Conformité RGPD: les défis juridiques

Pour se conformer au règlement sur la protection des données récemment adopté au sein de l'Union européenne, les entreprises ont du travail. Afin d'éviter les sanctions tout en restant concurrentielles et attractives, elles doivent en effet fournir des efforts certains. Décryptage avec l'expert juridique Jürg Schneider, spécialisé dans le domaine des technologies de l'information et Associé au sein de l'Etude Walder Wyss dont il dirige le bureau de Lausanne.

TEXTE **THOMAS PFEFFERLÉ**

Applicable depuis le 25 mai 2018, le nouveau Règlement général sur la protection des données (RGPD) concerne de près les entreprises helvétiques. Pour se mettre en conformité avec les exigences de cette réglementation, de nombreux aspects doivent être observés en détail par les acteurs économiques, notamment dans le secteur digital. Et les défis s'avèrent multiples. Il s'agit d'une part d'éviter les lourdes sanctions financières prévues pour les entreprises non conformes tout en continuant à pouvoir performer et attirer de nouveaux clients et partenaires. Garante du sérieux et de la maîtrise technique d'une société, la conformité RGPD constitue en effet un impératif qui, en cas d'absence, pourrait certainement pénaliser et entraver le développement des affaires des entreprises concernées.

Pour comprendre dans les détails comment implémenter ces nouvelles pratiques au sein de son entreprise, l'avocat Jürg Schneider, spécialisé dans le domaine des technologies de l'information et Associé au sein de l'Etude Walder Wyss dont il dirige le bureau de Lausanne, nous en dit davantage. Interview.

Avant de nous intéresser de plus près aux spécificités juridiques et techniques du RGDP, précisez-nous dans quelles mesures les entreprises helvétiques sont concernées par ce nouveau règlement?
Il est vrai qu'a priori le RGPD, en tant que réglementation européenne, concerne directement les entreprises établies dans les pays membres de l'Union européenne. Ce qui n'est pas le cas de la Suisse. Mais en réalité, le champ d'application de ce nouveau règlement concerne de près les acteurs économiques helvétiques. Le RGPD s'applique en effet à toute entreprise proposant des biens ou services à des personnes physiques établies dans les pays européens. Et cela vaut également pour des biens ou services gratuits. D'un point de vue juridique, les sociétés suisses s'avèrent donc majoritairement concernées à plus ou moins grande échelle. Il faut également considérer la plus-value commerciale que peut apporter la conformité RGPD. Car pour continuer à répondre de manière efficace et séduisante aux souhaits et demandes des clients européens, les entreprises helvétiques ont clairement intérêt à maîtriser tous les aspects du nouveau règlement. Même chose pour continuer à collaborer avec des partenaires européens dans le cadre de projets de grande envergure et pour anticiper les exigences futures de la Loi fédérale sur la protection des données qui est actuellement en révision.

Concrètement, que doivent faire les entreprises pour être conformes avec le RGPD?
Les exigences de la nouvelle réglementation s'avèrent multiples. Dans un premier temps, on peut donc conseiller aux entreprises de commencer par effectuer une analyse de leur activité dans l'optique d'identifier les domaines qui méritent une attention particulière pour

Jürg Schneider
Avocat, Dr. en droit, Associé
Walder Wyss SA, Lausanne

se conformer aux impératifs du RGPD. Cette démarche implique parfois de revoir le business model de la société. Par exemple, si les méthodes et objectifs liés au traitement des données personnelles ne répondent pas aux exigences du règlement. Dans ce sens, les démarches à entreprendre peuvent s'avérer particulièrement importantes et peuvent même engendrer des modifications en profondeur dans le fonctionnement de l'entreprise.

Quelles sont les principales exigences du RGPD à relever?
Les entreprises doivent notamment faire preuve de transparence quant à la nature des données personnelles qu'elles possèdent ainsi qu'à la manière dont elles les traitent. Pour leurs clients et les utilisateurs des services qu'elles proposent, elles doivent donc être en mesure de fournir une information claire et limpide sur ces aspects. En outre, les sociétés doivent permettre à quiconque d'accéder aux données personnelles traitées le concernant. Ensuite, elles doivent être en mesure de pouvoir remettre ou transmettre, voire même supprimer, ces données en fonction des souhaits et demandes des utilisateurs. Sauf exception, les entreprises doivent également tenir un registre des activités de traitement. Tout cela implique évidemment une infrastructure informatique bien gérée. Et en tenant compte de l'envergure et de sa structure, il faut pouvoir dédier suffisamment de ressources au sein de son entreprise à la gestion de ces demandes.

