# Evolution réglementaire du rôle du CIL et Obligation de notifier ses failles de sécurité

Bruno Rasle- Délégué Général AFCDP

8 décembre 2009

# L'AFCDP

## Association Française des Correspondant à la Protection des Données Personnelles

Créée en septembre 2004, présidé par Un Correspondant Informatique et Libertés.

Plus de 260 membres : Halde, Mairie de Paris, Caisse d'Epargne Provence Alpes Corse, Chambre de Commerce de Marseille, CCIP, Axa, Areva, Randstad, Carrefour, Groupama, Conseil Général 76, Crédit Immobilier de France, Bull, Les 3 Suisses, École des Hautes Études en Sciences Sociales, ISEP, Legrand, Gras Savoye, Swiss Life, Ecole Polytechnique, Malakoff Mederic, RATP, La Poste, Total, Chambre Nationale des Huissiers, Cofidis, Michelin, SNCF, etc.

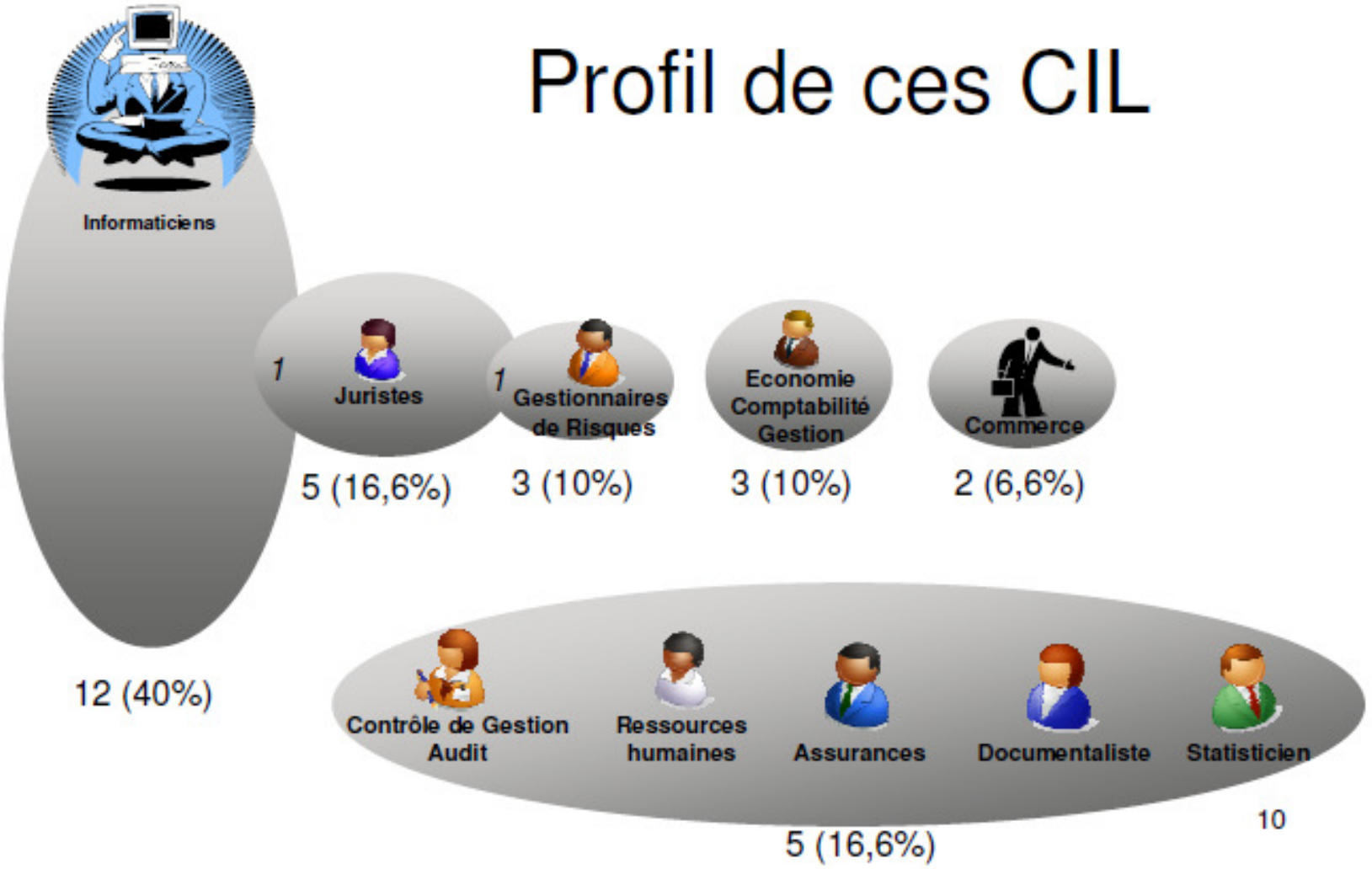
Plus de 400 individus : CIL, délégués à la protection des données, RSSI, juristes, avocats, consultants, enseignants-chercheurs, DRH, documentalistes, archivistes, qualiticiens, etc.

