Commentaire explicatif sur les modifications du 19 mars 2014 des «Directives sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir»

Conformément à l'art. 4 al. 3 de l'Ordonnance sur les certifications en matière de protection des données (OCPD; RS 235.13), le PFPDT a émis les directives sur les exigences minimales qu'un système de gestion de la protection des données (certification de l'organisation et de la procédure; ci-après directives SGPD) doit remplir. Celles-ci sont entrées en vigueur le 1er septembre 2008 et s'inspiraient fortement de la norme ISO/CEI 27001:2005. Cette norme ISO a été remplacée par la norme ISO/CEI 27001:2013 publiée le 1er octobre 2013. Les modifications de la norme ISO concernent surtout un remaniement technique des différentes exigences pour la sécurité de l'information. En même temps, la structure de la norme a été adaptée aux autres normes ISO concernant les systèmes de management (annexe SL). Vu le lien étroit avec la norme ISO/CEI 27001:2005 et vu que les directives SGPD renvoient à différents chiffres de ladite norme, une adaptation des directives SGPD s'imposait. Avec les modifications du 19 mars 2014, le PFPDT a adapté les directives SGPD à la norme ISO/CEI 27001:2013. Ce sont les seules modifications qui ont été faites.

Concernant les modifications en détail:

Désignation de la norme 27001

En premier lieu, le terme «ISO/CEI 27001:2005» a été remplacé partout par «ISO/CEI 27001:2013».

Chiffre 2. Définitions

Les chapitres 3.1-3.16 de la norme ISO 27001 sont devenus nouvellement les chiffres 2.1.-2.89 de la norme ISO/CEI 27000:2014. Les renvois ont été modifiés en conséquences dans les directives SGPD.

Concernant les définitions, les formulations de celles-ci ont été adaptées aux nouvelles formulations de la norme ISO 27000.

Chiffre 4. Réalisation (exigences minimales) et note de bas de page 6

À la lettre b, les désignations des chiffres de la norme ISO ont été adaptées conformément aux nouveaux chiffres de la norme ISO/CEI 27001:2013. Ainsi, le chiffre 4.2.1.a. est devenu le chiffre 4.3, le chiffre 4.2.1.b est devenu 5.2, le chiffre 4.2.1.d 1. est devenu 6.1.2.c.2., le chiffre 4.2.1.g. est devenu 6.1.3.b. et le chiffre 4.3.1.j. est devenu 7.5.1.c.

En plus, le terme de «politique pour le SGPD» du chiffre 5.2 (auparavant 4.2.1.b) de la lettre b a été remplacé par «politique de protection des données» en rajoutant une note de bas de page. Dans la note de bas de page, il a été précisé que cette politique de protection des données de niveau supérieur est étayée par d'autres politiques thématiques de sécurité de l'information ou de protection des données de la vie privée décrites dans la mesure A.5.1.1.

