Commentaire explicatif sur les « Directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir »

Conformément à l'art. 4 al. 3 de l'ordonnance sur la certification de protection des données (OCPD), il appartient au Préposé d'émettre des directives sur la base essentielle de la norme ISO/CEI 27001:2005 « Exigences pour les systèmes de gestion de sécurité de l'information (SGSI) », en conservant bien entendu **l'accent sur la protection des données**.

Pour ce faire, une première étape consiste à reprendre d'ISO 27001 les exigences génériques pour les systèmes de gestion, elles-mêmes issues de celles fondamentales d'ISO 9001 pour la gestion de la qualité, comme en témoigne l'annexe informative C d'ISO 27001. **L'accent sur la protection des données** se manifeste partiellement dans deux chapitres introductifs, à savoir « 2. Références normatives" et "3. Termes et définitions", substantiellement dans le chapitre **"4. Système de gestion »** avec en particulier son point **4.2.1 « Établissement du système de gestion»**, et de manière purement interprétative dans les deux premiers « 0. Introduction », « 1. Domaine d'application » et les quatre derniers chapitres « 5. Responsabilité de la Direction », « 6. Audits internes », « 7. Revue de Direction » et « 8. Amélioration ».

La difficulté majeure a consisté à mettre **l'accent sur la protection des données**, plutôt que sur la seule sécurité de l'information. Par le biais de l'art. 7 qui couvre les exigences de sécurité des données imposées par la LPD, on peut fort heureusement considérer la protection des données comme un objectif global remplaçant par extension celui de la *sécurité de l'information* visé par ISO 27001. On vise ainsi l'établissement d'un **système de gestion de la protection des données**, qui prescrit entre autre une **politique du système de gestion de la protection des données (SGPD)**, une **sélection de mesures** pour le traitement des non-conformités, une **déclaration d'applicabilité** des mesures implémentées avec justification de celles qui auraient été exclues, un **plan de traitement des non-conformités**, une **surveillance/revue des violations ou incidents** de protection des données et des **actions correctives ou préventives** pour améliorer le SGPD.
Le nœud de cette accentuation se situe sans conteste dans la procédure de *gestion des risques* qui préside à l'établissement et à la gestion d'un SGSI. Si une telle gestion des risques est bien adaptée à des objectifs « internes » de sécurité de l'information, elle ne l'est par contre pas du tout pour des exigences « externes » de protection des données. Un SGPD doit donc impérativement associer une **gestion de la conformité** à la *gestion des risques*, cette dernière étant maintenue pour les aspects de sécurité des données (cf. principe/objectif/article 7).

Concrètement, une **méthode d'appréciation de non-conformité** consiste en une **analyse de non-conformité** qui aboutit après identification des sources de non-conformité à une **estimation de non-conformité**, en règle générale sur une échelle à deux valeurs : non-conformité mineure ou majeure.

Il n'y a par contre **pas d'évaluation possible de non-conformité**, puisqu'une non-conformité ne saurait être ni acceptée (aucune non-conformité résiduelle, à partir d'un hypothétique niveau jugé acceptable), ni transférée ! En d'autres termes, une non-conformité doit nécessairement être **traitée** par l'adoption de mesures appropriées ou alors **évitée** en renonçant par exemple au traitement incriminé.

Dans un second temps, il s'est agi de reprendre l'annexe normative A d'ISO 27001 qui est en fait constituée de la table des matières de la norme ISO/CEI 27002:2005 plus connue sous le nom de « Code de pratique pour la gestion de la sécurité d'information ». Celui-ci comprend 15 chapitres, dont les 11 derniers forment des « groupes de contrôle », eux-mêmes subdivisés en 39 « objectifs de contrôle » conduisant à un total de 133 « mesures de contrôle ». L'**accent sur la protection des données** est ici tout tracé, étant donné la **mesure 15.1.4** qui porte sur la « Protection des données et confidentialité des informations relatives à la vie privée » et qui prescrit en substance que « celles-ci doivent être garanties telles que l'exigent la législation, les règlementations applicables, et les clauses contractuelles le cas échéant ».

Dans l'optique d'une certification d'organisation ou de procédure de protection des données, cette seule mesure très générale doit à l'évidence être détaillée et subdivisée en objectifs, eux-mêmes réalisables par des mesures concrètes de protection. Ceci est actuellement prévu dans le cadre d'un « **Guide d'implémentation** » ou encore « Code de pratique pour la gestion de la protection des données », annexé aux « **Directives sur les exigences minimales qu'un SGPD doit remplir** ». À l'instar de l'OCDE et d'autres pays tels l'Australie, le Canada et la Grande-Bretagne, nous avons retenu « **9 principes généraux de la loi sur la protection des données** » comme objectifs essentiels de ce « Guide d'implémentation des directives pour SGPD ». Ces objectifs se traduisent à l'heure actuelle par 20 mesures concrètes de protection des données, reprenant de manière non exhaustive les principales exigences issues de la loi ou de son ordonnance d'application. Afin de faciliter la lecture et la compréhension de cette annexe, chaque mesure est structurée conformément au standard ISO 27002, dont elle constitue une extension spécifique pour la protection des données. Tout comme la mesure 15.1.4 renvoie elle-même les SGSI aux SGPD, il faut encore relever que le 7^{e} objectif « Sécurité des données » avec ses mesures associées n'est rien d'autre que le renvoi des SGPD aux SGSI. Parmi les 133 mesures de sécurité proposées par ISO 27002, une présélection des plus pertinentes pour la protection des données a été effectuée.

S'il n'est bien sûr pas question d'imposer une certification SGSI pour obtenir une certification SGPD, le niveau de **reconnaissance d'une certification SGSI** préexistante, notamment par rapport aux exigences de « Sécurité des données », devra être évalué et décidé de cas en cas par le certificateur. S'agissant de l'accréditation effectuée par le SAS, il est par contre possible que l'accréditation SGPD soit prévue comme une extension de l'accréditation SGSI (ISO 27001), étant donné la référence étroite et explicite aux exigences de cette norme.

Pour tous les acteurs concernés (accréditeurs, certificateurs, certifiés, auditeurs, contrôleurs, etc.), il faut souligner que l'actuel lien étroit avec les normes internationales ISO 27001 et 27002 est en définitive judicieux et avantageux, étant donné leur importante **reconnaissance et pénétration sur le marché mondial**, ainsi que leur précieux **apport terminologique, structurel et systématique**. Ce contexte normatif est ou sera d'ailleurs bientôt élargi par des guides additionnels, comme ISO 27003 « Implémentation de SGSI », ISO 27004 « Métrique de l'efficacité des mesures », ISO 27005 « Gestion des risques » , ISO 27006 « Exigences d'accréditation » ou encore ISO 27007 « Audits de SGSI ».

La structure des documents normatifs se présente ainsi schématiquement comme suit :