Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Le préposé suppléant

Berne, le 31.10.2007

Aux organisations intéressées:

Audition: Projet de directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir (certification de l'organisation ou de la procédure)

Mesdames et Messieurs,

Le Conseil fédéral a fixé, le 28 septembre 2007, l'entrée en vigueur de la loi révisée sur la protection des données au 1er janvier 2008. La révision prévoit entre autre la possibilité de procéder à des certifications en matière de protection des données. Celles-ci servent à améliorer la protection et la sécurité des données. La certification sera entièrement du ressort d'organismes privés. Comme il s'agit d'une matière entièrement neuve, elle fait l'objet d'une nouvelle ordonnance (Ordonnance sur les certifications en matière de protection des données [OCPD]).

La loi révisée prévoit les deux objets de certification suivants : d'une part l'organisation et la procédure de protection de données (système de gestion de la protection des données), d'autre part les produits (programmes et systèmes). Le préposé fédéral à la protection des données et à la transparence est chargé d'émettre dans un premier temps des directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir, de même que – d'ici au 1er janvier 2010 – des directives fixant les critères spécifiques en matière de protection des données qu'un produit doit remplir dans le cadre d'une certification. Le préposé émettra ces directives concernant les produits ultérieurement, afin de pouvoir suivre l'évolution des travaux en cours au niveau européen pour élaborer des normes de certification de produits en matière de protection des données.

Selon l'art. 4, 3e al. OCPD, le préposé émet des directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir. Pour cela, il tient compte des normes internationales relatives à l'installation, l'exploitation, la surveillance et l'amélioration de systèmes de gestions et en particulier la norme ISO/CEI 27001:2005. Il s'agit d'un projet de directives importantes dans la pratique, notamment dans de nombreux domaines de l'économie. C'est pourquoi nous menons une audition au sens de l'art. 10 de la loi sur la consultation (RS 172.061). Nous vous soumettons donc pour prise de position le projet de directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir, ainsi que son annexe et le commentaire explicatif.

Les présentes directives se basent principalement sur **ISO/CEI 27001:2005**, en conservant l'accent sur la protection des données. Il s'agit essentiellement de remplacer la « sécurité de l'information » par la « protection des données » et de compléter la « gestion des risques » par la « gestion de la conformité ». Les exigences génériques pour les systèmes de gestions ont été reprises d'ISO 27001. Pour conserver l'alignement avec son annexe normative A formée des objectifs et mesures de sécurité tirées directement de la norme **ISO/IEC 27002:2005**, les directives contiennent en annexe un guide d'implémentation, consistant en 20 mesures concrétisant les « 9 principes généraux de la loi sur la protection des données ».

Feldeggweg 1, 3003 Berne
Tél. 031 322 43 95, Fax 031 325 99 96
www.edoeb.admin.ch

Nous vous prions de bien vouloir faire parvenir votre réponse par écrit, d'ici au **28 novembre 2007**, directement au Préposé fédéral à la protection des données et à la transparence, 3003 Berne. Monsieur Pierre-Yves Baumann (031 322 43 48; pierre-yves.baumann@edoeb.admin.ch) et Madame Caroline Gloor Scheidegger (031 322 47 52 caroline.gloorscheidegger@edoeb.admin.ch) répondront volontiers à toute question complémentaire. Vous pouvez télécharger d'autres exemplaires du dossier envoyé à l'adresse suivante : *www.leprepose.ch – thèmes – protection des données – autres thèmes – révision de la loi fédérale sur la protection des données*. Vous pouvez également commander d'autres exemplaires auprès du secrétariat du Préposé fédéral à la protection des données et à la transparence (du lundi au vendredi, de 10 h 00 à 12 h 00, au numéro 031 322 43 95).

Dans l'attente de votre réponse, nous vous prions d'agréer, Mesdames, Messieurs, l'expression de notre considération distinguée.

Jean-Philippe Walter

Annexes:
- Projet de directives avec annexe et commentaire explicatif
- Liste des organisations participant à l'audition