# Le CIL

- Possibilité introduite en 2004 (refonte de la loi du 6 janvier 1978)
- Décret d'application en octobre 2005
- Le Correspondant est « *chargé d'assurer d'une manière indépendante, le respect des obligations prévues dans la présente loi* »
- Désignation facultative, ouverte au secteur privé comme au secteur public
- Entraîne un allègement des formalités
- Implique un engagement du responsable de traitement

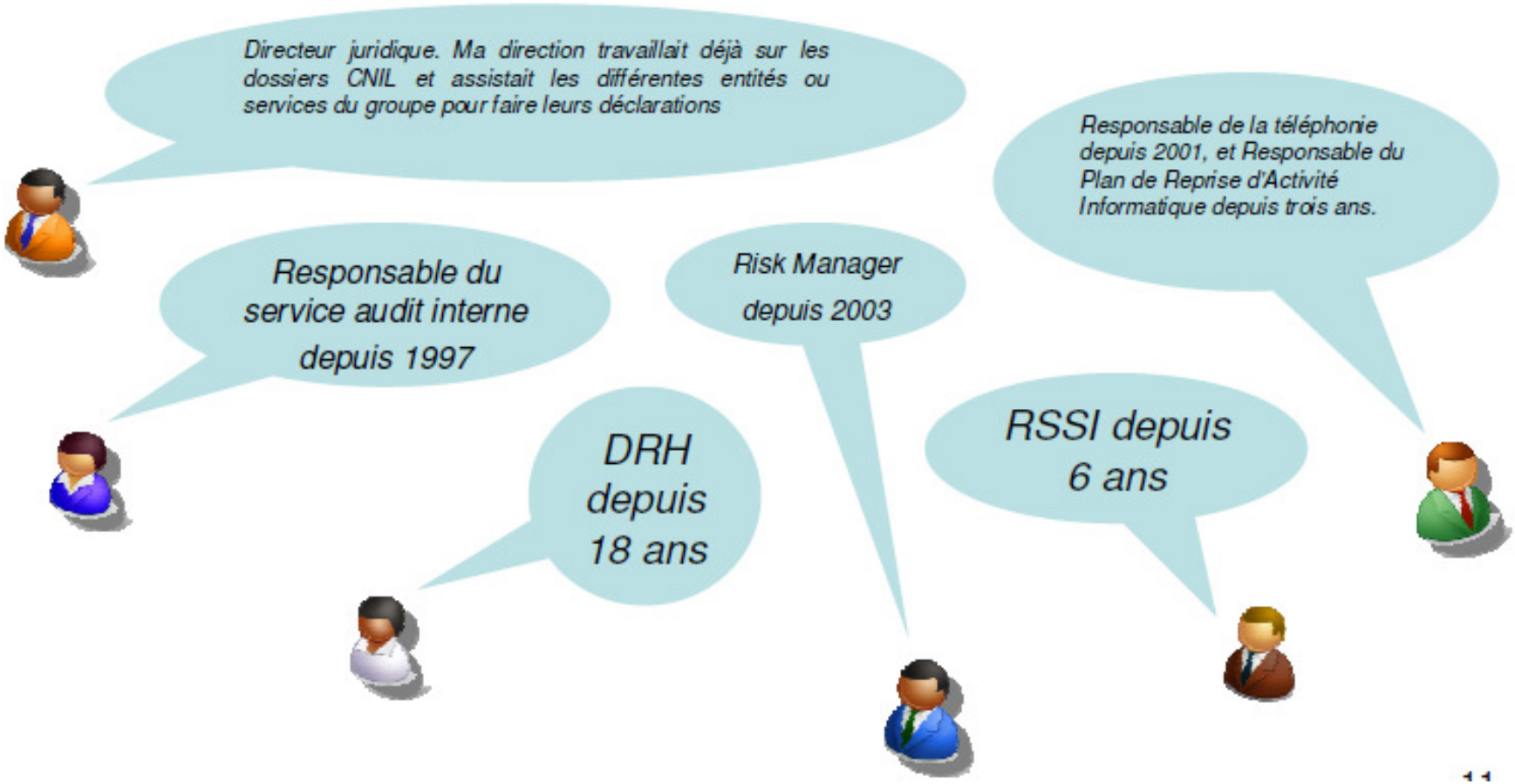
- 5500 entités ont désigné environ 2000 CIL

