



Conférence AFCDP

Notification des violations de traitements de données personnelles

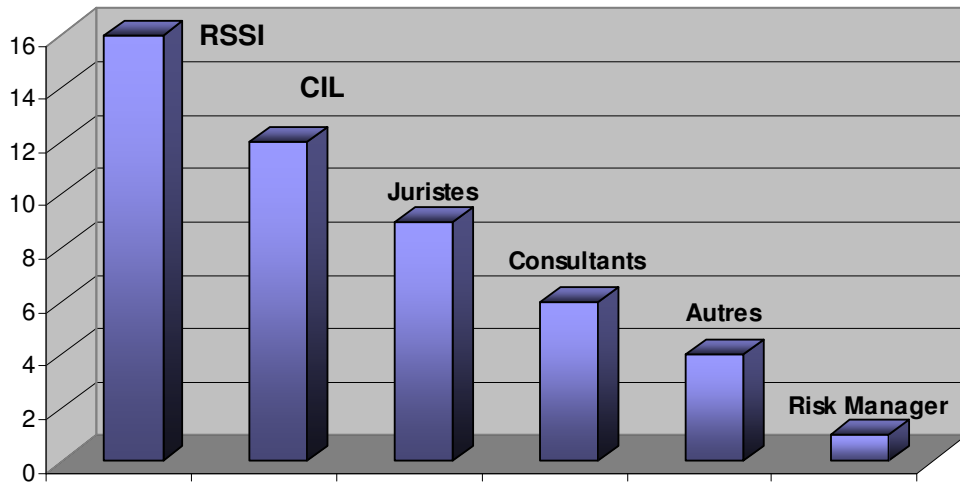
23 mars 2010

Palais du Luxembourg - Paris

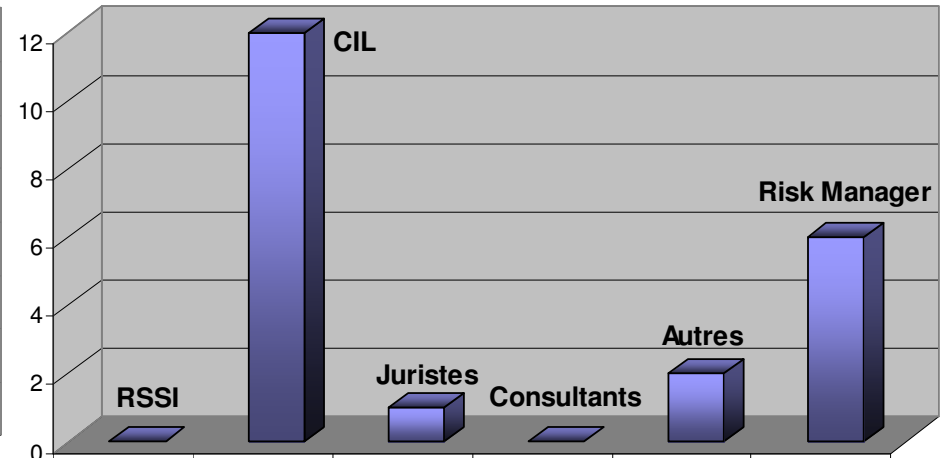
Vers une notification obligatoire des violations de traitements de données ?

Paul-Olivier GIBERT

Président de l'AFCDP,
Directeur de la Conformité et de la Déontologie,
Correspondants Informatique et Libertés

