AVOCATS

SCHELLENBERG WITTMER

SEPTEMBRE 2015

Newsletter

Auteur:
Roland Mathys

INFORMATION TECHNOLOGY / DATA PROTECTION

Importance croissante du respect de la protection des données – Guide pratique des programmes de conformité

L'importance des questions relatives à la protection des données s'est considérablement accrue ces dernières années. En conséquence, les entreprises sont plus attentives au respect de la réglementation y relative. Cependant, nombreuses sont les entreprises qui rencontrent des difficultés à adopter des programmes de conformité. Un guide pratique est le bienvenu.

1 INTRODUCTION

La **protection des données** a gagné en importance ces dernières années. Il n'y a pas si longtemps, ce domaine ne jouissait que d'une existence discrète, alors qu'aujourd'hui ces enjeux sont au premier plan.

Cette évolution a plusieurs **causes**: la création de nouvelles technologies connectées aux données personnelles (par ex. les réseaux sociaux, les appareils portables, les logiciels de suivi de la forme physique ou les analyses de "big data"); l'attention particulière des autorités et des tribunaux à l'égard de la protection des données (par ex. les décisions concernant Google Street View en Suisse ou le "droit à l'oubli" dans l'Union européenne); des évènements ponctuels touchant à la protection des données ont été relayés par les médias (par ex. "l'affaire de la NSA").

Cette tendance n'est pas prête de s'arrêter, comme le démontrent les **efforts législatifs** de l'Union européenne concernant l'avant-projet d'un règlement général sur la protection des données, ainsi que la révision corollaire de la loi fédérale suisse sur la protection des données. Par exemple, selon le nouveau règlement européen, les sociétés en infraction pourront être sanctionnées d'amendes jusqu'à 5% de leur chiffre d'affaire au niveau mondial ou, jusqu'à EUR 100 millions, si ce dernier montant est plus élevé.

En conséquence, le **respect de la protection des données** par les sociétés est devenu plus important: il y a quelques années, le respect du droit de la protection des données était considéré comme un obstacle au commerce, coûteux de surcroît. Aujourd'hui, c'est un pilier central de la conformité des entreprises. Le respect des dispositions légales et réglementaires applicables n'est désormais plus une fin en soi, mais tend souvent à gratifier l'entreprise d'un label de qualité en matière de protection des données, ce qui peut être utilisé pro-activement en vue d'une bonne image ainsi qu'à titre d'argument commercial.

Pour de nombreuses entreprises, la conformité en matière de protection des données est une nouveauté juridique. Par conséquent, elles tendent à rencontrer des difficultés

avec le **développement et l'introduction de programmes de conformité adéquats**. Des questions se posent, notamment de savoir comment structurer un tel programme, où commencer, dans quel domaine le besoin est-il le plus urgent, ou encore que doit-on prendre en considération au sein d'une entreprise multinationale ou plus généralement dans un environnement international. Cette newsletter a pour but de répondre à ces questions sans s'y limiter, ainsi que de fournir un plan d'action pour des programmes de conformité en matière de protection des données.

"Jusqu'à présent, la protection des données était principalement considérée comme un obstacle au commerce, coûteux de surcroît. Aujourd'hui, c'est un pilier central de la conformité des entreprises."

2 ANALYSE PRELIMINAIRE

Un programme de conformité débute avec l'établissement d'un **état des lieux en matière de protection des données**. D'un côté, l'entreprise doit déterminer quelles données personnelles sont effectivement traitées; d'un autre côté, les instruments existants de protection des données (par ex. réglementations, procédures, structures) doivent être identifiés.

2.1 ANALYSE DES INFORMATIONS EN LIEN AVEC LES DONNÉES

Il convient tout d'abord de déterminer **quels types de données personnelles** sont collectées et traitées au sein de l'entreprise. Les catégories typiques de données personnelles sont les données des employés, des clients ou encore des fournisseurs. Dans ce contexte, il faut prendre en considération que certains pays (comme la Suisse) ne protègent pas uniquement les données des individus mais également des entités juridiques. Les données doivent être analysées de manière à déterminer si elles comportent des données sensibles (comme des données relatives à la santé) ou des profils de la personnalité, pour lesquels les exigences de protection sont plus élevées. Les données personnelles doivent également être examinées en vue de déterminer si une anonymisation ou une pseudonymisation entre en jeu, deux cas où le droit de la protection des données ne s'applique pas, et à quelles étapes du processus ces mesures doivent être prises.

Pour toute collecte de données, se pose la question de savoir si l'entreprise agit comme **propriétaire de la collecte des données** ("*maître du fichier*" ou "*controller*") ou si elle traite simplement les données au nom d'un tiers ("*processor*"). L'entreprise doit dès lors déterminer quelles opérations de traitement de données ont été confiées à des tiers (par ex. dans le contexte d'un outsourcing). De manière similaire, il doit être déterminé pour tout traitement de données si le fichier correspondant a été déclaré au Préposé Fédéral à la Protection des Données et à la Transparence ("**PFPDT**").

