Règlement général sur la protection des données (RGPD) :

Le guide de démarrage rapide de Sage pour les entreprises

Table des matières

Introduction

Le Règlement général sur la protection des données (« RGPD ») est le nouveau cadre juridique qui entrera en vigueur le 25 mai 2018 au sein de l'Union européenne (« UE »). La réglementation de l'UE a une incidence directe sur tous les pays membres de l'UE, ce qui veut dire que le RGPD l'emportera sur toute autre loi nationale.

Le RGPD porte essentiellement sur la protection des données personnelles, c'est-à-dire les données concernant les particuliers. En fait, le RGPD est un des plus importants bouleversements à ce jour et modifie la façon dont les données sur une personne devraient être traitées. Il pourrait également toucher non seulement les entreprises, mais aussi les particuliers, les sociétés, les autorités publiques, les organismes ou toute autre entité traitant les données personnelles de particuliers établis au sein de l'UE. Sont inclus les fournisseurs et autres tiers auxquels une entreprise peut avoir recours pour traiter des données personnelles.

Le RGPD a une portée étonnamment large et englobe tous les pays membres de l'Union européenne, ainsi que le Royaume-Uni post-Brexit en 2019, puisque le RGPD sera également intégré à la loi du R.-U. Contrairement aux règles sur la protection des données personnelles de la Directive européenne 95/46, le RGPD touche également les entreprises à l'extérieur de l'UE qui offrent des biens ou des services aux particuliers dans l'UE ou qui surveillent leur comportement au sein de l'UE. Par exemple, les entreprises américaines d'hébergement de sites Internet qui hébergent des sites à la disposition de personnes dans l'UE sont directement concernées.

Le RGPD a des répercussions énormes pour tous les services de bon nombre d'entreprises dans le monde entier. Par exemple, certaines entreprises pourraient devoir utiliser ou désigner un responsable de la protection des données. Presque toutes les entreprises devront mettre en place des pratiques et des mécanismes de protection supplémentaires. Une vérification réalisée par un spécialiste qualifié est vivement recommandée, et compte tenu de la possibilité de s'exposer à des amendes allant jusqu'à 4 % du chiffre d'affaires mondial annuel ou 20 millions d'euros, le plus élevé des deux, la connaissance du RGPD devrait être considérée obligatoire.

Ce document se veut un guide concis et simplifié pour les entreprises. Pour de plus amples renseignements, il faut s'adresser aux autorités de surveillance, comme l'Information Commissioner's Office (ICO) au R.-U. et son document intitulé « Overview of the General Data Protection Regulation ». Veuillez lire l'avertissement légal de Sage apparaissant à la fin du présent guide.

Infographique :

Aperçu du RGPD

Règlement général sur la protection des données (RGPD)

Consentement

Doit être confirmé par une déclaration ou autre mesure affirmative claire. Vous ne pouvez pas présumer du consentement ou même utiliser des cases précochées dans un site Web.

Responsable de la protection des données

Pourrait être obligatoire. Doit avoir une connaissance approfondie de la loi sur la protection des données. Il peut s'agir d'un membre du personnel ou d'un employé contractuel.

Droits des personnes

Élargit considérablement les droits des personnes et l'information qu'elles doivent recevoir au sujet des activités de traitement.

La protection des renseignements personnels du début à la fin

Les considérations de confidentialité doivent être intégrées partout et seules les données strictement nécessaires aux fins stipulées peuvent être utilisées.

Peines

Pourraient aller jusqu'à 4 % du chiffre d'affaires mondial annuel, ou 20 millions d'euros, le plus élevé des deux. Vous pourriez recevoir une amende même en l'absence de perte réelle de données.

Portée élargie

Englobe votre entreprise, en plus des tiers qui traitent des données pour vous — même à l'extérieur de l'UE.

Portabilité des données

Les particuliers ont maintenant le droit de déplacer, de copier ou de transférer leurs données personnelles, même à un concurrent.

Signalement obligatoire des atteintes à la vie privée

Les responsables de traitement des données doivent avertir les autorités de surveillance, comme l'ICO au R.-U., dans un délai de 72 heures après en avoir pris conscience. En cas d'atteinte grave, les particuliers doivent être informés.