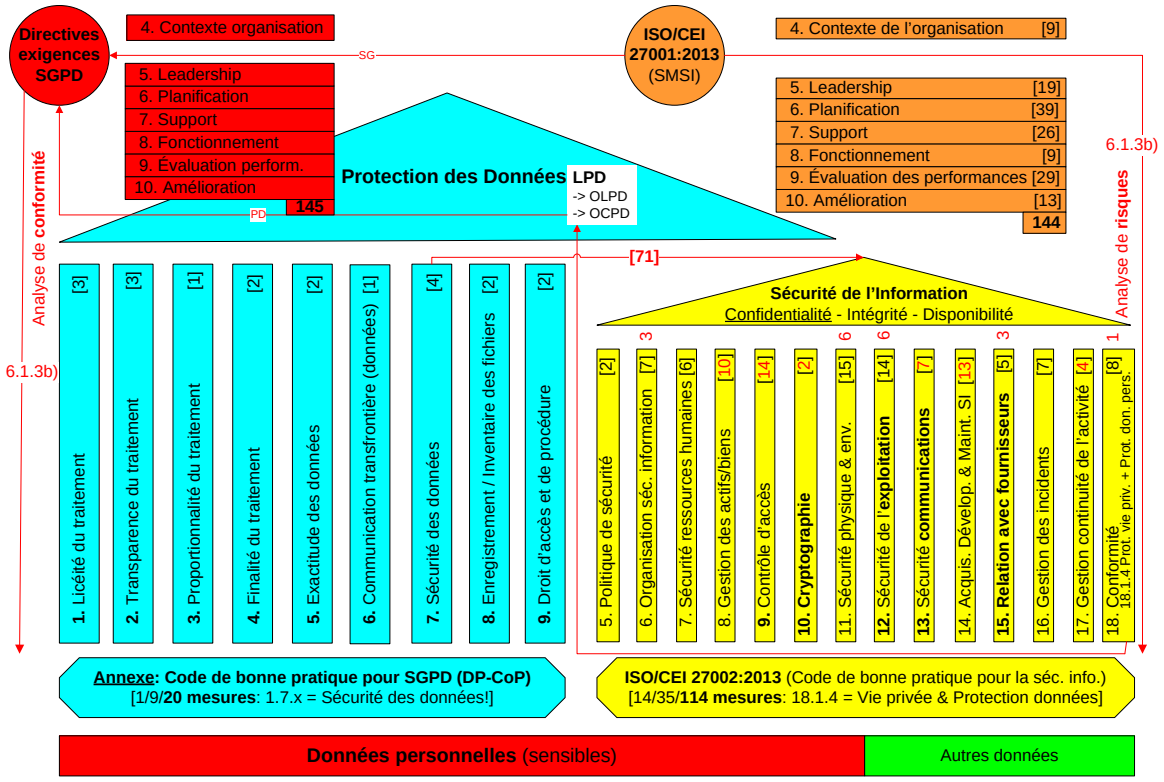
Chiffre 6. Abrogation d'un autre acte et 7. Disposition transitoire

Les directives SGPD du 19 mars 2014 remplacent celles du 16 juillet 2008. Pour cette raison, ces dernières sont abrogées. La disposition transitoire du chiffre 7 précise que les procédures de certifications en cours sont régies par les anciennes directives. Ces procédures de certifications doivent cependant être achevées jusqu'au 1er octobre 2014. Les organismes de certifications

obtiennent ainsi suffisamment de temps pour adapter leurs procédures de certification et entreprendre les modifications nécessaires auprès des entreprises dont les certifications sont en cours. Cette date correspond également à la date, à laquelle les audits peuvent encore être réalisés selon la norme ISO/CEI 27001:2005. L'adaptation d'ISO/CEI 27001:2005 à ISO/CEI 27001:2013 devrait se faire sans grandes difficultés. De même, l'adaptation de la procédure de certification SGPD aux nouvelles directives du 19 mars 2014 ne devrait pas créer de problèmes majeurs.

Concernant l'interprétation et l'application des nouvelles directives SGPD, il peut être renvoyé au commentaire explicatif existant de 2008 sur les «directives sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir», en particulier en ce qui concerne l'appréciation de (non-)conformité, l'analyse de non-conformité (évaluation, traitement, élimination, évitement) et du rapport des directives SGPD avec l'annexe aux directives sur les exigences minimales qu'un SGPD doit remplir.

Les schémas des pages 5 et 2 ont été adaptés comme suit:



Il peut être fait mention du nouveau 15e groupe concernant les «relations avec les fournisseurs», dont les objectifs (A.15.x) ont été repris dans les mesures de protection des données a.3 et g.4 concernant le «traitement de données par un tiers». En plus, les nouveaux objectifs A.6.1.5 concernant la «sécurité de l'information dans la gestion de projet» (=> «Privacy by Design»), ainsi que A.6.2 concernant «appareils mobiles et télétravail» ont été insérés dans la mesure de protection des données g.1 concernant la confidentialité des données.

Hiérarchie des documents normatifs

PFPDT/BY/05.04.2014