# Profil de ces CIL



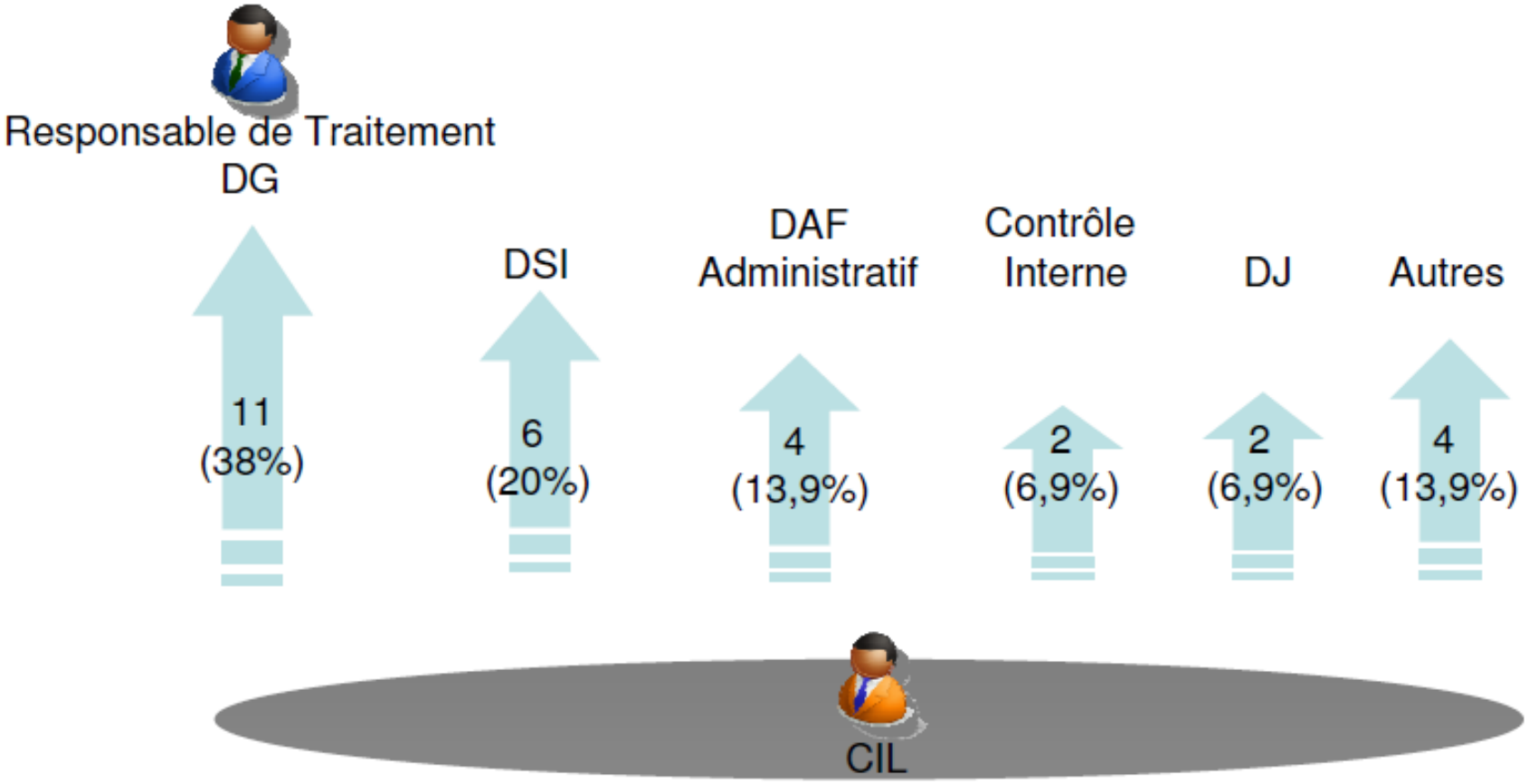

(Source : Etude AFCDP janvier 2009
« Désigner un CIL, un vrai projet »)

