Kellerhals Carrard

L'essentiel en bref

2/2017

Règlement européen sur la protection des données – Ce que les entreprises suisses doivent savoir

Le Règlement européen sur la protection des données (RGPD) sera directement applicable dans tous les Etat membres de l'UE dans environ une année, soit dès le **25 mai 2018**.

Qu'est-ce que cela implique pour les entreprises suisses? Le RGPD est-il également contraignant pour les entreprises suisses? Quels sont les devoirs qui s'imposent aux entreprises dans le domaine de la protection des données?

Champ d'application du RGPD
Le champ d'application du RGPD est très large et s'étend au-delà des frontières de l'UE. Dans certaines configurations, le RGPD s'applique également aux entreprises ayant un siège en Suisse.

En vertu de l'art. 3 du RGPD, c'est le cas lorsqu'une entreprise suisse traite de données à caractère personnel relatives à des personnes qui se trouvent sur le territoire de l'UE, lorsque les activités de traitement sont liées :

1. à l'offre de biens ou de services à ces personnes concernées, qu'un paiement soit exigé ou non desdites personnes; ou
2. au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'UE.

Pour déterminer si **des biens ou services sont offerts**, on retient comme critère pertinent le fait de savoir si l'entreprise (suisse) offre ouvertement et intentionnellement des produits et services à des personnes dans l'UE. Sont considérés comme des indices d'une telle intention des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'UE. La simple accessibilité du site Internet d'une entreprise suisse depuis l'UE ne constitue par contre pas un indice de l'intention de cette entreprise d'offrir des biens ou des services dans l'UE.

La volonté de procéder à **un suivi de comportement de personnes dans l'UE** est établie par exemple si l'activité de la personne sur Internet est tracée (p. ex. Google Analytics) et/ou si des techniques de profilage de personnes physiques qui permettent d'analyser et de prédire les goûts, comportements et habitudes des personnes sont employées.

Dans ce cadre, il ne fait aucun doute que le champ d'application du RGPD est large et que les entreprises suisses doivent vérifier si elles doivent prendre en compte ou non les nouvelles règles du RGPD. Les exemples choisis qui suivent visent à fournir une première idée des devoirs incombant aux entreprises dans l'UE. Cet exposé ne saurait être considéré comme une liste exhaustive de ces devoirs.

Devoirs des entreprises

A. Information et consentement de la personne concernée
En droit de la protection des données de l'UE, contrairement au droit suisse, s'applique ce que l'on appelle l'interdiction sous réserve d'autorisation. En d'autres termes, 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.

Pour que le consentement de la personne concernée soit valable, un certain nombre d'exigences doivent être réunies :

- **Une décision libre**
  Le consentement n'est valable que si la personne concernée l'a donné librement. La personne concernée 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. Dans ce contexte, il faut signaler en particulier "l'interdiction de couplage", en vertu de laquelle la conclusion d'un contrat ne doit pas être conditionnée à un traitement de données plus large que ce qui est nécessaire pour l'exécution dudit contrat.
- **Une information complète, reconnaissable et certaine**
  Avant de donner son consentement éclairé, la personne concernée doit être préalablement informée du but de la collecte et du traitement de ses données personnelles. A cet effet, toutes les informations pertinentes dans le cas d'espèce doivent être divulguées et être suffisamment concrètes. Le consentement est toujours lié à une finalité spécifique. Il ne peut être donné de manière générale. La personne concernée doit être en mesure de reconnaître l'information et de reconnaître que son comportement sera qualifié de consentement.
- **Forme et comportement actif**
  Selon le RGPD, il suffit que l'entité récoltant les données puisse apporter la preuve du consentement de l'utilisateur. Le consentement ne doit donc pas revêtir une forme particulière et peut également être donné sous forme électronique ou orale. Il doit dans tous les cas être donné explicitement. Partant, un comportement actif des personnes concernées est généralement requis, et d'autres variantes telles un consentement tacite, une case pré-cochée ou la passivité de la personne concernée ne suffisent pas à déduire un consentement. Lorsque le consentement est donné sous forme écrite, l'invitation à consentir doit se faire sous une forme compréhensible et facilement accessible dans un langage clair et simple et être distinct d'autres sollicitations.
- **Révocabilité**
  La personne concernée peut en tout temps révoquer son consentement. Il faut veiller à ce que la révocation puisse intervenir de manière simple, comme le consentement lui-même.

B. "Privacy by design" et "Privacy by default"
Le principe "Privacy by design" (protection des données par des moyens techniques) 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 mo-

ment de la planification d'un traitement de données (p. ex. par de nouveaux systèmes informatiques ou procédures). Il faut prévoir la suppression régulière des données ou leur anonymisation. Est particulièrement importante pour la protection des données l'application systématique du principe de minimisation des données.

