_swissprivacy.law

Documentation externe et interne aux entreprises en matière de protection de données

Jürg Schneider et Hugh Reeves, le 2 mars 2021

Les démarches à entreprendre pour respecter le droit de la protection des données sont diverses. Celles-ci peuvent être explicitées dans les nombreux documents qu'exigent aussi bien le droit suisse qu'européen ou qui, sans être obligatoires, sont tout de même souhaitables. Le présent article revient sur les documents les plus importants sous l'empire de la nouvelle Loi sur la protection des données et du RGPD.

I. Introduction

Les règles en matière de protection des données revêtent une grande importance pour les entreprises. En effet, tant les obligations légales et réglementaires que le risque réputationnel en cas de manquements poussent les acteurs économiques à mettre l'accent sur leurs pratiques en matière de protection des données.

De nombreuses juridictions, dont en particulier l'Union européenne et la Suisse, ont révisé leur réglementation en matière de protection des données, afin notamment de l'adapter aux nouvelles technologies et de renforcer la protection de la sphère privée des individus.

Malgré l'importante médiatisation des thématiques ayant trait à la protection des données et des conséquences en cas de violations des dispositions applicables, un flou subsiste. En effet, nombreux sont les acteurs qui, malgré leurs bonnes intentions, ne savent quelles démarches mettre en œuvre afin de respecter le droit applicable.

Le présent article vise à lever une partie du voile en passant en revue les différents documents, politiques et directives exigées ou souhaitables sous la version révisée de la Loi fédérale sur la protection des données (nLPD) et le Règlement général sur la protection des données de l'UE (RGPD).

D'emblée, il convient de relever que la nLPD, que le Parlement fédéral a adoptée le 25 septembre 2020, n'appartient pas encore formellement au droit positif. Son entrée en vigueur devrait survenir en deuxième moitié d'année 2022, de sorte qu'il apparaît d'ores et déjà opportun de traiter dans cet article de la version révisée et non de la version actuelle de la LPD, toute référence à la LPD se voulant une référence à sa version révisée. Le RGPD est

déjà en vigueur et pleinement effectif depuis le 25 mai 2018. Par rapport à cet instrument, il est souvent nécessaire, même pour des entreprises basées en Suisse, actives principalement en Suisse et sans filiales ou succursales à l'étranger, de tenir compte du RGPD lorsqu'elles cherchent à implémenter la législation pertinente en matière de protection des données, ce au vu notamment du champ d'application étendu du RGPD.

II. Catégories de documents

Nous proposons de distinguer la documentation interne à l'entreprise de la documentation que l'entreprise partage avec des acteurs externes, tels que les clients concernés ou les autorités. Cette distinction n'est cependant pas nécessairement reflétée dans les actes normatifs. Ainsi, une entreprise pourrait par exemple choisir de publier sur son site internet également (certaines de) ses directives internes, par souci de transparence ou à des fins de marketing.

En revanche, nous ne distinguerons pas strictement entre la documentation exigée selon la LPD révisée et celle requise par le RGPD. En effet, le champ d'application du RGPD étant large, il n'est pas recommandable selon nous d'entreprendre un exercice d'implémentation de la LPD révisée qui ne tiendrait pas compte des exigences du RGPD. De plus, certains documents ne sont pas strictement exigés par la nLPD et par le RGPD, mais servent à mettre en œuvre les exigences souvent formulées en termes généraux de ces actes normatifs. Enfin, certains documents sont mentionnés tant par la nLPD que par le RGPD mais avec des attributs légèrement différents (par exemple le registre des activités de traitement).

La liste qui suit ne se veut pas exhaustive, tant il est possible d'avoir un nombre quasi illimité de politiques et de directives internes. En effet, les entreprises sont libres d'avoir des politiques et des directives pour tout sujet qui leur paraît important après avoir effectué une analyse de conformité de leur modèle d'affaires et de leurs activités de traitement avec la législation pertinente. Dans ce contexte, la taille de l'entreprise concernée ainsi que son secteur d'activité nous paraissent jouer un rôle primordial. Ainsi, une grande entreprise pourrait choisir d'avoir une directive interne très précise en matière d'accès à divers types de données (personnelles) indiquant dans les moindres détails quelles personnes sont autorisées à accéder à certaines données, tandis qu'une petite entreprise pourrait éventuellement se contenter d'une directive interne moins détaillée. D'autre part, une entreprise spécialisée dans la fourniture de services en *cloud* aura besoin de régir clairement ses activités de traitement de données personnelles, tandis qu'une entreprise active dans le secteur de la construction pourra se passer d'une réglementation interne détaillée, ce qui ne veut pas pour autant dire qu'elle n'est pas soumise aux obligations légales en matière de protection des données.