# Que faisaient-ils avant ?

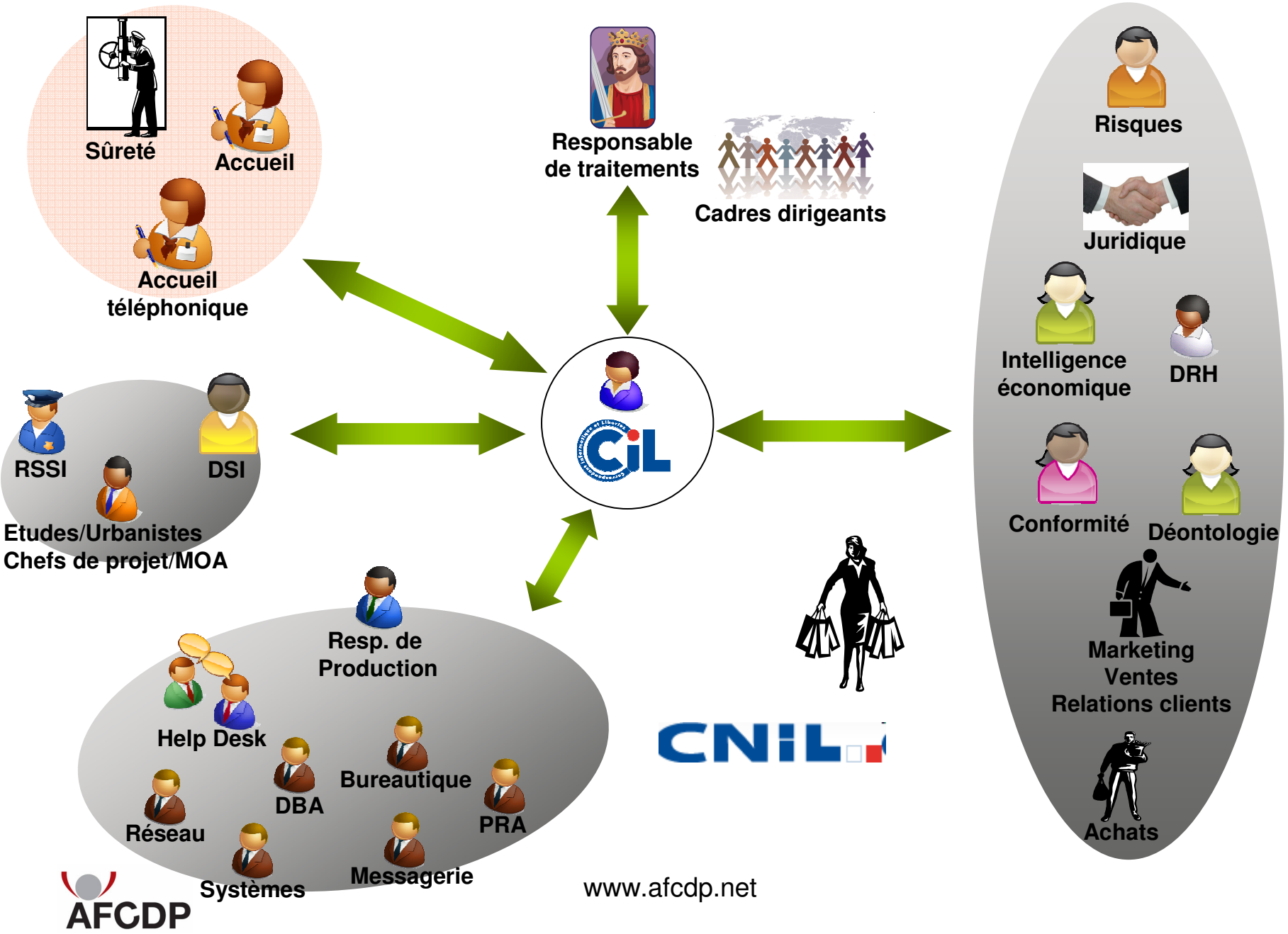



(Source : Etude AFCDP janvier 2009
« Désigner un CIL, un vrai projet »)

# Rattachement ?




(Source : Etude AFCDP janvier 2009
« Désigner un CIL, un vrai projet »)


Sûreté
Accueil
Accueil téléphonique
Responsable de traitements
Cadres dirigeants
Risques
Juridique
Intelligence économique
DRH
Conformité
Déontologie
Marketing
Ventes
Relations clients
Achats
RSSI
DSI
Etudes/Urbanistes
Chefs de projet/MOA
CiL
Resp. de Production
Help Desk
Bureautique
DBA
PRA
Réseau
Systèmes
Messagerie
CNIL
AFCDP
www.afcdp.net

# Bientôt obligatoire ?

Proposition de rendre le CIL obligatoire pour toute entité ayant plus de 50 personnes accédant aux données personnelles ou mettant en œuvre les traitements. En Allemagne, il l'est depuis plus de 30 ans.

# Points communs entre CIL et RSSI ?

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 également ressentis/perçus comme

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

Mais le CIL a la loi pour lui…

# Informatique & Libertés

- Obligation de sécurité :
  - Il appartient au responsable du traitement 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. (34 de la loi modifiée )

# Commentaires de la CNIL

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 accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que 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* ».

# Directive 95/46

*Considérant que la protection des droits et libertés [...] exige que des mesures techniques et d'organisation appropriées soient prises tant au moment de la conception qu'à celui de la mise en œuvre du traitement, en vue d'assurer en particulier la sécurité et d'empêcher ainsi tout traitement non autorisé; … que ces mesures doivent assurer un niveau de sécurité approprié tenant compte de l'état de l'art et du coût de leur mise en œuvre au regard des risques présentés par les traitements et de la nature des données à protéger;*

# Article 34

Obligation de moyens

Comment juger le type et le niveau de sécurité à mettre en place ?

