RGPD quelles sont les implications pour les entreprises suisses ?

Nombreuses sont les entreprises suisses qui traitent sans y porter une attention particulière des données personnelles de résidents de l'Union européenne. Or depuis le 25 mai 2018, est entré en vigueur le nouveau règlement européen RGPD qui s'est donné pour objectif de donner aux résidents de l'Union européenne d'avantage de visibilité et de contrôle sur leur donnée personnelle. Ce règlement est –il applicable à votre entreprise ? Et si oui quelles sont les démarches à entreprendre ?

RGPD de quoi s'agit-il ?

Le RGPD a pour objectif la protection des personnes physiques pour ce qui est du traitement de leurs données personnelles. Il s'applique à toute information se rapportant à une personne physique identifiée ou identifiable.[1] En d'autres termes, l'application du règlement est subordonnées à la possibilité d'identifier directement ou indirectement la personne concernée par une ou des données, notamment par référence à un identifiant tel que les nom et prénom, l'adresse e-mail, le numéro de téléphone, des données de localisation, l'IBAN, ainsi que l'adresse IP. En revanche, le règlement ne s'applique ni aux données anonymes, ni à celles qui concernent des personnes morales ou des personnes physiques décédées.

Le règlement ne s'applique pas non plus aux traitements de données à caractère personnel effectués dans le cadre des politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration. Tout comme il ne s'applique pas non plus aux contrôles effectués par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces[2].

Il n'en demeure pas moins que la conception de la notion de donnée à caractère personnel adoptée par le législateur européen est particulièrement large. Le champ d'application de ce règlement englobe par ailleurs toutes les formes que peut prendre l'information, indépendamment du message véhiculé. Il peut s'agir d'image ou de sons, tels que des entretiens téléphoniques, relevant de la vie privée ou professionnelle de la personne concernés, ainsi que certains aspects de sa vie publique.

Concrètement, le RGPD légifère en prenant des mesures de bon sens concernant la sécurité des données à caractères personnel comme minimiser leur collecte, supprimer celles qui ne sont plus utiles, restreindre l'accès à ces données, et les sécuriser tout au long de leur durée de vie utile. Plus les données personnelles sont considérées comme sensibles, plus la législation exige une protection renforcée. Par donnée personnes sensibles, il faut comprendre toute donnée personnelle qui fait apparaître directement ou indirectement des informations liées à la santé, la sphère intime ou l'origine raciale ou ethnique, des mesures d'aide social, des opinions ou

[1] Art. 4 RGPD
[2] Art. 2 RGPD

activités religieuses philosophiques politiques ou syndicales, des poursuites ou sanctions pénales et administratives, des données biométriques et génétiques.

Le traitement de donnée tel que l'entend le règlement européen consiste quant à lui non pas seulement à la collecte, l'utilisation et la suppression de donnée personnelles par l'entreprise, mais concerne également par exemple le simple enregistrement de données personnelles. Au vu de la quantité incommensurable de données électroniques que les entreprises traitent chaque jour, il est aisé de comprendre l'impact d'un tel règlement sur une entreprise qui y serait soumise.

Le RGPD peut –il s'appliquer à des entreprises suisses ?

La principale question est sans nul doute de savoir si le RGPD s'applique à votre entreprise. Après avoir vu le champ d'application matériel avec la notion de données personnelles auxquelles le règlement s'applique, il y a lieu de déterminer l'applicabilité du règlement du point de vue territoriale. Le règlement s'applique en premier lieu aux traitements de données à caractère personnel effectués sur le territoire de l'Union européenne. Si l'impact sur les entreprises suisses disposant de succursales en Europe est évident, il l'est moins pour les entreprises ayant leur siège en Suisse. Etant donné que la Suisse est un pays non membre de l'union européenne, le RGPD n'est pas repris dans le droit suisse. Toutefois, le RGPD connaît un champ d'application extraterritorial et peut s'appliquer à une entreprise ayant son siège en Suisse dans les quatre situations suivantes[3] :