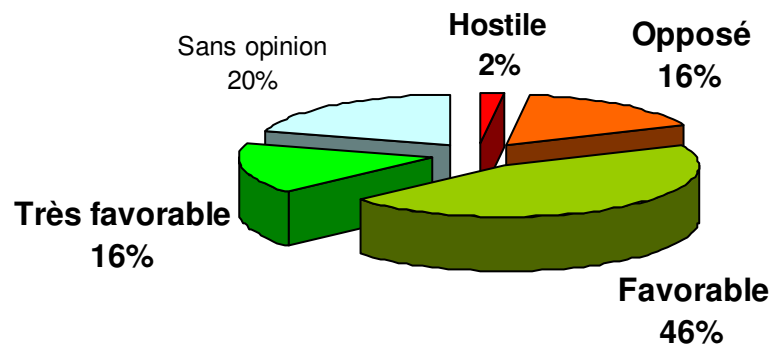


Ma fonction principale

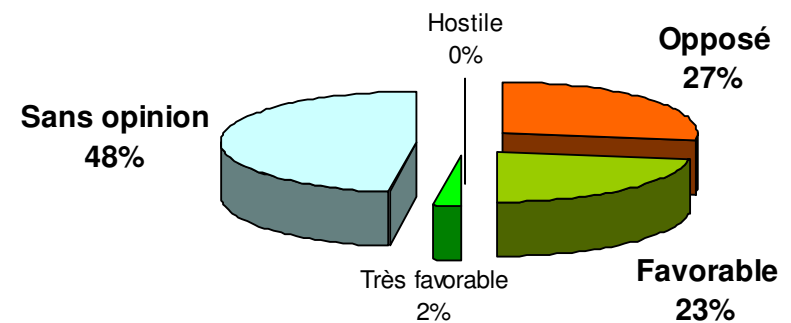


Ma fonction secondaire

Ma position vis-à-vis de la proposition
avant la conférence



La position supposée de mon
Organisme vis-à-vis de la proposition



62% favorables, voire très favorables

Opposés, voire hostiles

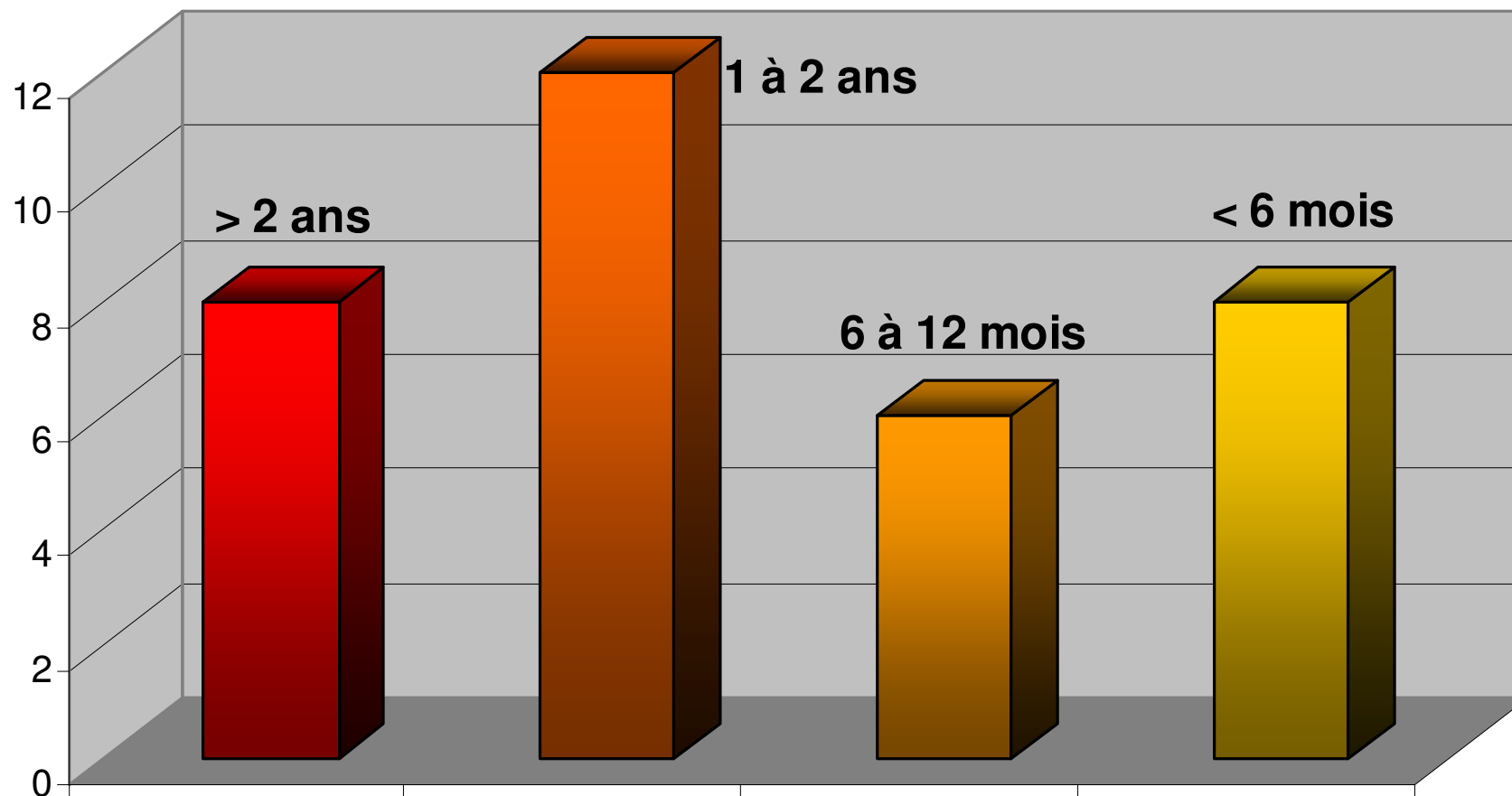
« ... texte trop imprécis... l'avertissement à faire aux personnes est au bon vouloir de la CNIL ... Cela peut engendrer pour l'entreprise des risques juridiques ou financiers supplémentaires, sans apporter en contrepartie une véritable amélioration de la sécurité ni réparer les dommages occasionnés, souvent irréversibles... **Il existe déjà dans la loi actuelle informatique et libertés l'article 34 : il suffit de l'appliquer...** Nous perdrons le contrôle de notre communication, sur le calendrier et la priorisation de la couverture de nos risques. Et qui prendrait en charge les coûts induits ? Le principe général semble bon mais il me semble très difficile de généraliser des dispositifs qui permettent de centraliser les informations et de garantir un résultat exhaustif et uniforme entre les entreprises... Le fait de devoir notifier les failles de sécurité à la CNIL qui dispose du pouvoir de prononcer des sanctions administratives et/ou de transmettre le dossier au parquet ne serait-il pas en contradiction avec le droit de ne pas s'auto-incriminer ? **J'y suis opposé... mais uniquement parce que cela ne me paraît pas réaliste...** il est illusoire de penser que, de lui-même, un responsable de traitement déclarera ses propres failles. Ou alors, **il les camouflera d'une manière ou d'une autre et on aura un effet inverse à celui recherché** ... Il faut prévoir la possibilité pour le CIL d'avertir la CNIL s'il pense que le sujet est traité à la légère dans l'entreprise, et non une obligation »