Absence de référentiel (réflexions en Suisse)

La loi est technologiquement neutre, mais…

L'absence de réaction de la CNIL (lors d'une déclaration) ne vaut pas blanc seing

# La CNIL recommande

- Une évaluation des risques et une étude de la sécurité avant tout nouveau traitement (réexamen pour les traitements existants)
- Une définition des dispositions de sécurité ( formalisation et mises à jour)
- Une définition des responsabilités
- Une sensibilisation des personnes concernées
- De penser aux sous-traitants (art. 35)…

(Délibération n°81-094 du 21 juillet 1981)

# Rapport d'activité de 2003

La CNIL regrette certains constats dans les communes :

« *Il est fréquent que les mots de passe soient trop simples… sont souvent partagés… en cas d'absence temporaire du titulaire habituel du poste… pas de fermeture des logiciels lors de la pause… pas de hiérarchisation en fonction des habilitations des agents… absence de journalisation des connexions* ».

# Condamnations ?

**Cour de Cassation, Chambre criminelle 30 octobre 2001**

« *…a condamné le premier à 50 000 francs d'amende et le deuxième à 30 000 francs d'amende et qui a prononcé sur les intérêts civils…. que le système informatique mis en place n'assurait pas une protection suffisante de la confidentialité des données enregistrées ; Jean C., président du SIMTPA et Jean-Claude D. directeur de ce syndicat … que le fait qu'à un moment donné, la mauvaise utilisation des motifs de passe ait pu permettre à des administratifs de prendre connaissance des données médicales… recueillies dans le système, constitue en l'espèce le seul délit de l'article 42 de la loi du 6 janvier 1978 devenu 226-16 du Code pénal* »

[! Absence de déclaration également]

# Avertissement pour le site entreparticuliers.com

## 17/11/2008 - Echos des séances

*« plusieurs manquements… »*

**Par décision du 20 mai 2008, la CNIL, a prononcé un avertissement à l'égard de la société entreparticuliers.com en raison de plusieurs manquements à la loi informatique et libertés.**

Le site internet entreparticuliers.com a, comme son nom l'indique, pour but de mettre en relation des particuliers, vendeurs et acheteurs de biens immobiliers. La CNIL a été saisie de plaintes d'annonceurs particuliers, dénonçant des failles de sécurité (ils arrivaient à accéder au compte d'autres annonceurs), l'absence de prise en compte de leur demande de suppression de leurs données personnelles, ainsi que leur démarchage par des agences immobilières.

Après avoir mis en demeure la société d'améliorer l'information de ses clients sur les droits offerts par la loi informatique et libertés et de prendre des mesures afin de sécuriser ses traitements informatiques, la CNIL a effectué un contrôle sur place dans les locaux de cette société. Ce contrôle a permis de constater les manquements suivants :

- une faille de sécurité permettant d'accéder, depuis le site internet, à l'espace personnel des particuliers annonceurs (données de facturation, possibilité de modifier les annonces à leur insu…),
- l'absence de durée de conservation des données à caractère personnel,
- des carences en matière d'information sur les droits offerts par la loi informatique et libertés, en particulier l'absence de prise en compte du droit d'opposition ou des mentions d'informations insuffisantes sur les formulaires en ligne,
- des campagnes de prospection commerciale par SMS ou courriel sans recueil du consentement préalable des personnes contactées (en violation de l'article L. 34-5 du code des postes et télécommunications).