L'analyse des **buts du traitement de données** est d'une importance centrale. En raison du principe de la finalité en matière de protection des données, les données personnelles ne peuvent être traitées que dans les buts qui ont été communiqués à l'individu ou qui lui sont apparents. Les opérations de traitement peuvent être distinguées sur la base du cycle de vie des données, à savoir depuis leur collecte jusqu'à leur évaluation, usage, modification, stockage, publication, rétention et enfin suppression. Il est recommandé d'analyser attentivement les scénarios de traitement typiques des services spécifiques d'une entreprise (dans la division RH par ex. les postulations, les compétences, la gestion des absences, l'usage privé d'internet et les emails, l'évaluation de l'employé, les démissions).

La sécurité des données constitue une composante importante de la protection des données et doit être impérativement inclue dans l'analyse. Les données personnelles sont régulièrement classées confidentielles et protégées des modifications ou d'accès non autorisés par des mesures techniques (par ex. cryptage) et organisationnelles (par ex. restriction d'accès).

Dans un environnement globalisé, le trafic de données est rarement limité à la Suisse. **Le flot de données transfrontière** est la règle, en particulier avec les entreprises actives sur le plan international. Les différents degrés de protection des données au sein des différents systèmes légaux requièrent une analyse à plusieurs niveaux, à savoir les pays dans lesquels les données personnelles sont stockées, depuis quels destinations les données sont-elles accessibles, et enfin quelles données sont transférées, dans quels pays, au sein et hors de l'entreprise.

"Le flot de données transfrontière est la règle, en particulier avec les entreprises actives sur le plan international."

2.2 ANALYSES RELATIVES À LA SOCIÉTÉ

D'un **point de vue organisationnel**, la question se pose de savoir si la société a nommé un conseiller à la protection des données indépendant, dédié à cette tâche. Ce n'est pas une exigence légale mais cela peut conduire à un soulagement administratif certain. De plus, on doit clarifier quelles sont les divisions au sein de l'entreprise qui sont responsables de la protection des données (par ex. le département juridique, compliance, RH, IT).

En fonction de la situation existante, un inventaire de tous les **documents pertinents** en matière de protection des données devrait être dressé. Cela inclut les lignes directrices (par ex. au sein des RH ou de IT), les règlements pour la collecte des données, les accords contractuels (par ex. dans le contexte d'une délégation de traitement de données ou de transfert de données), les déclarations de consentement ou encore les règlements d'entreprise relatifs à la protection des données ("*Binding Corporate Rules*").

Enfin, les **processus** internes de l'entreprise doivent être évalué: quelles mesures de contrôle de qualité ont été prises (par ex. audits, homologations), comment les incidents en lien avec le droit de la protection des données sont traités (par ex. rapport des fuites de données, information ou rectification des requêtes), quels efforts de formation sont fournis (par ex. formation interne ou externe)?

3 IDENTIFICATION, MISE EN PRIORITÉ ET CORRECTION DES DOMAINES A PROBLÈMES TYPIQUES

Dans un second temps, la situation actuelle doit être comparée avec une **situation pleinement conforme** et les domaines dans lesquels des mesures doivent être prises en lien avec la protection des données doivent être identifiés et classés en fonction de leur priorité.

3.1 IDENTIFICATION DES DOMAINES A PROBLÈMES

Les domaines requérant des actions en matière de protection des données dépendent de chaque cas d'espèce. Sur la base de l'expérience générale, **les activités économiques suivantes** peuvent être classifiées comme **sensibles**:

> **IT**: Au sein du département IT d'une entreprise, des lacunes en matière de protection des données émergent souvent lorsque les services individuels sont centralisés à l'interne ou externalisés à un fournisseur externe. Ceci est accentué lorsque les données sont transférées au sein d'un "*cloud*", où l'entreprise ne sait plus (ni ne peut influencer par elle-même) dans quel pays les données sont finalement stockées. Il est ainsi fréquent qu'une action soit requise dans le domaine de la sécurité IT (par ex. manque d'autorisations échelonnées pour l'accès aux données).

> **RH**: Les départements RH engendrent et stockent souvent des données sensibles (par ex. les données relatives à la santé en connexion avec des maladies ou des accidents) ou des profils de la personnalité (par ex. des dossiers de postulation avec des références, des évaluations). Par conséquent, les exigences de conformité en matière de protection des données sont plus élevées. Les domaines sensibles comprennent la phase de recrutement (par ex. la rétention des documents personnels d'une postulation rejetée), la réglementation concernant l'utilisation de l'infrastructure d'une société à des fins privées (internet, email), ou l'utilisation d'infrastructure privée pour des raisons professionnelles ("*Bring Your Own Device*"), la question de la licéité de la surveillance de l'employé, de même que le traitement des données de l'employé après sa démission ou durant ses absences.

> **Marketing/Ventes**: Dans le marketing et la vente, un traitement approfondi des données est effectué, par exemple dans le but d'analyser et évaluer et de regrouper des données personnelles, ou pour des opérations de marketing direct. Ceci peut mettre en danger des principes comme celui de la transparence (l'individu sait-il dans quel but ses données personnelles sont utilisées?), la limitation de la finalité (est-ce que le traitement est légitime dans sa finalité?), et la proportionnalité (le traitement des données se limite-il au nécessaire?).

