ADaCoR Panel Discussions

Day 3: Data Protection

Durée:	15:50 – 16:50
Modérateur:	Carlo Harpes
Participants:	C. Harpes (*itrust consulting*), M. Aubigny (*itrust consulting*), G. Wantz (*CNPD*), P. Steichen (*CLUSIL*), A. Herrmann (*CNPD*), A. Grosjean (*Bonn & Schmitt Avocats*)

Le troisième « discussion panel » du workshop ADaCoR avait pour thème « Data protection aspects of data collection ». Plusieurs points de discussion ont été traités par les intervenants de la dernière journée du workshop ADaCoR.

Le premier point de discussion concernait les différents types de certification. Il existe des certifications de type technique telles qu'EuroPrise, qui vont s'appliquer à démontrer que le produit ou service respectent les exigences propres au cadre de certification. Il existe aussi des certifications des systèmes de management de la sécurité qui vont regarder si la mise en œuvre du service est conforme aux exigences (ex. : ISO 27001). A noter aussi que d'autre cadre de certification orienté protection des données personnelles existent comme celle proposée par TrustE.

Le deuxième point de discussion portait sur le fait que les sanctions prises considèrent que les entreprises ou les organisations respectent ou non les normes de sécurité. Les intervenants ont tenu à préciser qu'un incident de sécurité ou le vol de données ne signifie pas forcément qu'il y aura une sanction contre l'organisation ou l'entreprise. Des sanctions seront données seulement si le responsable du traitement n'a pas fait son travail. Si le vol de données est inévitable pour l'entreprise alors aucune sanction ne sera prise. Donc, pour éviter au maximum les sanctions, les entreprises doivent avoir une bonne collaboration et une ouverture avec la CNPD.

Dans la continuité de cette discussion, la CNPD tenait à ajouter que l'établissement d'une guidance pour les organisations et les entreprises est en cours en collaboration avec plusieurs acteurs des différents corps de métier.

Le troisième point de discussion a permis aux intervenants d'expliquer en quoi l'arrivée du nouveau règlement européen va modifier la procédure d'investigation qui permettra ou non de sanctionner une organisation ou une entreprise. Les intervenants ont expliqué qu'au niveau européen, trois commissaires vont procéder aux investigations et décider de la sanction à donner aux entreprises. Au niveau luxembourgeois, la CNPD a autorité pour investiguer. De plus, elle peut s'autosaisir, ce qui veut dire qu'il ne faut pas forcément qu'il y ait plainte pour que la CNPD soit saisie. La CNPD peut également faire des contrôles sporadiques dans les entreprises.

Il a été relevé au cours de cette discussion que le nouveau règlement UE peut :

- inciter les entreprises à moins reporter les incidents
- rendre moins attractif le Luxembourg.

Par Guillaume Schaff, *itrust consulting*.

Pour le premier point, les intervenants ont expliqué que le fait que les entreprises communiquent contribuera à l'amélioration de son image auprès de ses clients. La transparence est un atout pour les entreprises et elles le comprendront. Les intervenants ont tenu à préciser qu'avec le nouveau règlement, une entreprise qui ne communique pas des failles de sécurité relative à la protection des données risque 4% de son chiffre d'affaires mondial ou 20 Mio € . Pour le deuxième point, les intervenants ont souligné que dans tous les cas, il y a une obligation pour tous les états membres de se conformer au règlement UE.

Pour le quatrième point de discussion, les intervenants ont pu s'exprimer sur l'élément le plus important pour eux dans la protection des données. Les intervenants ont été unanimes sur le fait que former et sensibiliser les utilisateurs à tous les niveaux à la protection des données est l'élément le plus important ici. Cependant, cette sensibilisation doit être proportionnelle au traitement (type de données traitées).

Au cours de cette discussion, il a été relevé le fait que beaucoup de gens savent que leurs données personnelles sont traitées et parfois vendues sans que cela l'inquiète. Les intervenants ont expliqué que ce comportement est dû à un manque de sensibilisation des utilisateurs et qu'ils ont le plus souvent une fausse impression sur la maitrise de leurs données personnelles.

Par Guillaume Schaff, *itrust consulting*.