*« ..durée de conservation… »*

*« …une faille de sécurité… »*

AFCDP

PFPDT

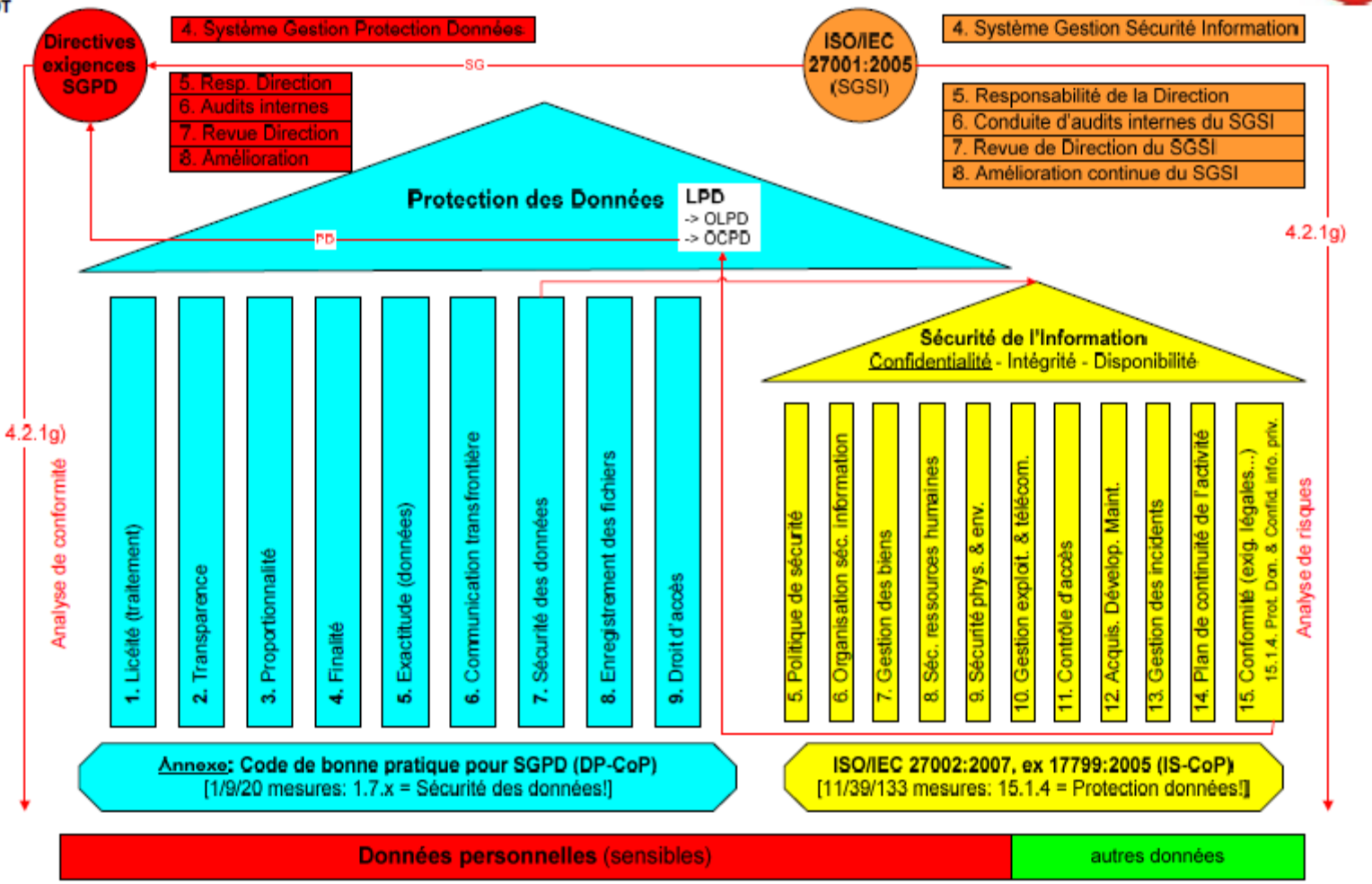
# Nouvel article 11 (FF 2006 3424)

*Art. 11 (nouv.)* Procédure de certification

- [1] Afin d'améliorer la protection et la sécurité des données, les fournisseurs de systèmes de logiciels et de traitement de données ainsi que les personnes privées ou les organes fédéraux qui traitent des données personnelles peuvent **soumettre leurs systèmes, leurs procédures et leur organisation à une évaluation effectuée par des organismes de certification agréés et indépendants**.
- [2] Le Conseil fédéral édicte des dispositions sur la **reconnaissance des procédures de certification** et sur l'**introduction d'un label de qualité** de protection des données. Il tient compte du droit international et des normes techniques reconnues au niveau international.

PFPDT

# Interdépendance entre SGPD et SGSI



# Juin 2009

**→ Compléter le cadre juridique actuel**

- Créer *a minima* une obligation de notification des failles de sécurité auprès de la CNIL

**b) Améliorer les dispositions relatives à la sécurité des données**

Le principe de la sécurité des données est probablement celui qui mériterait les aménagements les plus importants. …Il semble possible d'aller un peu plus loin en créant *a minima* **une obligation de notification des failles de sécurité à la CNIL**, des critères et des seuils devant être définis pour ne pas la submerger. Cette obligation pèserait sur tous les responsables de traitement. Bien maîtrisée et encadrée, l'obligation de notification des failles de sécurité peut être **une incitation forte au renforcement de la sécurité des données.**

*In. Rapport sénatorial « La vie privé à l'heure des mémoires numériques »*

# Novembre 2009

« 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 »

