Situation en matière de révision de la loi suisse sur la protection des données (LPD) – entrée en vigueur du règlement général sur la protection des données (UE-RGPD) de l'Union européenne

Dans la première partie de la présente lettre, nous vous informons sur la situation actuelle en matière de révision législative en Suisse. Dans un même temps, dans la deuxième partie, nous évoquons le règlement général sur la protection des données de l'UE qui entrera en vigueur le 25 mai 2018 et qui est en partie aussi pertinent pour les entreprises suisses. Vous trouverez la synthèse assortie de recommandations en page 3.

Situation en matière de révision de la loi suisse sur la protection des données (LPD)

Comme communiqué le 13 avril 2018 (communiqué consultable à l'adresse : https://www.parlament.ch/press-releases/Pages/mm-spk-n-2018-04-13.aspx), la Commission des institutions politiques du Conseil national a décidé de réviser en deux étapes la loi suisse sur la protection des données. La première étape vise à adapter la législation suisse à la directive de Schengen qui se rapporte au traitement des données à caractère personnel dans le domaine du droit pénal. La révision totale de la loi sur la protection des données ne sera abordée que lors de la deuxième étape. Elle s'appliquera à tous les traitements de données par des personnes privées ou par des organes fédéraux. Le Conseil national s'attèlera aux adaptations effectuées dans le cadre de la 1re étape (directive de Schengen) lors de sa session d'été et décidera dans un même temps s'il approuve la division de la révision de la loi sur la protection des données.

Le Conseil national sera la première chambre à débattre sur le projet qui sera ensuite soumis au Conseil des États pour délibérations.

Par conséquent, une entrée en vigueur des dispositions de la loi sur la protection des données révisée pertinentes pour nos membres n'est actuellement attendue que pour la mi-2019 voire plutôt la fin 2019.

Entrée en vigueur du règlement général sur la protection des données de l'Union européenne (UE-RGPD)

L'UE-RGPDD entrera en vigueur dans tous les États membres de l'UE le **25 mai 2018**. La synthèse suivante vise à exposer rapidement les implications pour les entreprises suisses et les éventuelles obligations qui leur incombent.

A. Champ d'application de l'UE-RGPD

Le champ d'application de l'UE-RGPD est vaste et ne se limite pas aux frontières de l'UE. Selon l'art. 3 UE-RGPD, le règlement s'applique aussi aux entreprises suisses si ces dernières traitent des données à caractère personnel de personnes physiques résidant dans l'UE, si l'entreprise suisse

1. propose des produits ou des prestations (gratuites ou payantes) à des personnes concernées de l'UE ou
2. si le traitement des données vise à observer le comportement de personnes concernées dans l'UE.

Pour décider si des **produits et des prestations sont proposés**, on examine si l'entreprise (suisse) a *de toute évidence l'intention* de proposer des produits ou des prestations à des personnes concernées situées dans l'UE.

AGVS/UPSA
Wölflistrasse 5, Postfach 64, 3000 Bern 22
Telefon 031 307 15 15, Fax 031 307 15 16
info@agvs-upsa.ch, www.agvs-upsa.ch

Afin de déterminer si on a une telle intention, on pondère différents facteurs comme l'utilisation d'une langue ou d'une devise utilisée dans un État membre de l'UE mais non en Suisse en combinaison avec la possibilité de commander des produits ou des marchandises dans cette autre langue ou la mention d'autres clients ou utilisateurs se trouvant dans l'UE. Le seul fait que le site Internet d'une entreprise suisse soit accessible dans l'UE ne constitue par contre pas une indication que cette entreprise a l'intention de vouloir y proposer des produits ou prestations.

L'intention **d'observer le comportement de personnes concernées se trouvant dans l'UE** par le traitement de données est par exemple constatée si on suit les activités Internet des personnes concernées (par exemple Google Analytics) et/ou si on utilise des techniques de création de profils de personnes physiques analysant ou prévoyant les préférences personnelles, les comportements ou les habitudes des personnes.

Il est ainsi clair que le champ d'application de l'UE-RGPD est très vaste et que les entreprises suisses doivent elles aussi contrôler si elles doivent respecter ces nouvelles règles. La sélection suivante d'exemples d'obligations résultant de l'UE-RGPD pour les entreprises vise à donner un premier aperçu mais n'est nullement exhaustive au sens d'une liste de contrôle complète.

