_swissprivacy.law

Conseils pratiques pour la mise en place d'un programme de gestion de la protection des données

Juliette Ancelle et Alexandre Jotterand, le 30 octobre 2020

Nous mettons en ligne, de manière périodique, les contributions d'auteurs externes nous ayant fait l'honneur d'accepter d'accompagner le lancement de Swissprivacy. Nous accueillons cette semaine la contribution de Juliette Ancelle, avocate associée au sein de l'Étude id est avocats Sàrl et Alexandre Jotterand, avocat collaborateur au sein de la même étude

Le programme de gestion de la protection des données (*data protection management programme* ou DPMP) peut se définir comme un cadre mis en place au sein d'une entreprise relevant d'une approche structurée et multidisciplinaire de la protection des données. Son utilité dépasse souvent la conformité réglementaire (*compliance*), bien que celle-ci demeure sa fonction principale. Ainsi, de nombreuses entreprises étendent le cadre de leur DPMP au-delà des strictes obligations réglementaires, notamment en se conformant volontairement à des standards édictés (p. ex. la norme ISO/IEC:27001 ou le NIST Privacy Framework) ou en alignant toutes leurs activités sur les standards les plus élevés (souvent ceux du RGPD), indépendamment des lois qui leur sont applicables. Ces démarches peuvent viser à simplifier les processus au sein de l'entreprise ou à servir de *différentiel concurrentiel*, en accroissant la confiance des consommateurs et en renforçant la réputation de l'entreprise. Elles permettent également de limiter les risques de violation de la sécurité des données, de responsabilité ou de procès et, dans l'ensemble, d'apporter un retour sur investissement intéressant pour les entreprises.

S'il n'est pas mis en place correctement, un DPMP peut toutefois être inefficace (car il n'est pas suivi), voire être contre-productif, en bloquant les activités de l'entreprise. Cet article liste nos conseils pratiques, regroupés en cinq étapes, afin de mettre en place un DPMP réussi.

1. Définir des objectifs adaptés

La première étape clé dans la mise en place d'un DPMP consiste à déterminer le « contexte » de l'entreprise, c'est-à-dire son positionnement dans l'écosystème de protection des données (lois applicables et autres référentiels auxquels l'entreprise adhère volontairement), ainsi que

son exposition et appétence aux risques. Ces éléments sont essentiels pour calibrer le programme et prioriser les actions à entreprendre. Un programme mal calibré ou trop ambitieux risque d'échouer. Il est donc souvent préférable de fonctionner par étapes et de fixer dans un premier temps des objectifs plus modestes, qui seront mieux adaptés aux besoins de l'entreprise et ainsi mieux acceptés par les équipes *business*.

Il est conseillé de définir la vision et mission de l'entreprise en lien avec la protection des données (*company vision* et *mission statement*), en résumant dans un document de façon claire et concise (30 secondes de lecture au maximum) la position de l'entreprise en matière de protection des données, afin de guider la mise en place et l'implémentation du DPMP.

2. Définir les rôles et responsabilités au sein de l'entreprise

La gestion d'un DPMP ne peut pas être intégralement déléguée à une seule personne, ou uniquement à un service (souvent le service juridique). Elle nécessite une forte collaboration au sein de l'entreprise et l'allocation des ressources nécessaires. Naturellement, la répartition des rôles dépendra du type d'entreprise, de son fonctionnement (plus ou moins centralisé) et de sa taille : alors que les équipes des grandes entreprises seront composées de juristes, spécialistes IT et des responsables des départements les plus concernés (*RH*, *Marketing*, *Procurement*, etc.), les entreprises plus petites s'appuieront principalement sur une seule personne, en veillant à ce qu'elle puisse bénéficier de l'assistance de ses collègues. Toutes les entreprises (grandes et petites) devraient toutefois s'assurer de l'appui d'un membre de la direction (souvent désigné *project sponsor*), qui assume la responsabilité du succès du programme et s'assure que les ressources suffisantes soient affectées au projet.

3. Analyser les flux de données (*data mapping*) et identifier les lacunes (g*ap analysis*)

Une approche structurée de la protection des données nécessite une connaissance précise des informations qui sont traitées par l'entreprise – de ce qu'elle en fait et à qui elle y donne accès – pour l'ensemble du cycle de vie de la donnée (de sa collecte à sa destruction ou son anonymisation). Pour ce faire, la première étape consiste à dresser un inventaire de tous les services et supports de données – qu'ils soient physiques (ordinateurs, *flash drives*, smartphones, photocopieuses et autres équipements) ou virtuels (logiciels, services web et autres solutions) – qui traitent des données personnelles de l'entreprise. Les sous-traitants ayant accès à des données de l'entreprise doivent également être identifiés. Lors de la constitution

de cet inventaire, une approche dynamique devra être privilégiée, dans la mesure où ce document sera amené à être régulièrement mis à jour au sein de l'entreprise et il s'agira donc d'adopter un format flexible et intégrant éventuellement les outils nécessaires à une mise à jour facilitée.

Une fois cette étape achevée, les flux de données, ainsi que les activités de traitement (ce qui en est fait et pourquoi), doivent être analysés (*data mapping*), au regard des exigences posées par les lois applicables et autres référentiels. A ce sujet, il convient de relever qu'il ne s'agira pas uniquement ici d'identifier les flux de données mais bien de comprendre les projets commerciaux dans lesquels ces flux s'insèrent, et les objectifs visés par ces projets. Ceci effectué, la dernière étape consiste à dresser la liste des lacunes constatées par rapport aux référentiels sélectionnés (*gap analysis*) et à prioriser les mesures à entreprendre pour les résoudre, compte tenu des objectifs définis dans le cadre de l'étape 1 (*action plan*).

4. Implémenter le programme

L'étape 4 consiste à implémenter les mesures définies, qui peuvent notamment porter sur la correction de certaines activités (cesser/modifier un traitement, sécuriser certains outils), la révision ou la conclusion de nouveaux contrats et la rédaction de politiques et directives internes. Les mesures d'implémentation doivent s'étendre à la gestion des sous-traitants, en s'assurant qu'ils traitent les données en conformité avec le cadre légal applicable et les contrats conclus.

Les lois sur la protection des données imposent souvent une réaction rapide à certains évènements, avec potentiellement des conséquences importantes, tant réputationnelles que financières. Il en va ainsi des demandes de droit d'accès, qui doivent être identifiées et traitées dans des délais courts, ainsi qu'en matière de sécurité. Sur ce dernier aspect, l'entreprise doit non seulement limiter les risques de violations de la protection des données, mais également se préparer à devoir résoudre et notifier l'incident le plus rapidement possible. Pour se préparer au mieux, il est donc conseillé de concevoir à l'avance un *Incident Response Plan*.

5. Assurer le suivi

Un bon DPMP doit être connu des personnes impliquées et continuellement mis à jour. Des formations internes doivent donc être mises sur place pour s'assurer que chaque employé est conscient de ses obligations en matière de protection des données. Le programme doit également être régulièrement audité et mis à jour, en fonction notamment de développements externes (p. ex. réformes législatives) ou internes (p. ex. un nouveau produit ou

nouveau marché).

Enfin, comme indiqué dans l'étape 1, un programme n'est jamais exhaustif dès le début. Les objectifs et priorités initialement fixés doivent donc être périodiquement revus et améliorés.

Proposition de citation : Juliette ANCELLE / Alexandre JOTTERAND, Conseils pratiques pour la mise en place d'un programme de gestion de la protection des données, 30 octobre 2020 *in* www.swissprivacy.law/21