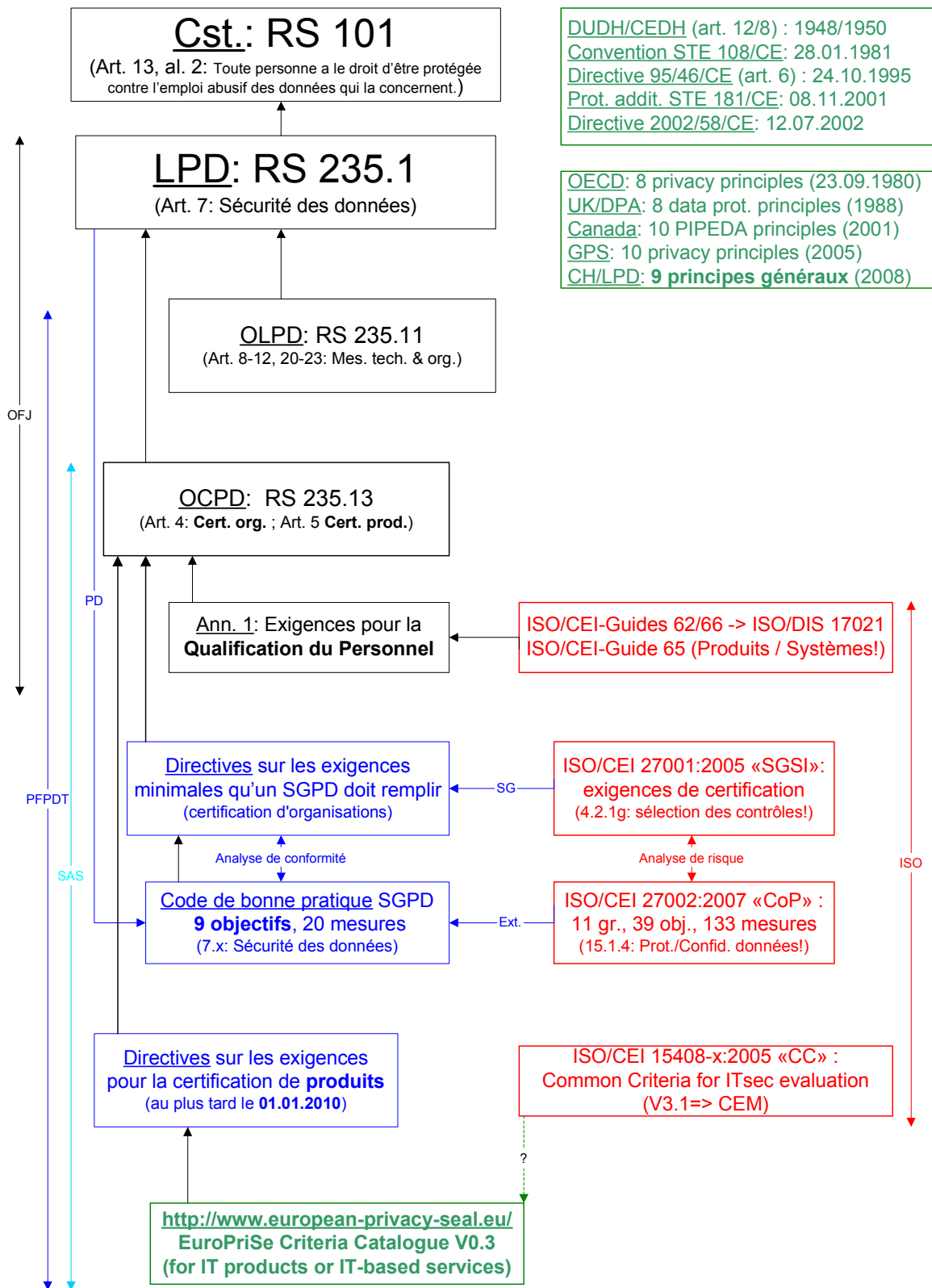




Commentaire explicatif sur les «directives sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir»

Les «directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir» sont une concrétisation de la délégation de l'ordonnance sur les certifications en matières de protection des données (art. 4 al. 3 OCPD ; RS 235.13), qui renvoie aux normes internationales relatives à l'installation, l'exploitation, la surveillance et l'amélioration de systèmes de gestion, en particulier aux normes ISO 9001:2000 et 27001:2005. Afin de mettre à disposition un instrument déjà connu et utilisé par les spécialistes en la matière, le PFPDT a suivi les exigences portant sur les systèmes de gestion, en mettant l'accent principal sur les aspects de protection des données plutôt que sur la sécurité de l'information.

