

Sécurité de l'information

Garantir la libre circulation des données à caractère personnel

Frank Robben

Membre de la Commission de la protection de la vie privée (CPVP)

Administrateur général de la Banque-carrefour de la Sécurité sociale

Chaussée Saint-Pierre, 375

B-1040 Bruxelles

E-mail : Frank.Robben@ksz.fgov.be

Site Internet CPVP : www.privacycommission.be

Site Internet personnel : www.law.kuleuven.be/icri/frobben

Sécurité de l'information – disposition de la Directive

Article 17 – Sécurité des traitements

Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

Sécurité de l'information

- la sécurité absolue ne constitue pas, à juste titre, un but à poursuivre, car on perd alors de grandes opportunités en matière d'efficacité
- l'article de la Directive ne requiert aucune adaptation étant donné qu'il exige des mesures pour garantir un niveau de protection adéquat en fonction des risques et de la nature des données traitées et compte tenu de l'état de la technique et des coûts liés à leur mise en œuvre.
- il pourrait par contre être utile de prévoir
 - une méthodologie d'appui pour l'analyse et la gestion des risques
 - une précision des domaines de sécurité de l'information pour lesquels des mesures pourraient être nécessaires
 - des best practicesau besoin, à préciser au fur et à mesure par secteur

L'analyse et la gestion des risques comme fondement

- sécurité de l'information = éviter des dommages aux informations et aux systèmes de traitement de l'information ainsi que pour toutes les personnes concernées (titulaires de données, utilisateurs, ...)
- nécessité d'accorder de l'attention aussi bien aux dommages directs qu'aux dommages indirects ; plus les liens entre les (systèmes d') informations sont importants, plus le risque augmente
- risque = chaque facteur externe et interne qui peut menacer la sécurité de l'information
- nécessité d'accorder de l'attention aux mesures sur 3 niveaux :
 - comment éviter les dommages ?
 - comment limiter les dommages lorsqu'ils surviennent ?
 - comment réparer au mieux les dommages survenus ?

L'analyse et la gestion des risques comme fondement

- la sécurité de l'information implique de se concentrer sur les risques au niveau de :
 - l'exactitude et de l'intégrité
 - la disponibilité
 - la confidentialité
 - la non réfutabilité
 - l'authenticité
 - l'auditabilité
- des informations et des systèmes de traitement des informations

Quelques types de menaces

- menaces humaines

- volontaires

- internes : propres collaborateurs, collaborateurs de sous-traitants, ...
 - accès non autorisé, sabotage, vol, ...
 - externes : hackers, espions, concurrents, ...
 - accès non autorisé, sabotage, effraction, ...

- non volontaires

- internes : propres collaborateurs, collaborateurs de sous-traitants
 - faute, négligence, prise de conscience insuffisante, ...
 - externes : clients, partenaires, fournisseurs, ...
 - faute, négligence, insécurité de leurs systèmes, ...

- menaces physiques

- coupure de courant, tremblement de terre, incendie, inondation, humidité, variations de température, ...

Méthode de gestion des risques

- identification des risques
- évaluation des risques
 - probabilité
 - impact
 - possibilité de contrôle
- détermination des niveaux de risque acceptables
- identification et analyse des mesures existantes de gestion des risques
- évaluation des mesures existantes de gestion des risques
- analyse des autres options de gestion des risques
- définition d'un plan d'action pour la gestion des risques
- monitoring

Domaines de sécurité de l'information

- Série ISO 27000, en particulier l'ISO 27002
 - Évaluation et traitement des risques
 - politique de sécurité : management direction
 - organisation de la sécurité de l'information
 - gestion des biens : inventaire et classification des informations
 - sécurité liée aux ressources humaines : aspects relatifs à la sécurité pour les employés qui rejoignent une organisation, s'y déplacent ou la quittent
 - sécurité physique et environnementale : protection de l'équipement informatique
 - gestion des communications et de l'exploitation : gestion des contrôles de la sécurité technique dans les systèmes et réseaux
 - contrôle d'accès : restriction des droits d'accès aux réseaux, systèmes, applications, fonctions et données

Domaines de sécurité de l'information

- Série ISO 27000, en particulier l'ISO 27002
 - acquisition, développement et maintenance des systèmes d'information : intégrer la sécurité aux applications (immunité)
 - gestion des incidents liés à la sécurité de l'information : anticiper et réagir correctement aux violations de sécurité de l'information
 - gestion de la continuité d'activité : protéger, maintenir et reconstituer les processus et systèmes cruciaux pour l'activité
 - conformité : assurer la conformité avec les politiques, normes, lois et règlements de sécurité de l'information
- à ajouter éventuellement
 - exigences particulières pour le traitement de données à caractère personnel
 - communication quant à la politique et aux mesures en matière de sécurité de l'information et de protection de la vie privée

Libre circulation – disposition de la Directive

Article 1 – Objet de la Directive

1. Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.
2. Les États membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre États membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1.

Néanmoins ...

- certains États membres entravent ou refusent, pour un bon fonctionnement de l'administration, l'échange nécessaire de données à caractère personnel avec d'autres États membres qui ont transposé correctement la Directive en droit national
- pas de nécessité de modifier la Directive
- mais il est souhaitable de prévoir :
 - une campagne d'information sur cette disposition de la Directive
 - une instance d'autorisation formelle ou du moins une instance de médiation au sein de la Commission européenne en cas de problème entre États membres
 - un système de sanction effectif en cas de non-respect de cette disposition par un État membre

Merci !

**Avez-vous des
remarques ou des
questions ?**