Favorables, voire très favorables

« ... Enfin un moyen de **casser le mur du silence** prévalant en France sur ces événements... Pour contraindre les entreprises à **se préoccuper réellement de la sécurité** des informations qu'elles manipulent... Cette notification permettra de **limiter les risques en matière d'usurpation d'identité**... Le CIL devrait se voir confier l'appréciation de l'opportunité de saisir la CNIL, dans les seuls cas de violation grave d'un traitement de données à caractère personnel... La tendance semble être internationalement engagée, notamment au sein de l'U.E., **y-a-t-il vraiment possibilité de ne pas suivre ?** J'y vois une garantie forte de conformité à la loi Informatique et Libertés... Obligation de notification uniquement si risque de préjudice aux personnes, sinon notification au CIL avec tenu d'un registre interne tenu à disposition de l'autorité de contrôle... Cinq ans après la refonte de la Loi, il peut paraître normal pour la CNIL de ne plus se contenter que des bonnes intentions... Cette mesure est le meilleur argument dont disposerait un CIL pour convaincre à la fois les dirigeants et les RSSI de leur intérêt à toujours intégrer la protection avant la mise en œuvre d'une application (« **Privacy by Design** »)... Ayant moi-même subi la diffusion de mes données par des opérateurs et ayant travaillé pour/avec des sociétés ayant perdu des données sans que les dirigeants prennent la décision d'en avertir les personnes concernées, je suis très sensibilisé à ce sujet »

Six mois pour appliquer la mesure : Est-ce suffisant ?

Combien de temps faudrait-il, à votre avis, à votre organisme pour se mettre en conformité ?



Plus d'un an :

- « *Au niveau mondial, nous estimons qu'**il nous faudrait quatre à cinq ans** pour respecter une telle obligation»*
- « *Ce serait **une véritable révolution** culturelle pour des européens ! »*
- « *Il me semble difficile que cela prenne moins de temps : la route est longue pour faire entrer une nouvelle culture dans une grande organisation ».*
- « *La prise de conscience de la sécurité est récente dans l'entreprise et nous n'avons pas encore désigné de CIL malgré mes demandes répétées »*
- « ***On part de zéro** : pas d'étude de valeurs ni de risques, faible formalisme concernant la gestion des identités, des rôles et des accès, mais surtout frein conséquent au niveau des équipes SI ».*