Les grandes lignes

Le RGPD établit les exigences minimales concernant le traitement de toutes les données personnelles. Les données personnelles peuvent se définir comme les données identifiant ou concernant un particulier de la plupart des façons (y compris l'apparence physique ou même les données biométriques).

La plupart des entreprises recueillent des données personnelles dès leur première interaction avec un particulier, et dans certains cas, elles n'ont même pas conscience de l'avoir fait. Par exemple, la collecte de données personnelles peut être aussi simple que la surveillance de témoins de sites Web qui identifient un utilisateur de votre site Internet. Elle peut aller jusqu'à quelque chose d'aussi détaillé que le dossier d'une personne dans une base de données pour la gestion des relations avec les clients (« GRC »), et bien plus. Même les cas où les données personnelles sont recueillies ou traitées pour l'avantage exclusif du particulier relèvent du RGPD.

À l'instar de la législation de la Directive 95/46 de l'UE, le RGPD réitère trois grands ensembles de règles qui ont trait aux données personnelles : les principes de protection des données, le traitement licite et les restrictions relatives aux transferts internationaux. La plupart des entreprises devraient déjà les connaître, et bien des particuliers les connaitront aussi. Ces trois ensembles de règles sont décrits en détail dans le présent document, et il vaut la peine de les lire, ne serait-ce que pour mettre à jour les connaissances existantes.

Cependant, le RGPD instaure plusieurs nouvelles exigences importantes.

Le RGPD en bref

Voici les grands thèmes du RGPD, en particulier en ce qui concerne les exigences de protection des données de la Directive 95/46 de l'UE.

Les droits des personnes — et comment les faire connaître

La législation actuelle de l'UE sur la protection des données (Directive 95/46) accorde aux particuliers des droits à l'égard de leurs données personnelles et décrit les renseignements que les entreprises doivent fournir aux particuliers, y compris de l'information sur ce que l'entreprise a l'intention de faire avec ces données personnelles. Souvent, cette information était communiquée au moyen de déclarations ou d'avis de confidentialité affichés sur un site Web.

Le RGPD va beaucoup plus loin, en accordant des droits supplémentaires qui doivent encore une fois être communiqués aux particuliers. Plus précisément, les personnes doivent être informées qu'elles ont entre autres les droits suivants :

1. porter plainte aux autorités de surveillance, comme l'ICO au R.U.;
2. retirer leur consentement au traitement de leurs données personnelles (voir ci-dessous);
3. accéder à leurs données personnelles et les faire rectifier ou effacer (le « droit à l'oubli ») par l'entreprise, ainsi que par les tiers qui pourraient y avoir accédé;
4. être informées de l'existence de tout mécanisme de traitement automatisé des données personnelles (y compris l'établissement de profils);
5. s'opposer à certains types de traitement, comme le marketing direct et les décisions basées exclusivement sur le traitement automatisé;
6. savoir pendant combien de temps leurs données personnelles seront conservées;
7. obtenir des détails au sujet du responsable de la protection des données, le cas échéant (voir ci-dessous).

De plus, les particuliers ont le droit de demander aux organismes sans but lucratif d'exercer des droits et d'intenter des poursuites en leur nom, de façon semblable au recours collectif à l'américaine.

Consentement

Si vous recueillez des données en fonction du consentement des personnes, bien que la législation de l'UE sur la protection des données ait toujours exigé que ce consentement soit donné de façon libre, précise et éclairée, le RGPD exige une confirmation au moyen d'un énoncé ou d'une autre mesure affirmative claire. Autrement dit, les cases de consentement précochées dans les sites Web, ou le silence ou l'inactivité de la part de la personne après examen d'un énoncé de confidentialité, ne constituent pas un consentement.

De plus, le consentement ne peut pas être universel, ce qui fait qu'une entreprise ne peut pas utiliser le consentement d'une personne à un stade de ses transactions commerciales comme consentement pour d'autres types de traitement de données personnelles. Des consentements distincts sont nécessaires pour différentes opérations de traitement des données.

Enfin, non seulement les personnes doivent-elles être informées qu'elles ont le droit de retirer leur consentement en tout temps, mais il doit également leur être tout aussi facile de retirer leur consentement qu'il l'était de l'accorder.