> **Gestion des dossiers**: La rétention de données est un élément central de la conformité en matière de protection des données. La réglementation de l'archivage des données est souvent inexistante (par ex. délai, forme) ou inappropriée (par ex. uniquement le respect des devoirs de rétention selon le droit commercial).

> **Communication**: le terme communication comprend toutes les opérations de l'entreprise liées aux médias "*offline*" et "*online*", en particulier les sites web, les réseaux sociaux, les messages et les blogs. Une politique de protection des données est désormais habituelle pour les sites internet, mais elle est fréquemment simplement "empruntée" à d'autres sources et n'est ainsi pas adaptée à la présence online spécifique de l'entreprise.

> "Les domaines requérant des actions en regard au droit de la protection des données dépendent de chaque cas d'espèce."

D'autres domaines requérant une évaluation approfondie sont déterminés selon le domaine d'activité spécifique de l'entreprise et de ses secteurs commerciaux (par ex. les données sensibles dans le secteur de la santé, exploitations complètes des données ("*Data Mining*") dans le secteur de la vente au détail).

3.2 MISE EN PRIORITÉ DES ACTIVITÉS

La variété des domaines requérant des actions ne permet souvent pas une mise en œuvre standardisée. Afin de regrouper les ressources, les déficits en matière de protection des données devraient être **éliminés graduellement**. Cela nous conduit à la question de la mise en priorité.

Dans ce but il est recommandé d'utiliser une **grille de risque**, avec comme critères centraux la probabilité d'une violation de la protection des données et les conséquences de la violation (par ex. le nombre de personnes atteintes, la gravité de la violation, la publicité négative et les éventuels dommages à la réputation, le risque d'actions civiles, les procédures administratives conduites par le PFPDT ou même les sanctions pénales).

La mise en priorité peut aussi être influencée par des **facteurs additionnels**, comme la possibilité d'intégrer des mesures spécifiques à des projets en cours ou imminents, ou de mettre en œuvre des solutions réalisables en pratique.

Par ailleurs, les entreprises multinationales doivent décider comment assurer la **conformité dans un grand nombre de pays**. En pareille situation, une approche graduelle par laquelle la mise en œuvre est initiée dans un pays (souvent au siège de l'entreprise ou au lieu de son marché le plus important) et ensuite étendue dans d'autres pays (en impliquant des départements juridiques internes locaux ou des conseils externes), est généralement adoptée.

3.3 LA MISE EN ŒUVRE DES MESURES

Il n'y a pas de réponse simple à la question de savoir quelles mesures spécifiques doivent être mises en œuvre dans le but d'aboutir à la conformité en matière de protection des données. La gamme **des mesures possibles est large** et se compose principalement des éléments suivants:

> **Cessation** complète ou **ajustement** des traitements non conformes de données;

- **information** des personnes concernées, éventuellement doublé de leur accord pour des traitements spécifiques de données;
- établissement ou modification de **clauses contractuelles, lignes directrices ou réglementations de traitement** de données personnelles;
- **déclaration** de fichiers de données au PFPDT;
- mesures organisationnelles telle la nomination d'un **conseiller à la protection des données indépendant**;
- établissement ou ajustement de la documentation des **procédures** requises;
- **information et communication** interne et externe;
- **formation et audit**.

4 OBSERVATIONS FINALES

Les paragraphes qui précèdent démontrent que le respect de la protection des données est devenu un **élément important de la conformité des entreprises**. Les programmes de protection des données contribuent à assurer la conformité aux lois applicables et à récompenser les entreprises avec un label de qualité.

Afin que le programme de conformité aboutisse aux objectifs fixés, il doit être soigneusement planifié, recevoir le soutien juridique approprié et bénéficier de **l'attention requise de la direction**.

Contacts

Le contenu de cette Newsletter ne peut pas être assimilé à un avis ou conseil juridique ou fiscal. Si vous souhaitez obtenir un avis sur votre situation particulière, votre personne de contact habituelle auprès de Schellenberg Wittmer SA ou l'un des avocats suivants répondra volontiers à vos questions:

A Genève:

Philippe Ducor
Associé
philippe.ducor@swlegal.ch

Virginie A. Rodieux
Avocate
virginie.rodieux@swlegal.ch

A Zurich:

Roland Mathys
Associé
roland.mathys@swlegal.ch

Andrea Mondini
Associé
andrea.mondini@swlegal.ch

SCHELLENBERG WITTMER SA / Avocats

ZURICH / Löwenstrasse 19 / Case postale 1876 / 8021 Zurich / Suisse / T +41 44 215 5252
GENÈVE / 15bis, rue des Alpes / Case postale 2088 / 1211 Genève 1 / Suisse / T +41 22 707 8000
SINGAPOUR / Schellenberg Wittmer Pte Ltd / 6 Battery Road, #37-02 / Singapour 049909 / www.swlegal.sg

www.swlegal.ch