Quelle marche à suivre pourrait-on donner aux entreprises pour implémenter une politique conforme au RGPD?
Le principal point à observer consiste à agir avec pragmatisme. Dans le cadre d'une entreprise déjà familière aux exigences de la nouvelle règlementation, on peut déjà agir de manière ciblée et locale afin de corriger certains aspects des projets en cours. Ce qui peut par exemple se traduire par des actions simples à effectuer dans le cadre d'un nouveau projet pour s'assurer qu'il soit conforme au RGPD dans son intégralité. Pour une entreprise qui serait confrontée pour la première fois à ce règlement, on peut définir quatre étapes clés dans l'implémentation d'une politique conforme. Dans un premier temps, on veillera à identifier clairement le périmètre de ses services, prestations et produits pour identifier dans quelle mesure son activité est soumise à la réglementation. Il s'agit ensuite d'effectuer ce que l'on pourrait appeler du data mapping. Une sorte de scan global de l'ensemble des données personnelles et de leur traitement dans le cadre de l'activité de son entreprise et des mesures déjà mises en place. Cela permet alors de passer à l'étape suivante: l'analyse d'écart. Soit une analyse qui doit permettre de cibler les aspects qui manquent encore pour être en conformité. Dans un dernier temps, il s'agira de mettre en place les différentes stratégies qui permettront de combler ces manques.

Et de quelle manière les entreprises seront surveillées? Y-a-t-il un organe de contrôle dédié à la vérification de la conformité des acteurs économiques?
Les contrôles peuvent être menés de différentes manières. Chaque Etat-Membre de l'Union européenne dispose d'un ou de plusieurs organes de contrôle pour surveiller l'application du RGPD et son respect par les acteurs économiques. Les particuliers directement concernés par ces activités et les associations actives dans le domaine de la protection des données personnelles peuvent directement s'adresser à ces organes pour déposer une réclamation ou demander une intervention en cas de non-respect du RGPD. En Suisse, et s'agissant de la vérification de la bonne application de la Loi fédérale sur la protection des données, le Préposé fédéral à la protection des données et à la transparence fait office de référent légal. Son rôle consiste à conseiller, sensibiliser et veiller à la protection des données personnelles en Suisse. Il est administrativement rattaché à la Chancellerie fédérale. A noter que les particuliers peuvent également ouvrir une procédure auprès des juges civils.

Les entreprises suisses, entre le RGPD et la Loi fédérale sur la protection des données, sont donc soumises à une double règlementation?
En quelque sorte. A terme, dans le cadre du processus de révision actuellement en cours, il est probable que le Parlement opte pour une refonte de la loi fédérale en se calquant sur le modèle du RGPD. Pour l'instant, il faut tout de même préciser que la loi fédérale suisse peut parfois s'avérer plus exigeante que la réglementation européenne. Car son application s'étend aussi aux données personnelles concernant les personnes morales, et non seulement aux données personnelles concernant les personnes physiques comme dans le cadre du RGPD.

La Suisse est-elle soumise à des mesures particulières en tant qu'acteur économique lié à l'Europe sans pour autant faire partie de l'Union européenne?
Oui. Le RGPD stipule précisément que pour les sociétés établies dans des pays hors de l'Union européenne qui sont soumises au RGPD, un représentant doit le cas échéant être désigné dans l'Union européenne, notamment dans l'optique de répondre aux demandes ou réclamations pouvant être émises par des personnes établies dans les Etats-Membres.

Et quelles sont les sanctions prévues en cas de non-conformité avec le RGPD?
Au niveau administratif, les sanctions peuvent être particulièrement sévères. Les amendes prévues peuvent en effet aller jusqu'à 20 millions d'euros, voire même être fixées dans le cadre d'une entreprise à une somme allant jusqu'à 4% du chiffre d'affaires mondial durant le précédent exercice. Outre ces sanctions administratives évidemment lourdes, il faut également considérer les répercussions sur les affaires et la réputation de l'entreprise. Car en termes d'image, la non-conformité au RGPD peut impacter gravement l'activité d'une société, en particulier pour les entreprises qui traitent de grandes quantités de données. Et par conséquent faire fuir ses clients et partenaires.

Avec l'essor du cloud, que peut-on dire quant aux défis juridiques concernant cette nouvelle pratique?
Le fait de ne plus posséder physiquement ses données engendre en effet des enjeux juridiques importants. Parmi eux, il s'agit notamment de veiller à se prémunir contractuellement contre les risques potentiels. Par exemple en cas de faillite de la société qui héberge les données ou encore pour répondre au droit à la portabilité des données dont bénéficient les clients selon le RGPD. En fonction de leurs demandes, il faut en effet, toujours selon le RGPD, pouvoir être en mesure de donner aux clients la possibilité de récupérer les données personnelles dans un format structuré, couramment utilisé et lisible par machine ou même les transférer vers un autre prestataire actif dans l'hébergement.

Et que dire du domaine médical, dont la digitalisation fait également évoluer les pratiques à grande échelle?
Les applications web et mobiles dans le domaine de la santé se multiplient sans cesse, et il faut entre autres veiller aux questions du lieu de stockage, du transfert des données collectées à des tiers ainsi que de leur utilisation pour fixer le prix des produits et primes d'assurances. De même, se pose la question de savoir si une application digitale dans le domaine de la santé est qualifiée le cas échéant de dispositif médical, ce qui la soumettrait à des exigences particulières.

Plus d'informations:
www.walderwyss.com
www.dataprotection.ch

walderwyss