Les consentements existants donnés par des particuliers devraient être passés en revue pour en assurer la conformité avec les exigences du RGPD. En cas de conflits ou d'ambiguïtés, les entreprises devront établir un nouveau fondement juridique pour le traitement des données (p. ex. c'est nécessaire pour l'exécution du contrat), obtenir un nouveau consentement ou cesser de traiter ces données personnelles.

Droit de déplacer ou de transférer des données personnelles (portabilité des données)

Les particuliers ont maintenant le droit de déplacer, de copier ou de transférer leurs données personnelles d'un endroit à un autre, même à un concurrent. Par exemple, une liste d'écoute pourrait être créée pour un utilisateur par un service de musique, et si l'utilisateur décide de changer de fournisseur, il peut emporter cette liste avec lui. Par conséquent, les données personnelles doivent être dans un format structuré, courant et lisible par machine pour pouvoir être facilement utilisées et partagées.

L'exigence relative à la portabilité réelle des données et à leur facilité d'utilisation par d'autres risque fort d'entraîner d'importants ajustements de TI, et donc des coûts.

Portée élargie

En gros, en ce qui concerne les atteintes à la vie privée, le RGPD responsabilise non seulement l'entreprise qui recueille les données personnelles, mais aussi tout tiers qui traite les données personnelles au nom de cette entreprise, qu'il s'agisse d'une autre entreprise, d'un organisme ou d'un particulier. Cependant, il ne faut pas en conclure pour autant qu'une entreprise peut se contenter de remettre les données personnelles à un tiers puis de fermer les yeux. L'entreprise doit s'assurer que le fournisseur tiers respecte également le RGPD.

De plus, la portée géographique potentielle est élargie au-delà de l'UE pour inclure toute entreprise — ou encore une fois tout tiers traitant des données personnelles en son nom — qui offre des biens ou des services aux résidents de l'UE, ou qui surveille le comportement de ces derniers au sein de l'UE. Il convient de souligner que le fait qu'un paiement soit exigé ou pas pour les biens ou les services ne fait pas de différence, ce qui fait que les ONG sont assujettis au RGPD.

Étant donné que l'UE est un partenaire commercial pour la plupart des pays, la portée élargie du RGPD se traduit par des conséquences pour bien des entreprises dans le monde entier, et elle exigera effectivement la conformité des entreprises qui souhaitent mener leurs activités dans des pays membres de l'UE, que ce soit directement ou en tant que tiers pour d'autres.

Preuve de conformité

Il ne suffit pas de respecter le RGPD. Une entreprise doit prouver qu'elle le fait en vertu de l'exigence du RGPD en matière de « reddition de comptes », ce qui veut dire qu'elle doit respecter certaines exigences plutôt lourdes en ce qui concerne la tenue de dossiers. Plus précisément, des dossiers devraient être tenus à jour pour décrire les activités de traitement*, les demandes d'accès au sujet, les atteintes à la vie privée, les façons dont les consentements sont obtenus et les évaluations des facteurs relatifs à la vie privée (voir ci-dessous).

Cette exigence touche encore une fois les tiers qui traitent des données personnelles au nom d'une entreprise, bien que les exigences ne soient pas aussi détaillées.

** S'applique aux entreprises comptant plus de 250 employés, ou aux entreprises comptant moins d'employés lorsque le traitement effectué est susceptible de mettre en péril les droits et libertés des personnes, n'est pas occasionnel, ou comprend des catégories spéciales de données, comme de l'information sur la santé, la religion ou l'orientation sexuelle.*

La protection des renseignements personnels du début à la fin

Des mesures techniques et organisationnelles doivent être en place tout au long de la durée de vie des données personnelles pour répondre aux attentes en matière de protection des renseignements personnels de la personne — de la création à l'exécution et enfin à la cessation de cette activité. On parle ici de « confidentialité planifiée », c'est-à-dire que les considérations relatives à la vie privée doivent faire partie intégrante de chacun des aspects de ce traitement.

De plus, seules les données personnelles strictement nécessaires à cette fin doivent être effectivement traitées; c'est ce qu'on appelle la réduction des données au minimum, ou « confidentialité par défaut ».