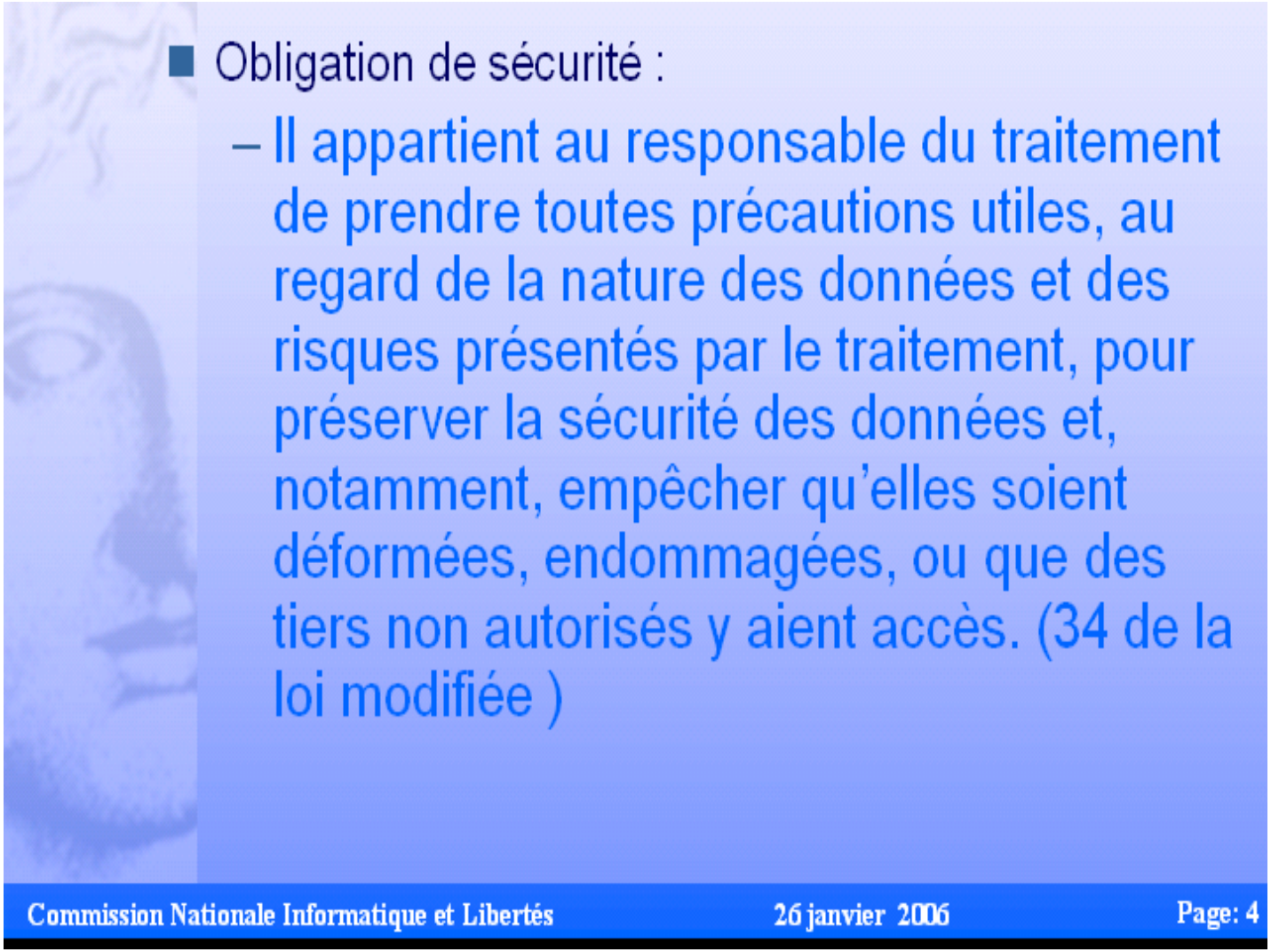
*Préambule de la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, Présentée par les Sénateurs M. Yves Détraigne et Mme Anne-Marie Escoffier – 6 novembre 2009*

# Article 7

L'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« *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, particulièrement lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ».

# Informatique & Libertés



# Article 7 (suite)

« En cas d'atteinte au traitement de données à caractère personnel, le responsable du traitement avertit sans délai la Commission nationale de l'informatique et des libertés qui peut, si cette atteinte est de nature à affecter les données à caractère personnel d'une ou de plusieurs personnes physiques, exiger du responsable du traitement qu'il avertisse également ces personnes. Le contenu, la forme et les modalités de ces notifications sont déterminés par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés ».

# Aux USA

- Californie dès 1993, imitée par pratiquement tous les états
- Beaucoup de variantes :
    - Nombre minimum de données personnelles
    - « *may have been* » ou vol assuré ?
    - Définition des données personnelles concernées
    - Supports papiers concernés ?
    - Destinataire de la notification et contenu de celle-ci
    - Cas d'exclusions
    - Sanctions (FTC : 11.000$ par violation)
- Loi fédérale HIPAA (secteur santé)
    - HITECH Act impose la notification
    - Sanctions allant jusqu'à 1.500.000$

Quels impacts ?

- Efforts réels de sécurisation
- Désignation de CPO Chief Privacy Officer)
- Purge des données !
- Protection contre l'Intelligence économique

# Bientôt une loi fédérale ?

Le Sénat américain va bientôt se prononcer sur une loi qui obligerait toute entités privées ou publiques manipulant des données personnelles sensibles à mettre en place des mesures de gestion de risques, de traçabilité aux données, de sécurisation et de notification des violation de données.

Ce texte remplacerait le patchwork des lois existantes.

