AFCDP

Association Française des Correspondants à la Protection des Données a Caractère Personnel

Groupe de Travail « Notification des violations aux traitements de données personnelles » 30/11/2010

Pascale Gelly	**Avocate, Administratrice AFCDP**
Eric Doyen	**RSSI de Generali, Président du Club 27001**
Bernard Foray	**DSSI de Casino Information Technology, CIL, RSSI de l'année 2010**

AFCDP

Association **F**rançaise des **C**orrespondants à la protection des **D**onnées à caractère **P**ersonnel

www.afcdp.net

Présentation de l'AFCDP

- Créée en septembre 2004, lors de la refonte de la loi Informatique et Libertés
- Objectifs
  - Faire de la fonction de CIL un METIER
  - Proposer un cadre d'échanges,
  - Concevoir des outils, méthodes et pratiques utiles aux CIL,
  - Soutenir la fonction auprès des pouvoirs publics,
  - Prendre position sur les évolutions prévisibles
- Présidé par un CIL
- 750 professionnels, pas uniquement des CIL : RSSI, Juristes d'entreprise, Qualiticien, Auditeur, Déontologue, Risk Manager, Avocats, Consultants, PRADA, Archivistes, etc.
- De nombreux groupes de travail, thématique et régionaux
- Des manifestations : Université, Assises, Débats
- Interaction avec la CNIL

Groupes de Travail

- *Formation du CIL*
- *Cybersurveillance*
- *Préparation à un contrôle de la CNIL*
- *Référentiels & Labels*
- *Bilan annuel du CIL*
- *Données Prospects et Clients*
- *Flux transfrontières*
- *Données de santé*
- *Géolocalisation et Libertés*
- *Notification des violations de données*
- *Responsabilité du CIL*
- *Durée de conservation*
- *Relations entre CIL, Responsable de traitement et IRP*
- *Traitements de Ressources Humaines… etc.*

Les apports et les missions d'un CIL

- Maîtrise les risques d'application de la loi
- Inventorie les traitements automatisés des données personnelles
- Définit les procédures d'accès aux données individuelles
- Allège les formalités CNIL et rend compte de son action
  - Service préférentiel et personnalisé
- Conseille, recommande, concilie et alerte le responsable des traitements
- Met en œuvre les plans de mise en conformité

Article 34 de la loi « informatique et libertés » du 6 janvier 1978: L'obligation de sécurité

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Les risques en cas de non-conformité (loi n°78-17)

- Sanction pécuniaires pouvant aller jusqu'à 300k€
- Injonction de cesser ou suspendre le traitement
- «Verrouillage» des données à caractères personnel
- La non-conformité à la loi peut être rendue publique

Article 7 de la proposition de loi

« L'article 7 précise l'obligation de sécurisation des données incombant au responsable du traitement et crée une obligation de notification à la CNIL des failles de sécurité, transposant par anticipation la directive modifiant la directive 2002/58/CE concernant la vie privée dans le secteur des communications électroniques »

2002/58/CE : Directive du « paquet télécom » opérateurs et ISP – notification des incidents de sécurité ou perte d'intégrité des données des abonnés ayant eu un impact significatif

Préambule de la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, Présentée par les Sénateurs M. Yves Détraigne et Mme Anne-Marie Escoffier – 6 novembre 2009

- **…« Créer à minima une obligation de notification des failles de sécurité auprès de la CNIL »**

Recommandation n°11 du rapport d'information du groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques

Texte voté par le Sénat

« *Art. 34. –* ***Le responsable du traitement met en œuvre toutes mesures adéquates****, au regard de la nature des données et des risques présentés par le traitement,* ***pour assurer la sécurité des données*** *et en particulier protéger les données à caractère personnel traitées contre toute* ***violation entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation, la diffusion, le stockage, le traitement ou l'accès non autorisés ou illicites.***

Texte (suite)

« ***En cas de violation du traitement de données*** *à caractère personnel,* ***le responsable de traitement avertit sans délai le correspondant "informatique et libertés" ou****, en l'absence de celui-ci,* ***la Commission nationale de l'informatique et des libertés****. Le responsable du traitement, avec le concours du correspondant "informatique et libertés", prend immédiatement les mesures nécessaires pour permettre le rétablissement de la protection de l'intégrité et de la confidentialité des données. Le correspondant "informatique et libertés" en informe la Commission nationale de l'informatique et des libertés.*

Texte (suite)

Si la violation a affecté les données à caractère personnel d'une ou de plusieurs personnes physiques, le responsable du traitement en informe également ces personnes*, sauf si ce traitement a été autorisé en application de l'article 26. Le contenu, la forme et les modalités de cette information sont déterminés par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés.*

Un inventaire des atteintes aux traitements de données à caractère personnel est tenu à jour par le correspondant "informatique et libertés".

« Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés aux 2°et 6°du II de l'article 8. »

La loi : introduction et calendrier

- La loi : contenu, enjeux, contexte
- La loi, votée par le Sénat, n'est pas à l'agenda des députés
- MAIS l'actualité c'est la directive européenne + un projet de loi français sectoriel (télécom)
- Quelle est la position du gouvernement Français ?
  - Mettre en « standby la loi » ?
  - Ne pas la modifier «trop tôt » ?

Création du groupe « Notification »

- En réaction à la proposition de loi
  - Détraigne/Escoffier
- Pour réfléchir
- Pour prendre la sécurité des données au sérieux
- Pour chercher des leviers qui vont nous permettre de le faire

Conférence de lancement : 23 mars 2010

Palais du Luxembourg

1ère réunion de travail : 8 juin 2010

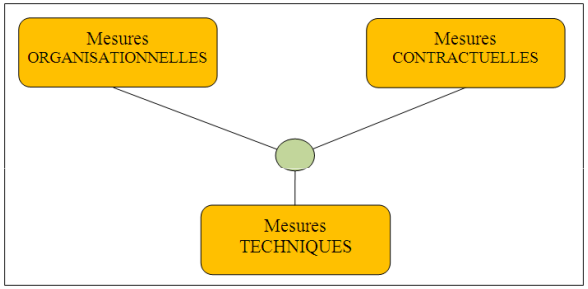
Lexique
Thésaurus : les documents et sites Web incontournables sur le sujet
F.A.Q : les questions
Audition d'entreprises ayant notifié

2ème réunion de travail : fin juin 2010

Audition de CPO de grandes entreprises américaines (*IAPP Delegate tour*)
Check-list préventive
Check-list curative

Comment se prépare-t-on à la loi

- Coordonner les acteurs
  - DG, juridique, propriétaire des données et des processus associés, communication, RSSI, cellule d'intelligence économique, marketing
- Analyse de risque, classification des données
- S'assurer de l'efficacité des processus
  - Gestion des incidents
  - Gestion de crise
  - Information/communication (Salariés, Clients, IRP, Actionnaires)
- Examiner les moyens
  - Protections techniques
  - Protections « humaines »
  - Procédures et courrier type, Service consommateur
  - Evaluation des impacts, conservation des preuves
- Revoir les contrats passés avec des tiers
  - art. 35 de la Loi Informatique & Libertés



Questionnement

- Qu'est-ce qu'une violation ?
- Quelle différence y-a-t-il entre exposition et exploitation d'une vulnérabilité ?
- Quels sont les critères de notification ?
- Notifie-t-on lorsqu'une vulnérabilité est connue ou en cas de violation ?
- Quel lien doit-on maintenir avec les autorités judiciaires ?
- Quelle interprétation peut-on faire de « Notification sans délai » ?
- Quelles sont les modalités opérationnelles (évaluation du préjudice et la conservation des données…)
- Comment différentier les données (chiffrées ou non…) ?
- Comment faire avec les sous-traitants , le cloud computing ?

CIL et RSSI : une collaboration nécessaire

Ils éprouvent les mêmes difficultés pour…

- être impliqués en amont
- faire passer l'idée que « mieux vaut prévenir que guérir »
- sensibiliser utilisateurs et direction
- faire appliquer les décisions, politiques, charte, etc.
- contrôler, (faire) sanctionner, (inciter à) corriger
- s'engager auprès de leur direction sur une obligation de résultats
- justifier leurs demandes de dépense (ROI sécurité ?)
- valoriser leurs actions (si pas d'incident, avions nous réellement besoin de faire des efforts ?)

Ils sont parfois ressentis/perçus comme

- des « improductifs »
- des « empêcheurs de tourner en rond »

En revanche le CIL dispose (de par les textes) d'une **indépendance** et est **directement rattaché au Responsable de traitement**.

… et la fonction du CIL est encadrée par une loi et un décret…

Prochaine réunion du groupe Mars 2011

Merci pour votre attention

www.afcdp.net

AFCDP