83	148, 149, 150, 151, 152	Les amendes sont déterminées en fonction du préjudice aux personnes concernées, du nombre de personnes concernées touchées et du degré de diligence dont a fait preuve le responsable du traitement ou le sous-traitant. Selon la violation, l'amende peut s'élever à 20 millions d'euros, ou à un montant représentant 2 % à 4 % du chiffre d'affaires annuel mondial brut de l'exercice précédent.	
b. Sanctions	84	149, 150, 151, 152	Il revient aux États membres désirant imposer d'autres sanctions aux responsables du traitement ou aux sous-traitants d'en établir les règles.	