A) Documents externes

1. Politique de confidentialité : Il s'agit probablement du document le plus « célèbre » en matière de protection des données, soit la partie émergée de l'iceberg. Rares sont les entreprises responsables du traitement qui n'ont (toujours) pas de politique de confidentialité. Nombreuses, en revanche, sont celles qui disposent d'une politique de confidentialité ne correspondant pas à leurs pratiques réelles en matière de traitement des données.

La politique de confidentialité doit expliquer de façon claire et transparente notamment l'identité et les coordonnées de l'entreprise responsable du traitement, les activités de traitement auxquelles l'entreprise responsable du traitement se livre, les destinataires ou les catégories de destinataires auxquels les données personnelles sont transmises, une éventuelle communication des données personnelles à l'étranger et les droits des sujets. En réalité, le contenu des politiques de confidentialité est, de par la loi, relativement étoffé, de sorte qu'il n'est pas toujours aisé de fournir des renseignements clairs et compréhensibles, ce qui peut exposer le responsable du traitement à des reproches de manque de transparence…

2. Registre des activités de traitement : Les responsables du traitement et les sous-traitants doivent en général disposer d'un registre des activités de traitement. Il s'agit, contrairement à la catégorisation ici proposée, d'un document interne à l'entreprise. Toutefois, les autorités disposent (en particulier sous le RGPD) de la faculté d'accéder à ce registre, de sorte qu'il sert non seulement un but de fonctionnement interne, mais également une finalité administrative et donc externe.

Ce registre doit en particulier détailler le but du traitement (pour le responsable du traitement), les catégories de données personnelles traitées, ainsi que fournir des informations sur les transferts internationaux, les durées de conservation des données (pour le responsable du traitement) et un descriptif des mesures techniques et organisationnelles en place pour assurer la sécurité des données.

3. Analyses d'impact relatives à la protection des données personnelles : Lorsque le responsable du traitement considère qu'une activité de traitement envisagée est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées, il doit en amont procéder à une analyse d'impact s'agissant du traitement en question. À l'instar du registre des activités de traitement, les analyses d'impact ne sont en principe pas partagées avec des tiers et il s'agit donc d'un document interne à l'entreprise. Toutefois, il peut être nécessaire de partager une ou plusieurs analyses d'impact (ou leurs résultats) avec l'autorité de protection des données compétente, notamment dans le cadre

d'une consultation, laquelle n'est pas une procédure d'approbation toutefois.

4. Formulaires de consentement : Dans certains cas, les responsables du traitement nécessitent, comme fondement à leurs activités, d'obtenir le consentement des personnes concernées. Or ledit consentement doit être libre et éclairé, voire soumis à des conditions complémentaires lorsqu'il s'agit de données sensibles, par exemple médicales. Un formulaire de consentement préétabli, détaillant notamment les droits des personnes concernées, permet à l'entreprise de mieux gérer ses processus tant internes (par exemple l'enregistrement du consentement dans un registre interne) qu'externes (par exemple sa relation avec ses clients).

B) Documents internes

1. Politique de protection des données : Il est nécessaire pour le responsable du traitement de s'assurer que ses activités de traitement sont conformes aux exigences légales. Cela implique en particulier d'avoir en place des mesures techniques et organisationnelles, dont un des buts est notamment d'assurer la sécurité des données. Le responsable du traitement doit dès lors établir une politique interne de protection des données. Son contenu dépend toutefois fortement de l'analyse que l'entreprise effectuera au préalable portant sur son modèle d'affaires et ses activités de traitement, de sorte que le contenu de la politique ne saurait être résumé de façon abstraite.

2. Directive en matière d'accès aux données : De nombreuses entreprises cherchent à protéger non seulement les données elles-mêmes, par exemple par le biais de technologies de chiffrement, mais également à restreindre le personnel qui peut avoir accès à ces données. Cela suit typiquement un raisonnement de type « *need-to-know* » et peut souvent résulter en une liste de personnes ou de postes/rôles spécifiques.