Pour commencer, il peut être utile de situer ces directives au sein de l'ordre juridique suisse, en parallèle avec les fondements européens de la protection des données et avec les normes ISO concernées, sans oublier que le PFPDT a jusqu'au 01.01.2010 pour édicter les autres «directives fixant les critères spécifiques en matière de protection des données qu'un produit doit remplir dans le cadre d'une certification (art. 5 al. 3 OCPD)»:



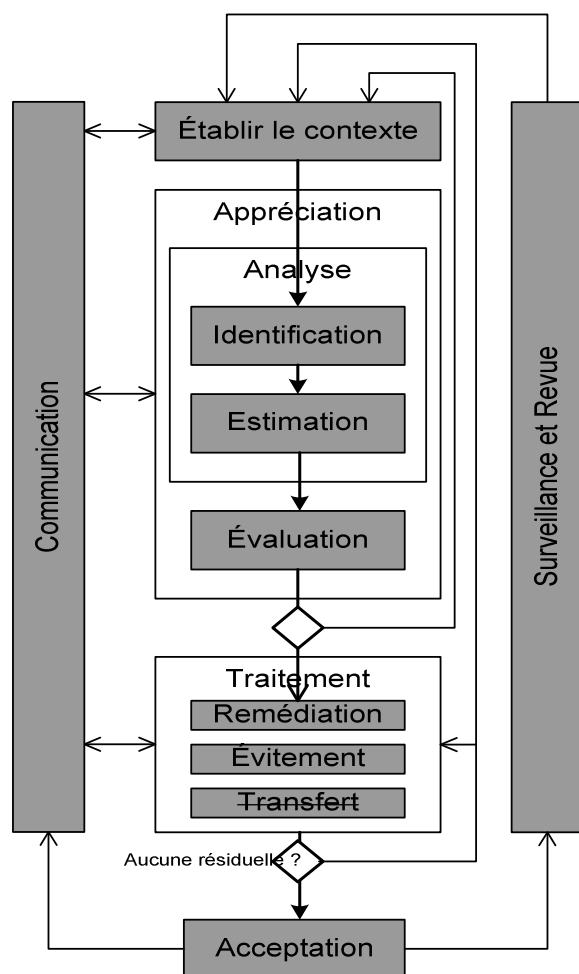
Une première étape a consisté à reprendre d'ISO 27001 les exigences génériques pour les systèmes de gestion, elles-mêmes issues de celles fondamentales d'ISO 9001 pour la gestion de la qualité, comme en témoigne l'annexe informative C d'ISO 27001. L'accent sur la protection des données se manifeste globalement par une **analyse de non-conformité** venant compléter l'analyse de risques et spécifiquement par une **interprétation de certaines clauses** liées à l'établissement et à la

documentation du SGPD.

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 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*.

Un des nœuds de cette accentuation repose sur 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 volontaires de sécurité de l'information, elle ne l'est par contre pas du tout pour des exigences légales 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 (identification des sources et estimation de non-conformité), suivie d'une **évaluation** de non-conformité aboutissant traditionnellement à deux valeurs : non-conformité mineure ou majeure. Il s'agit ensuite de passer au **traitement** des non-conformités, à savoir d'y **remédier** par l'adoption de mesures appropriées ou de les **éviter** en renonçant par exemple au traitement concerné, étant donné qu'une non-conformité ne saurait être ni transférée, ni acceptée (aucune non-conformité résiduelle)!