# En Asie

Hong Kong :

• L'autorité de marché impose aux banques une notification auprès des clients

• Consultation sur une éventuelle modification du *Personnal Data Ordinance* (août 2009), proposition n°3 (Personal Data Security Breach notification). Obligation de notification si « high risk or significant harm ».

• D'abord un régime de volontariat, pour préparer des règles plus précises. Le Gouvernement s'impose cette démarche depuis novembre 2008.

Singapour :

• L'autorité de marché impose aux banques une notification auprès des clients

• Notification à la MAS (*Monetary Authority Of Singapore*) et à la police en cas de hacking et d'intrusion.

# En Europe

Angleterre :
• Sanctions infligées par la FSA (Financial Services Authority) : HSBC 3 millions de £, Nationwide 1 million de £, Norwich Union (1,2 millions de £)
• L'ICO demande l'extension de ses pouvoirs (audit des entreprises) et l'augmentation des sanctions (500.000 £ au lieu de 5.000 et la possibilité de demander des peines de prison)

Allemagne :
• Nouvelle loi (1er septembre 2009) avec obligation de notifier les « *data breach* » (existence d'un risque, notification à l'autorité et aux personnes, liste de données personnelles concernées)
• 300.000€ d'amende par atteinte (et 2 ans de prison en cas d'enrichissement personnel ou préjudice causé à des tiers),
• Sanctions supplémentaires du DPA (dont la suspension du traitement incriminé)

# Mais aussi…

Notification obligatoire en République Tchèque, Estonie, Lituanie, Slovaquie, Afrique du Sud

Notification recommandée en Irlande, Canada, Japon

Notification « indirecte » en Espagne

Notification prévue en Autriche

# Opérateurs et ISP

Le Paquet Telecom vient de passer un cap important.

La directive Européenne 2002/21/CE comprend une disposition prévoyant que tout opérateur de réseau ou de services de communication électronique au public doive avertir leur autorité de contrôle nationale des incidents de sécurité ou de la perte de l'intégrité des données de leurs abonnés, ayant eu un impact significatif.

# Code de la Santé Publique

L'article R1111-14 du code de la Santé Publique prévoit que l'hébergeur de données de santé doit avoir une politique de confidentialité qui comporte notamment les précisions suivantes :

1° En matière de respect des droits des personnes concernées par les données hébergées : ...
e) Les procédures de signalement des incidents graves, dont l'altération des données ou la divulgation non autorisée des données personnelles de santé ; ....

# Que faire ?

S'y préparer (pas de déni ni politique de l'autruche)

Comité ad hoc (comité « Informatique & Libertés ») - leadership CIL
- Direction
- Direction juridique
- Direction opérationnelle concernée (*data owner*)
- Communication
- Gestion de risques, gestion de crises
- Intelligence économique
- Courrier, standard
- Commerciaux
- Informaticiens (récupération des données, préparation du fichier de diffusion)
- Relations sociales
- Relations actionnaires
- RSSI…

Revoir tous ses contrats (art. 35 de la Loi Informatique & Libertés)

# Impacts prévisibles ?

- Davantage de CIL ! Plus de RSSI qui deviennent CIL, plus de pouvoirs pour les CIL
- Mutation défense périmétrique vers sécurité Data Centric
- Prise de conscience Direction – Révision des délégations de pouvoirs
- Analyse de valeur
- Analyse de risques
- Classification des données (synergie avec RSSI et Resp. Intelligence économique)
- IAM, DLP et ERM, Monitoring/Traçabilité, Gestion des configurations, Vulnérabilités Management, Chiffrement, Sécurité des bases de données, Anonymisation, Vulnérabilité Scan, Tests de pénétration, audit de sécurité, etc.
- Consolidation (IBM s'offre Guardium)
- Compliance ISO 27001
- RSSI, PSSI, Charte, sensibilisation
- Impacts induits sur les partenaires et sous-traitants (Cloud computing ?)
- Effet de bord sur les purges de données (également à cause de l'eDiscovery)

# Création d'un groupe de travail

- Lancement au Sénat courant mars 2010
- Etudier tous les aspects de la question (juridiques, organisationnels, responsabilités, assurances, techniques, etc.) du « nombril du CIL »
- Coopération avec l'IAPP et la GDD
- Préparation pour l'éventuel décret
- Prise en compte des effets de bord
    - Exemple 1 : Si l'adresse IP est une données personnelle et qu'il faut notifier toute violation de donnée personnelle, alors…
    - Exemple 2 : Friction entre cette mesure et la loi Godefrain ?
- Anticiper (chantiers de plusieurs mois, voire années)
- Les Opérateurs et ISP, les entreprises qui opèrent en Allemagne, Angleterre et USA vont de toute façon devoir s'y mettre
- Et si cette mesure n'est pas adoptée ?

# Discussion

## www.afcdp.net