- une société suisse vend des articles en ligne à une clientèle d'un pays membre de l'UE par le biais d'un site internet dédié à la clientèle d'un pays membre de l'UE. Dans ce contexte, il convient d'établir s'il est clair que la société envisage d'offrir des services à des personnes concernées dans un ou plusieurs Etats membres de l'Union. Afin d'établir cette intention, il y a lieu de prendre en compte un faisceau d'indices comprenant, par exemple l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs Etats membres, la possibilité de commander des biens et des services dans cette autre langue, la mention de clients ou d'utilisateurs qui se trouvent dans l'Union européenne, un numéro de téléphone avec un indicatif téléphonique international ou encore l'utilisation d'un domaine internet de premier niveau autre que celui de l'Etat membre où le service est offert.

- Un résident européen navigue sur un site suisse qui intègre un cookie[4] pour traquer le comportement de l'utilisateur.

- Une entreprise suisse sous-traite à une entreprise localisée dans un pays de l'Union européenne le traitement de données personnelles.[5]

---

[3] Art. 3 et 27 RGPD

[4] Le cookie est l'équivalent d'un fichier texte de petite taille, stocké sur le terminal de l'internaute. Ils permettent aux développeurs de sites web de conserver des données utilisateur afin de faciliter la navigation et de permettre certaines fonctionnalités. Les cookies ont toujours été plus ou moins controversés car contenant des informations personnelles résiduelles pouvant potentiellement être exploitées par des tiers.

[5] Par exemple, la filiale suisse d'un groupe stocke toutes les données relatives aux collaborateurs dans une base de données centralisée localisée auprès de la société mère du groupe dans l'UE

- Une entreprise suisse traite des données personnelles en qualité de sous-traitant d'une entreprise localisée dans l'UE.

Au vue de ce qui précède, force est de constater que d'une manière générale, le règlement protège les personnes physiques indépendamment de leur nationalité ou de leur lieu de résidence. Par conséquent, chaque entreprise suisse doit vérifier si elles doivent prendre en compte ou non les nouvelles règles du RGPD.

Quelles sont les conséquences de l'application du RGPD ?

Les entreprises suisses touchées par le nouveau règlement européen devront respecter les devoirs supplémentaires suivants[6] :

a) Informer et obtenir le consentement de la personne concernée

Avant toute collecte et utilisation de données personnelles, il est obligatoire d'annoncer aux personnes concernées ce à quoi elles vont servir et d'obtenir leur consentement. Ces personnes gardent le droit d'accéder à leurs données, de les rectifier, de s'opposer à leur utilisation ou de les supprimer. En effet, en droit de la protection des données de l'Union européenne, contrairement au droit suisse, le traitement de données est de manière générale interdit, aussi longtemps qu'il n'est pas formellement autorisé par une loi ou que la personne concernée n'a pas consenti au traitement. Le consentement n'est valable que si la personne concernée l'a donné librement. Cette dernière doit avoir un vrai choix, c'est-à-dire qu'au moment où son consentement est recueilli, elle ne doit pas être mise devant le fait accompli ou être limitée dans sa liberté de décision. La personne concernée doit être préalablement informée du but de la collecte et du traitement de ses données personnelles, afin de pouvoir donner un consentement non pas général, mais pour chacune des actions liées à ses données personnelles. Le consentement peut être donné aussi bien par écrit que oralement, tant que celui-ci est donné de manière explicite et active. La personne concernée peut par ailleurs en tout temps révoquer son consentement.

b) Assurer le « Privacy by design » et le « Privacy by default »

« Privacy by design » signifie que le responsable de traitement doit s'efforcer de réduire le risque d'atteinte à la personnalité ou de violation de droits fondamentaux de la personne concernée et prévenir de telles atteintes déjà au moment de la planification d'un traitement de données. Un exemple de droit fondamental est le fait que chaque personne a le droit d'accéder à ses données, de les rectifier de les mettre à jour ou de les faire supprimer. Chaque entreprise doit donc s'assurer que les données sont stockées de manière facilement accessible, de façon à pouvoir répondre rapidement à des requêtes d'accès par exemple. Elle doit également prendre toutes les mesures nécessaires pour garantir la sécurité des données que le responsable de traitement a collectées, mais aussi leur confidentialité, c'est-à-dire s'assurer que seules les personnes autorisées y accèdent. Une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu par exemple de les conserver et elles doivent être supprimées.