Moins d'un an :

- « *Etant déjà soumis à PCI DSS et SOX, un certain nombre de synergies quant aux mesures sont identifiables »*
- « ***Pratique et organisation sont déjà en place** ».*
- « *...compte tenu du faible nombre de failles constatées jusqu'à présent ».*
- « *Notre société dispose des instances et mécanismes de gouvernance, d'organisation et techniques permettant d'être conforme le cas échéant »*
- « *Nous sommes une petite structure »*
- « *Nous avons l'habitude des cadres réglementaires, nous avons un très fort niveau de sécurité : **Nous serions prêts le cas échéant** »*

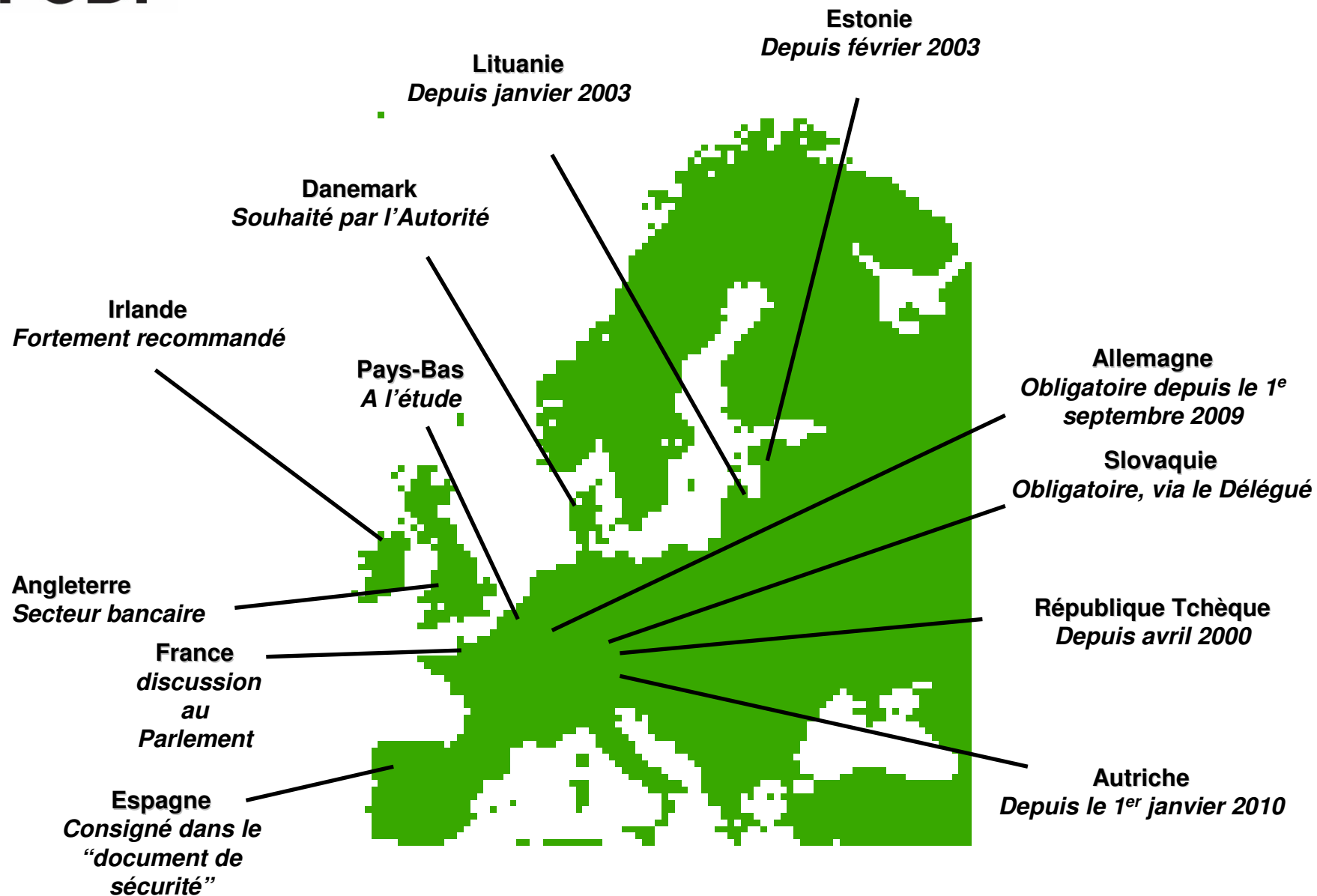


Data Breach : Le paysage légal (actuel et à venir)

Pascale GELLY

Avocat, Administrateur AFCDP et membre du European
Advisory Board de l'IAPP







Proposition de Loi visant à garantir le droit à la vie privée à l'heure du numérique

Texte de la Commission des Lois du sénat du 14.02.2010

« Art. 34. —

Le responsable du traitement met en oeuvre 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.