3. Directive pour la mise en œuvre de pratiques de protection des données dès la conception (*privacy by design*) et par défaut (*privacy by default*) : Des mesures, y compris des directives, doivent être instaurées, afin d'assurer que la protection des données est prise en compte dès la genèse d'un nouveau projet impliquant un traitement de données personnelles, par exemple en assurant que seule la quantité minimale des données soit traitée. En outre, la protection des données doit avoir lieu par défaut de sorte que les paramètres de base du traitement ne doivent pas impliquer de traiter plus de données personnelles que nécessaire.

4. Directive détaillant les marches à suivre en cas de demandes d'accès (ou de correction ou

suppression des données personnelles) : Il est de plus en plus fréquent que des personnes demandent l'accès à leurs données personnelles. Les entreprises se doivent de pouvoir analyser la situation rapidement et y réagir de manière appropriée, sous peine d'encourir des amendes ainsi qu'un risque réputationnel. Des directives présentant des marches à suivre claires facilitent ainsi grandement la tâche des entreprises qui reçoivent une demande d'accès. Il en va de même en présence de demandes visant la correction ou la suppression de données personnelles.

5. Directives détaillant la marche à suivre en cas de violation de la sécurité des données personnelles (*data breach*) : Les sous-traitants doivent annoncer les violations de la sécurité de données aux responsables du traitement, c'est-à-dire à leurs partenaires contractuels, par exemple les clients de fournisseurs de services de stockage informatiques. Le responsable du traitement doit à certaines conditions annoncer ces violations à l'autorité compétente et, éventuellement aux personnes concernées elles-mêmes. En raison des brefs temps de réaction accordés par les actes normatifs applicables, il est souhaitable que les acteurs concernés disposent au préalable d'une directive qui détaille les responsabilités et les procédures à suivre pour procéder aux éventuelles annonces à temps et de façon claire et complète.

6. Politique de protection des données envers les employés et directive réglant le traitement des données par les employés : La relation de travail implique nécessairement le traitement de données personnelles. Les employeurs, responsables du traitement, se doivent d'informer clairement leurs employés et également d'attirer leur attention sur les éventuelles conséquences d'activités sortant du cadre des rapports de travail. Ainsi, en plus d'une politique de protection des données réglant le traitement par l'entreprise des données personnelles concernant ses employés dans le cadre du rapport de travail, il est fortement recommandé de mettre en place une directive sur l'usage des outils informatiques au bureau par les employés, réglementant entre autres les éventuels e-mails privés, l'utilisation d'internet, etc.

7. Politique de périodes de rétention : Les données personnelles ne peuvent être gardées indéfiniment. Cependant, elles doivent souvent être gardées pendant une certaine période. Il en va ainsi des pièces comptables qui doivent être gardées pendant dix ans, tandis que des données relatives à une postulation d'emploi non retenue doivent, sauf exception, être effacées promptement après la décision de ne pas donner suite à la candidature. Une documentation interne énumérant les différentes périodes de rétention des données concernées et pertinentes pour l'entreprise permet d'assurer une conformité aux exigences légales sur la durée.

8. Vérification de la mise en œuvre effective des mesures de protection des données : Un

constat pratique récurrent est qu'il y a un décalage entre les différentes politiques et directives en matière de protection des données et la pratique réelle de l'entreprise concernée. Outre des activités d'audit et de contrôle interne, une documentation permettant à l'entreprise de suivre la mise en œuvre de ses mesures d'implémentation des règles en matière de protection des données peut s'avérer utile.

III. Conclusion

Les listes qui précèdent ne sont nullement exhaustives. Ces documents permettront à l'entreprise concernée de réduire certains risques de non-conformité avec le RGPD et la nLPD. Elles permettent également d'avoir un certain confort dans les affaires au quotidien.

Il convient de préciser que, même si les règles applicables peuvent paraître de prime abord relativement rigides, l'implémentation du droit de la protection des données laisse une grande liberté et nécessite une analyse au cas par cas. Ainsi, les activités de traitement des données personnelles effectuées par l'entreprise auront un grand impact sur la documentation à adopter.

Cela dit, force est de constater que s'agissant des différents types de documents à adopter et leur contenu, certaines pratiques et standards ont été élaborés. Pour limiter le temps, l'effort, ainsi que les coûts, nous recommandons aux entreprises de ne pas « réinventer la roue » et de se baser sur les pratiques et standards déjà établis et ayant fait leurs preuves.

Proposition de citation : Jürg Schneider / Hugh Reeves, Documentation externe et interne aux entreprises en matière de protection de données, 2 mars 2021 *in* www.swissprivacy.law/59