B. Obligations pour les entreprises

Information et autorisation de la personne concernée

Contrairement à la Suisse, une « interdiction avec réserve d'autorisation » s'applique dans le droit de l'UE en matière de protection des données. Cela signifie que le traitement des données est en général interdit dans la mesure où il n'est pas expressément permis par une loi ou si la personne concernée n'a pas autorisé le traitement. La personne concernée peut à tout moment révoquer son autorisation. Il faut veiller à ce que cette révocation puisse être effectuée tout aussi facilement que l'autorisation.

« Privacy by Design » et « Privacy by Default »

Le principe « Privacy by Design » (protection des données par la technique) signifie que le responsable doit limiter le risque de violations de la protection des données et le prévenir dès la planification d'un traitement des données. Une suppression régulière des données ou leur anonymisation par défaut doit être prévue.

Le principe « Privacy by Default » (protection des données par un réglage par défaut favorisant la protection des données) signifie que seuls les traitements des données requis pour l'usage préconisé sont possibles par défaut. Un site Internet doit par exemple permettre en principe d'effectuer des achats sans avoir besoin de créer un profil utilisateur.

Nomination d'un représentant au sein de l'UE

Les entreprises suisses concernées par le champ d'application de l'UE-RGPD doivent en principe désigner un représentant dans l'UE. Cette obligation disparaît cependant lorsque le traitement est seulement occasionnel, que l'entreprise ne traite pas de catégories de données spéciales et que le traitement n'entraîne pas de risque pour les droits et les libertés de la personne physique.

Registre des activités de traitement

Le responsable doit tenir un registre des activités de traitement au sein de l'entreprise. Il s'agit d'une documentation ou d'un récapitulatif de tous les processus et de toutes les procédures de l'entreprise

dans le cadre desquels l'entreprise traite des données à caractère personnel. Dans ce contexte, il faut indiquer les données essentielles relatives au traitement des données comme par exemple les catégories de données, le cercle de personnes concernées, le but du traitement et les éventuels destinataires des données.

Obligation d'informer « Data Breach Notification »

En cas de violations de la protection des données à caractère personnel, les autorités de surveillance doivent être notifiées sous 72 heures dans la mesure du possible. L'obligation d'informer disparaît uniquement quand le risque pour les droits et les libertés des individus est peu probable. Souvent, les personnes concernées doivent aussi être informées.

Estimation des conséquences en matière de protection des données

Si une forme de traitement entraîne probablement un risque élevé, notamment avec les nouvelles technologies ou en raison de leur nature, de leur volume, de leur contexte ou de leurs buts, une estimation des conséquences en matière de protection des données doit être effectuée. S'il ressort de l'estimation des conséquences en matière de protection des données qu'un traitement des données entraîne un risque élevé sans prise de mesures, les autorités de surveillance doivent être consultées.

Conséquences des violations de la protection des données

L'amende maximale peut atteindre 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires annuel total réalisé dans le monde entier au cours de l'exercice précédent ; selon la valeur qui est la plus élevée. Il s'agit du chiffre d'affaires annuel de tout le groupe et non de celui de la personne morale. Par ailleurs, l'UE-RGPD prévoit un droit sur les recours collectifs permettant désormais aux associations de consommateurs de faire valoir les droits des personnes concernées.

C. Synthèse et recommandations

Le champ d'application de l'UE-RGPD est très vaste. Les entreprises suisses doivent elles aussi contrôler si elles doivent respecter ces nouvelles règles. Les brefs exemples d'obligations résultant de l'UE-RGPD pour les entreprises doivent donner un premier aperçu des conséquences de cette législation de l'UE. Au vu de la gravité des sanctions prévues, il est conseillé aux entreprises suisses de prendre ces nouvelles directives au sérieux.

Il existe déjà des outils gratuits très utiles permettant d'évaluer si son entreprise est concernée par l'UE-RGPD et d'aider à déterminer les mesures éventuellement requises :

- Au sens d'un premier test succinct (env. 6 minutes) : les règles de protection des données « Online Check » d'economiesuisse consultables sur le site : https://www.economiesuisse.ch/fr/datenschutz-online-check.
- Plus détaillé et précis : l'outil d'autoévaluation de la protection des données (« Datenschutz Self Assessment Tool », abrégé DSAT), consultable sur le site (en allemand) : www.dsat.ch. Le DSAT a été développé par David Rosenthal du cabinet Homburger. David Vasella du cabinet Walder lui prête main-forte pour la rédaction.