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 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 et informe la Commission nationale de l'informatique et des libertés.

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.

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 personnelles est tenu à jour par le correspondant «informatique et libertés ».



Que peut-on apprendre de l'étranger ?

Bojana BELLAMY, Director of Data Privacy, Legal, Accenture. Vice-Présidente de l'IAPP

Rosa BARCELO, Legal Adviser at European Data Protection Supervisor

Session animée par Maître Pascale GELLY



Allemagne : Loi Fédérale sur la protection des données personnelles

Section 42a Obligation to notify in case of unlawful access to data

If a private body ... or a public body ... determines that

1. special categories of personal data ...,
2. personal data subject to professional secrecy...,
3. personal data referring to criminal or administrative offences or to suspected criminal or administrative offences, or
4. personal data concerning bank or credit card accounts

it has recorded have been unlawfully transferred or otherwise unlawfully disclosed to third parties,

threatening serious harm to the rights or legitimate interests of data subjects...



... then the private body shall notify the competent supervisory and the data subjects without delay ...

Data subjects shall be informed as soon as appropriate measures to safeguard the data have been taken and notification would no longer endanger criminal prosecution.

The notification of data subjects shall describe the nature of the unlawful disclosure and recommend measures to minimize possible harm.

The notification of the competent supervisory authority shall in addition describe possible harmful consequences of the unlawful disclosure and measures taken by the body as a result.

Where notifying the data subjects would require a disproportionate effort, in particular due to the large number of persons affected, such notification may be replaced by public advertisements of at least one-half page in at least two national daily newspapers, or by another equally effective measure for notifying data subjects.

Notification distributed by the body required to provide notification may be used against that body in criminal proceedings or proceedings under the Administrative Offences Act, or against an associate of the body required to provide notification as defined in Section 52 (1) of the Code of Criminal Procedure only with the consent of the body required to provide notification.



Notification : Quels seraient les acteurs impliqués ?

Gwendal LEGRAND, Responsable de l'expertise technique de la CNIL

Jeanne BOSSI, Secrétaire générale de l'ASIP Santé

Eric WIATROWKSI, Directeur Délégué à la Sécurité, Chief Security Officer, Orange Business Services

Jean-Marc BEIGNON, Expert en Intelligence économique

Christian PARDIEU, Privacy Lead Lawyer de GE en France et CIL de GE Real Estate, membre AFCDP

Session animée par Jérôme SAIZ, journaliste



Notification : Quels seraient les acteurs impliqués ?

Gwendal LEGRAND

Responsable de l'expertise technique
de la CNIL



Notification : Quels seraient les acteurs impliqués ?

Jeanne BOSSI

Secrétaire générale de l'ASIP Santé



Notification : Quels seraient les acteurs impliqués ?

Eric WIATROWKSI

Directeur Délégué à la Sécurité,

Chief Security Officer,

Orange Business Services

Orange Business Services

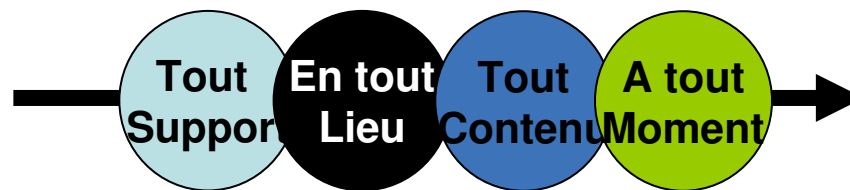
- Orange Business Services associe l'expertise et le savoir-faire d'Equant, d'Orange, de France Télécom et de ses filiales. Et porte la marque Orange sur l'ensemble du marché entreprises - PME, collectivités locales, grandes entreprises et multinationales - partout dans le monde (220 pays et territoires desservis).
- Au service de nos clients entreprises (3.700 multinationales, 130.000 PME), nous mettons à leur disposition des services de communication convergents : réseaux, sécurité, téléphonie, travail collaboratif, mobilité... (320.000 accès IP VPN).
- Une démarche de certification : ISO 9001, SAS70...
- <http://orange-business.com>
- « Chief Security Officer »