Le principe "Privacy by default" signifie que le responsable de traitement est tenu de s'assurer au moyen de paramètres par défaut appropriés qu'en principe seront seulement traitées les données personnelles qui sont nécessaires pour la finalité prévue. Un site Internet doit par exemple permettre de faire des achats sans qu'il soit nécessaire de créer un profil d'utilisateur.

C. Désignation d'un représentant dans l'UE
En principe le responsable de traitement et les sous-traitants qui tombent dans le champ d'application du RGPD doivent désigner un représentant dans l'UE. Ce devoir tombe lorsque le traitement est seulement occasionnel, qu'il n'implique pas de catégories particulières de données personnelles et est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

D. Registre des activités de traitement
Le responsable de traitement doit tenir un registre des activités de traitement. Les sous-traitants doivent tenir un registre analogue de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement. Par registre, on entend tout document ou abrégé concernant les méthodes et procédures de traitement des données personnelles par l'entreprise. Ce registre doit ainsi comporter les informations essentielles concernant le traitement de données, notamment les catégories de données, le cercle des personnes concernées, les finalités du traitement, les destinataires possibles des données.

Une entreprise doit préalablement déterminer dans quelles circonstances des données personnelles de clients, fournisseurs ou employés seront collectées et traitées. Il convient en premier lieu de lister les applications et outils utilisés par l'infrastructure des systèmes de l'entreprise (p. ex. saisie des heures, système de CRM, système d'information RH) dans lesquelles des données personnelles sont stockées. Cela permet de déterminer les flux de données dans l'entreprise et peut également servir de base pour la tenue du registre des activités de traitement. En outre, les entreprises suisses doivent de toute manière préalablement examiner et déterminer si elles tombent dans le champ d'application du RGPD.

E. Obligation de déclarer : notification d'une violation de données personnelles
En cas de violation de données personnelles, le responsable du traitement doit notifier la violation à l'autorité de contrôle compétente si possible dans un délai de 72 heures à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. En général, la personne concernée doit également être informée.

F. Analyse d'impact de la protection des données
Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, une analyse d'impact doit être menée. Lors-que l'analyse d'impact relative à la protection des données indique que le traitement ne pourrait se faire sans présenter un risque élevé, l'autorité de contrôle doit être consultée.

G. Sanction en cas de violation de la protection des données personnelles
L'amende administrative en cas de violation de la protection des données personnelles 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 déterminant le chiffre d'affaires du groupe et non pas seulement de l'entité juridique concernée. En outre, le RGPD introduit la possibilité d'introduire une action collective par laquelle les associations de consommateurs peuvent faire valoir les droits des personnes concernées.

Conclusion et suggestion

Révision du droit de la protection des données en Suisse
Le champ d'application du RGPD est très large et les sociétés suisses doivent vérifier qu'elles ne sont pas soumises aux nouvelles règles. Cela présuppose que des entreprises de toute taille doivent acquérir une compétence certaine en matière de protection des données personnelles et définir la responsabilité à l'interne. Les quelques exemples présentés ci-dessus de devoirs à charge des entreprises ont pour but de donner un premier aperçu des conséquences de la règlementation européenne. Etant donné les sanctions graves auxquelles elles s'exposent, il est conseillé aux entreprises suisses de prendre au sérieux le respect de ce nouveau règlement. Les entreprises concernées doivent en particulier adapter leurs procédures internes, lignes directrices, contrats et déclarations de confidentialité.

Les efforts pour respecter le nouveau RGPD devraient être doublement récompensés : la consultation de l'avant-projet de nouvelle loi fédérale sur la protection des données (LPD) s'est récemment achevée. Un projet révisé est déjà attendu pour l'automne prochain. La protection des données doit également être renforcée en Suisse – en accord avec les règles du RGPD et en exécution de la Convention du Conseil de l'Europe (STE 108) – la transparence du traitement et les possibilités de contrôle des personnes concernées sur leurs données seront renforcées. Bien que l'avant-projet du Conseil fédéral de type "Swiss finish" puisse paraître excessif sur certains points et qu'il est à prévoir que le débat parlementaire ne survive manifestement pas sous cette forme, la problématique de la protection des données devrait, quoi qu'il en soit, gagner de l'importance pour les entreprises suisses.

Nous vous tiendrons volontiers informés de la révision de la loi fédérale sur la protection des données.

Zurich, 25 mai 2017

Daniel Alder, docteur en droit
daniel.alder@kellerhals-carrard.ch

Nicolas Mosimann, docteur en droit, LL.M.
nicolas.mosimann@kellerhals-carrard.ch

Virginie A. Rodieux, LL.M.
virginie.rodieux@kellerhals-carrard.ch

Cornelia Stengel, docteur en droit
cornelia.stengel@kellerhals-carrard.ch