[6] Art. 5 RGPD

« Privacy by default » est un principe qui signifie que le responsable du traitement des données doit vérifier la pertinence des données et que seules les données strictement nécessaires à la réalisation de l'objectif sont collectées. Le responsable de traitement ne doit donc pas collecter plus de données que ce dont il a vraiment besoin. Il doit également faire attention au caractère sensible de certaines données, s'assurer qu'elles sont exactes et actuelles.

c) Désigner un représentant dans l'UE

Ce devoir tombe lorsque le traitement est seulement occasionnel, qu'il n'implique pas de données sensibles et est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

d) Tenir un registre des activités de traitement

Le responsable de traitement doit tenir un registre des activités de traitement. Ce registre doit comporter les informations essentielles concernant le traitement de données, notamment les catégories de données, le cercles des personnes concernées, les finalités du traitement et les destinataires possibles des données.

e) Déclarer les cas de violation des données à l'autorité de contrôle

En cas de fuite de données, il y a lieu d'informer sans attendre le responsable protection des données de l'entreprise. L'entreprise a en effet 72h pour réagir et notifier une violation susceptible d'engendrer un risque pour les droit et libertés des personnes physiques à l'autorité de contrôle compétente.

A noter qu'en cas de sous-traitance, l'organisation reste responsable des données transmises. Elle doit s'assurer que le sous-traitant respecte les mêmes règles en matière de protection des données.

Quelles sont les conséquences d'une violation du RGPD

Le RGPD reconnait le pouvoir aux autorités de contrôle d'imposer elles-mêmes des amendes administratives lorsqu'un certain nombre de conditions sont réunies. En cas de violation de la protection des données personnelles, l'entreprise s'expose à une amende administrative qui peut s'élever au maximum à 20 millions d'euros, ou dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Est donc déterminant pour calculer l'amende le chiffre d'affaire du groupe et non pas seulement de l'entité concernée par la violation. L'entreprise s'expose également à des sanctions d'ordre organisationnelle comme la suspension voir la suppression de l'autorisation de traitement des données. En cas de violation grave, une cessation complète des activités de traitement de données peut être prononcée par un pays de l'Union européenne. Le règlement met s à disposition tout un éventail de moyens dissuasifs comme l'avertissement, la mise en demeure, la limitation temporaire ou définitive d'un traitement et les rappels à l'ordre avant d'arriver à l'ultime recours de l'amende.

Conclusion

Pour l'employeur suisse devant appliquer les nouvelles règles, il est recommandé au début d'examiner la pratique de l'entreprise en matière de traitement des données et d'identifier quels traitements de données sont entrepris en quel domaine. Dans un deuxième temps, et afin d'optimiser les processus et combler les éventuelles lacunes de l'entreprise, il convient d'examiner de plus près les traitements de données identifiés. Il faut alors se poser les questions suivantes : d'où viennent les données ? Qui les traite ? Sur quel support sont-elles traitées ? Pourquoi sont-elles traitées ? Comment sont-elles traitées ? Quand seront-elles supprimées ? Ou seront-elles conservées ? A-t-on dû demander une autorisation à la personne concernée en vue de leur traitement ? Il y a ensuite lieu de déterminer quels sont les catégories de données personnelles qui doivent faire l'objet d'une protection particulière telles que celles qui permettent de déduire l'origine raciale et ethnique, les opinions politiques, religieuses ou les convictions philosophiques ou encore l'appartenance à un syndicat ou encore les données médicales ou relatives au comportement et l'orientation sexuelle de la personne concernée. Dans la mesure où le règlement est un acte juridique européen, il est conseillé de s'adresser aux autorités de protection des données européenne comme la CNIL, la CPVP belge ou encore la CNDP luxembourgeoise en cas de question.