En fait, la mise en œuvre de la confidentialité planifiée et par défaut nécessitera de la formation continue, des vérifications régulières, la réduction au minimum des données recueillies, la restriction de l'accès aux données personnelles aux seules personnes qui ont besoin de savoir et la mise en œuvre de mesures de sécurité techniques et organisationnelles appropriées, comme la pseudonymisation et le cryptage.

Signalement obligatoire des atteintes à la vie privée

En cas de non-respect du RGPD, les entreprises qui recueillent des données personnelles doivent avertir les autorités de surveillance, comme l'ICO au R.-U., dans un délai de 72 heures après en avoir pris conscience. Les tiers qui traitent les données personnelles au nom de ces entreprises doivent en informer l'entreprise dans les meilleurs délais.

Si l'atteinte pose un risque pour les personnes concernées, les entreprises doivent également avertir les personnes touchées sans tarder.

Responsable de la protection des données (RPD)

En vertu du RGPD, les entreprises et les éventuels tiers qui traitent des données personnelles en leur nom devront désigner un responsable de la protection des données (« RPD ») : (i) s'il s'agit d'une entité publique; (ii) si les activités principales de l'entreprise ou des tiers nécessitent la surveillance de personnes à grande échelle; ou si les activités principales consistent à traiter à grande échelle des catégories spéciales de données personnelles, y compris des données liées à des condamnations ou à des infractions au criminel. Le RPD doit avoir une connaissance approfondie de la loi sur la protection des données. Il n'est pas nécessaire que cette personne fasse partie du personnel, et un employé contractuel pourrait remplir ce rôle. Les détails du RPD devront être communiqués à l'autorité de surveillance, comme l'ICO au R.-U.

Peines

Les peines pour non-respect du RGPD sont sévères et pourraient aller jusqu'à 4 % du chiffre d'affaires mondial annuel, ou 20 millions d'euros, le plus élevé des deux. Vous pourriez recevoir une amende même en l'absence de perte réelle de données. Il convient de souligner qu'il n'y a pas d'exclusions ou d'exceptions pour les petites entreprises. De plus, les particuliers ont la possibilité d'intenter un recours collectif demandant une enquête réglementaire officielle lorsqu'une entreprise ne respecte pas le RGPD.

Brexit

Au terme des élections générales au Royaume-Uni en 2017, le gouvernement Conservateur a été réélu pour un mandat de cinq ans. Pendant ce mandat, en particulier en 2019, le R.-U. quittera l'Union européenne. Comme c'est le cas pour tous les pays membres de l'UE, le RGPD s'appliquera au R.-U. d'ici là. Toutefois, à l'annonce de nouvelles lois après les élections, il a été déclaré que les nouvelles lois sur la protection des données feront ce qui suit :

« … mettre en œuvre le Règlement général sur la protection des données et la nouvelle directive qui s'applique au traitement des données par les forces de l'ordre, respecter nos obligations pendant que nous conservons notre statut de pays membre de l'UE et contribuer à bien positionner le R.-U. pour conserver notre capacité de partager des données avec d'autres pays membres de l'UE et à l'échelle internationale après notre départ de l'UE. » (traduction)

Source : discours de la Reine, juin 2017

Par conséquent, il est possible, sans que l'on puisse le présumer pour autant, que le R.-U. soit, après le Brexit, considéré comme pays offrant une protection jugée « adéquate » par la Commission européenne, ce qui voudrait dire qu'il pourrait ne pas être touché par des problèmes potentiels tels que les interdictions relatives aux transferts de protection des données. Surveillez cette rubrique pour en savoir plus long au sujet des décisions à venir.

La nouvelle législation du R.-U. remplace la Data Protection Act 1998, qui était fondée sur la Directive 95/46 de l'UE.