- Un Groupe spécialisé dans les hautes technologies, les services financiers, et les médias
- Présent en France depuis près de 60 ans
- Siège Européen de 4 activités,
- 3 Centres d'Excellence mondiaux



La Protection des Données, une Histoire Ancienne chez GE



- En 1979, GE a édité la “Fair Information Practices Policy”
- GE Spirit & Letter: Fair Employment Practices Policy - Privacy Policy
- Adoption de “BCR” : Règles Contraignantes d’Entreprise approuvées par la CNIL en Novembre 2005
- Nomination d’un CIL le 19 décembre 2005





Notification : Quels seraient les acteurs impliqués ?

Jean-Marc BEIGNON

Expert en Intelligence économique



Lancement du groupe de travail AFCDP « Notification des violations de traitements de données personnelles »

Eric DOYEN, RSSI et Responsable de la Sécurité de l'Information du groupe Crédit Immobilier de France, Président du Club 27001, Membre AFCDP

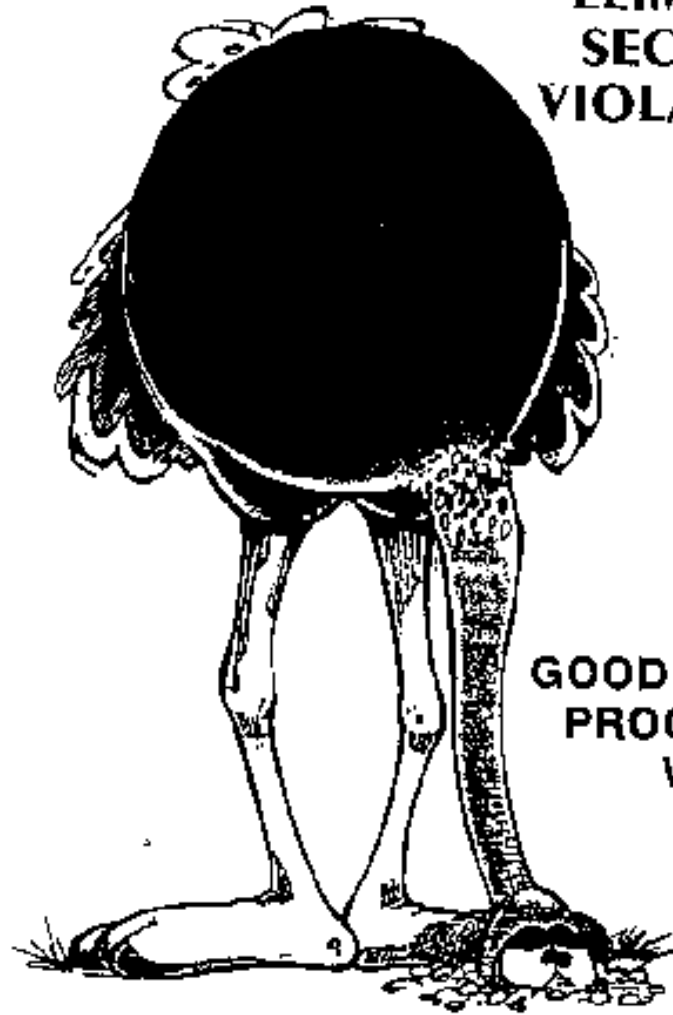
Bernard FORAY, DSSI et CIL Casino Information Technology, Membre AFCDP

Pascale GELLY, Avocat, Administrateur AFCDP

Session animée par Bruno Rasle, Délégué général AFCDP

BURYING YOUR HEAD IN THE SAND

**WON'T
ELIMINATE
SECURITY
VIOLATIONS!**



**GOOD SECURITY
PROCEDURES
WILL!**



Première réunion de travail
le mardi 8 juin après-midi
au Crédit Immobilier de France

www.afcdp.net

1^{ère} réunion de travail : 8 juin

Lexique

Thésaurus : les 5 documents et les 5 sites Web incontournables sur le sujet

F.A.Q : les questions

Audition d'entreprises ayant notifié

2^{ème} réunion de travail : fin juin

Audition de CPO de grandes entreprises américaines
(*IAPP Delegate tour*)

Check-list préventive

Check-list curative



Merci pour votre attention

www.afcdp.net