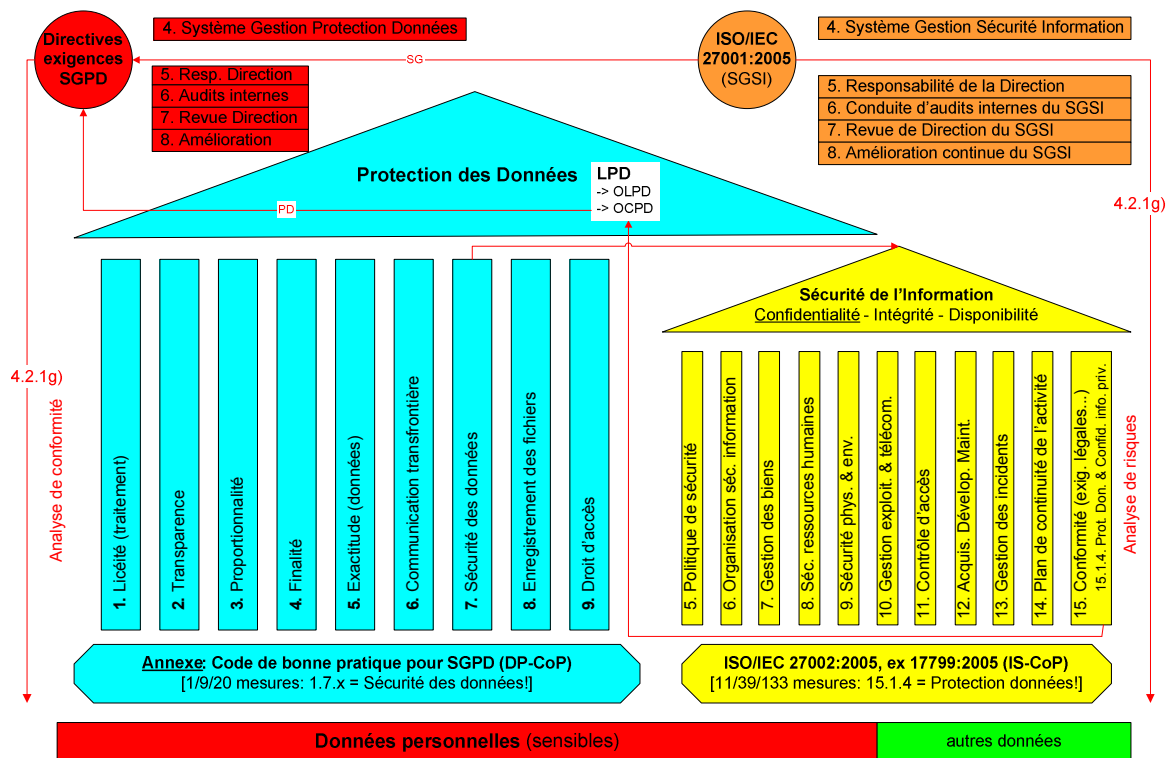


Dans une seconde étape, il s'est agi de remplacer l'annexe normative A d'ISO 27001 qui est en fait constituée de la table des matières de la norme ISO/CEI 27002:2005 plus connue sous le nom de «Code de bonne pratique pour la gestion de la sécurité d'information». Ce dernier comprend 15 chapitres, dont 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» portant sur la sécurité de l'information. L'**accent sur la protection des données** n'est ici qu'ébauché par 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 réglementations applicables, et les clauses contractuelles le cas échéant». Dans l'optique d'une certification d'organisation ou de procédure en matière de protection des données, cette seule mesure 15.1.4 très générale doit à l'évidence être renforcée, détaillée et subdivisée en objectifs, eux-mêmes réalisables par des mesures concrètes de protection des données.

Ceci est ainsi réalisé par le biais du «**code de bonne pratique pour la gestion de la protection des données**», dont les objectifs et mesures figurent synthétiquement au point 5 des «**Directives sur les exigences minimales qu'un SGPD doit remplir**» et intégralement en annexe de ces dernières. Autrement dit, le «code de bonne pratique pour la gestion de la protection des données» est aux directives SGPD, ce qu'ISO 27002 est à ISO 27001.

À l'instar de l'OCDE et de certains 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 « code de bonne pratique pour la gestion de la protection des données». 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 (mesure, mise en œuvre et autres informations). Tout comme la mesure 15.1.4 renvoie elle-même les SGSI aux SGPD, il faut ici relever que le 7^e objectif «Sécurité des données» avec ses mesures associées n'est rien d'autre qu'un renvoi des SGPD aux SGSI. Ainsi, parmi les 133 mesures d'ISO 27002, une présélection des plus pertinentes pour la sécurité des données au sens de 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 très probable 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», dont les SGPD pourront profiter.