Les principes de base du RGPD

En plus des nouvelles exigences susmentionnées, et à l'instar de la législation de la Directive 95/46 de l'UE, le RGPD réitère trois grands ensembles de règles qui ont trait aux données personnelles. En gros, ces ensembles de règles peuvent être décrits comme suit :

- ***Les principes de protection des données :*** Les données personnelles doivent être traitées d'une manière licite, juste et transparente à l'égard de la personne concernée. Elles doivent être recueillies à des fins précisées, explicites et légitimes, sans autre traitement incompatible avec ceci. Les données personnelles recueillies doivent être adéquates, pertinentes et limitées au strict nécessaire. Elles doivent être exactes et tenues à jour, et toutes les mesures nécessaires doivent être prises pour veiller à ce que les données personnelles inexactes soient effacées ou rectifiées sans tarder. Elles doivent être stockées de façon à identifier la personne sans dépasser les délais nécessaires, et traitées de façon à assurer la sécurité appropriée — y compris la protection contre le vol, la destruction ou les dommages, et l'accès non autorisé ou illicite.
- ***Traitement licite :*** Le traitement des données personnelles n'est licite que si au moins une des conditions suivantes s'applique : la personne a donné son consentement pour une ou plusieurs fins particulières; le traitement est nécessaire pour un contrat dont la personne est partie ou le deviendra bientôt; une obligation légale doit être respectée (p. ex. la présentation des dossiers fiscaux par une entreprise); une tâche est dans l'intérêt du public ou est effectuée dans l'intérêt d'une autorité officielle; le traitement est nécessaire pour des intérêts légitimes (ou ceux d'un tiers) sauf si les intérêts, les droits fondamentaux et les libertés de la personne l'emportent.
- ***Transferts internationaux :*** Le RGPD maintient l'interdiction générale relative à l'envoi de données personnelles à l'extérieur de l'Espace économique européen à destination d'un pays qui n'offre pas de protection adéquate. Au moment de la rédaction, les pays suivants étaient réputés fournir une protection jugée « adéquate »par la Commission européenne : les entreprises américaines qui s'autocertifient en vertu du bouclier de protection des données UE-États-Unis (remarque : cela ne signifie pas pour autant que les États-Unis soient réputés fournir une protection adéquate), Andorre, Argentine, Canada (limité à la LPRPDE), îles Féroé, Guernsey, Israël, île de Man, Jersey, Nouvelle-Zélande, Suisse et Uruguay. En l'absence d'une décision d'adéquation, les transferts peuvent être faits uniquement dans certaines circonstances limitées, y compris avec consentement, l'utilisation de clauses contractuelles publiées par la Commission européenne ou, dans le cas de transferts inter-entreprises, l'utilisation de règles d'entreprises contraignantes.

Mesures que vous pouvez prendre dès maintenant

- Visitez la rubrique sur la réforme de la protection des données du site Web de l'ICO pour en savoir plus long. Vous y trouverez plusieurs guides et des renseignements généraux. Plus précisément, consultez la publication de l'ICO intitulée « Preparing for the General Data Protection Regulation— 12 steps to take now ».
- Passez en revue vos systèmes de collecte et de traitement des données pour vous assurer de leur conformité au RGPD. Pensez à effectuer une vérification en vertu du RGPD d'une perspective juridique et technologique, entre autres.
- Assurez-vous que vos employés et partenaires sont au courant du RGPD et donnez de la formation pour les préparer. N'oubliez pas que le RGPD vous rend également responsable des tiers qui traitent des données personnelles en votre nom.
- Demandez des conseils juridiques pour mieux comprendre les conséquences du RGPD sur votre entreprise.

Pour en savoir plus long, visitez : sage.com/RGPD

Avertissement légal de Sage

L'information contenue dans le présent guide est à titre indicatif seulement. Elle ne vise pas à donner des conseils juridiques et ne doit pas être considérée en ce sens. Nous tenons à souligner qu'il n'y a pas de substitut pour les clients à mener leurs propres enquêtes approfondies ou à obtenir leurs propres conseils juridiques s'ils ont des doutes sur les conséquences du RGPD sur leur entreprise.

Bien que nous ayons fait notre possible pour nous assurer que l'information fournie dans le présent site Web soit exacte et à jour, Sage ne fait aucune promesse quant à l'intégrité ou à l'exactitude de l'information, qui est offerte « telle quelle » sans aucune garantie, explicite ou implicite. Sage n'assume aucune responsabilité pour toute erreur ou omission et n'est pas tenu responsable des dommages (y compris, entre autres, les dommages attribuables à la perte de clients ou de bénéfices) découlant d'un contrat, d'un délit ou de l'utilisation de cette information ou de toute mesure ou décision prise en conséquence de l'utilisation de cette information.