Paru in HR Today, n° 2, avril-mai 2018 – hrtoday.ch

Protection des données et Union européenne: ce qu'il faut savoir

Alors que l'Union européenne va introduire une nouvelle réglementation sur la protection des donnée en mai prochain (RGPD), voici un rappel du cadre légal suisse et un avant-goût des changements à venir

Texte: Isabelle Dubois, AD HOC RESOLUTION

La protection de la sphère privée est un droit fondamental, ancré dans la Constitution fédérale comme dans la Convention européenne des droits de l'Homme: «Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et de ses communications. Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent».

De là découlent les règles sur la manière dont les données personnelles et les données sensibles doivent être traitées pour ne pas porter atteinte aux droits de la personnalité des personnes concernées, règles que l'on trouve en Suisse dans notre loi fédérale sur la protection des données personnelles (ci-après LPD), et dans l'Union européenne dans une directive qui sera remplacée par un Règlement général dès le mois de mai prochain (ci-après RGPD).

De quelles données parle-t-on?

Les données personnelles regroupent toutes les informations qui se rapportent à une personne physique, qu'elle soit identifiée ou simplement identifiable. Ce sont, par exemple, les coordonnées complètes d'une personne, sa date de naissance, son état civil, un numéro d'immatriculation d'un véhicule, des coordonnées bancaires, le montant du salaire, l'adresse IP, un numéro d'identification, mais aussi les données sensibles que sont les opinions ou activités religieuses, philosophiques, politiques, syndicales, les informations sur la santé, la sphère intime, l'appartenance ethnique, les mesures d'aide sociale, les poursuites, et les sanctions pénales ou administratives.

À chaque fois que de telles données personnelles sont traitées, c'est-à-dire collectées, enregistrées, consultées, mises à jour, exploitées, communiquées, interconnectées, archivées, supprimées, une série de principes s'appliquent.

Les principes à respecter

Le principe de licéité: on ne traite des données personnelles que si l'on a un motif légitime comme une base légale, le consentement de la personne, ou un intérêt privé ou public prépondérant; **le principe de finalité**, selon lequel on collecte des données pour une fin précise, et on les utilise à cette seule fin; **le principe de proportionnalité**: les données sont traitées si elles sont pertinentes, aptes à nous permettre d'atteindre notre objectif, et le moins intrusives possible**; le principe d'exactitude** selon lequel le fichier doit être tenu à jour; **le principe de la bonne foi et de la transparence**: on ne traite pas les données personnelles à l'insu de la personne concernée, et l'on explique dans quel but les données sont collectées; **le principe de la sécurité**, selon lequel le responsable de traitement doit garantir la confidentialité, la disponibilité et l'intégrité des données.

S'y ajoute **le droit d'accès** de toute personne concernée à ses données personnelles, y compris le droit de les faire mettre à jour et de les supprimer si elles ne sont plus pertinentes.

Le nouveau règlement de l'Union européenne

L'union européenne dispose d'une directive sur le traitement des données à caractère personnel, que chaque pays de l'union a dû implémenter dans sa législation. Dès le mois de mai 2018, s'appliquera de plein droit sur tout le territoire de l'union européenne le Règlement général sur la protection des données personnelles (ci-après RGPD). La Suisse, pays tiers, doit mettre à jour sa législation pour continuer d'être considérée comme un pays à la législation adéquate. Les principes applicables sont identiques, même s'il font l'objet d'une terminologie un peu différente. L'objectif du règlement est de renforcer les droits des personnes physiques en matière de protection des données, et de faciliter la libre circulation des données à caractère personnel dans le marché unique numérique, notamment par une réduction de la charge administrative.

Ce règlement crée de nouvelles obligations, comme l'obligation d'annoncer les failles de sécurité dans un délai de 72 heures, et ce qui s'appelle la portabilité des données – pouvoir donner copie des données personnelles d'une personne dans un format clair et lisible par elle – ainsi que l'évaluation d'impact pour certains nouveaux traitements susceptibles d'enfreindre les droits de la personnalité des individus concernés, et les sanctions en cas de violation avérée du règlement sont très fortement augmentées.

Impact sur les entreprises suisses et les RH

Au sein d'une entreprise, beaucoup de données personnelles sont traitées, qu'il s'agisse de celles des clients, usagers ou bénéficiaires, du personnel, des fournisseurs et des partenaires. Parmi les données de l'entreprise, les données personnelles, les données sensibles mais aussi les secrets de fabrication ou d'affaires, sont à traiter de manière circonspecte et plus sécurisée encore.

Dans le domaine des RH, il est utile de revoir le contenu du dossier du personnel, la durée de conservation des divers documents qui s'y trouvent, le mode de destruction cas échéant, le respect du droit d'accès, mais aussi la conformité de divers traitements et applications comme le contrôle d'accès par badge, la géolocalisation dans les véhicules, la vidéosurveillance au sein de l'entreprise, et de revoir la conformité des documents réglementaires, tels que les contrats avec les sous-traitants, les contrats de travail, les règlements internes, les chartes informatiques.

Sur le plan matériel, le règlement s'applique aux traitements de données à caractère personnel automatisés ainsi qu'aux traitements manuels si les données sont contenues ou destinées à être contenues dans un fichier (structuré), à l'exception des fichiers d'usage strictement personnel ou domestique. Sur un plan territorial, il s'appliquera à tout traitement de données à caractère personnel intervenant dans le cadre des activités d'un établissement (exercice effectif et réel d'une activité), d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement lui-même ait lieu ou non dans l'Union; il s'appliquera aussi au traitement de données à caractère personnel relatives à des personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est, lui, pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, qu'un paiement soit exigé ou non. Idem lorsque ledit traitement est lié à l'observation du comportement de ces personnes, dans la mesure où il s'agit de leur comportement au sein de l'Union européenne.

Il faut garder à l'esprit que les entreprises suisses sont avant tout soumises à la législation suisse. Dans le cadre d'un groupe, les établissements stables installés sur le territoire de l'union devront appliquer le règlement européen, de même que les entreprises suisses qui sont sous-traitant d'une entreprise européenne elle-même soumise au règlement. L'entreprise suisse sera également tenue de respecter le règlement, par exemple, si elle décide de faire du commerce en ligne en ciblant expressément les citoyens de l'union européenne, en prévoyant par exemple un paiement possible en euros, et en traduisant le site de vente en ligne dans diverses langues, ou si elle déploie un système de surveillance à large échelle dans un pays de l'union ou qu'elle est active dans le profilage de certaines catégories de citoyens.

L’auteur

Avocate de formation et ancienne juge cantonale, Isabelle Dubois a été la première préposée à la protection des données et à la transparence du canton de Genève. Depuis 2014, elle met son expertise à disposition des organisations via sa société de conseils www.adhocresolution.ch