Le rôle pivot du CIL concernant la notification des violations aux traitements de données personnelles

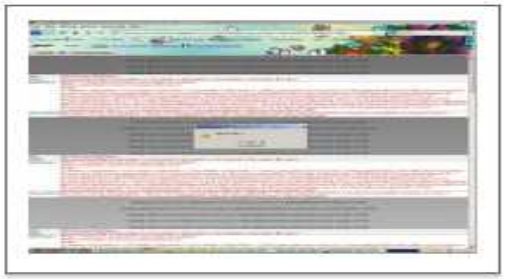
Bruno RASLE
Délégué général de l'AFCDP
Association Française des Correspondants à la protection des Données à caractère Personnel
www.afcdp.net

Deux internautes découvrent par hasard une faille sur Cnil.fr

La faille aurait permis à des individus d'afficher des informations sur le site de la Cnil. Elle a été colmatée avant que des dégâts ne soient constatés.

Damien Bancal | 01net | le 15/09/10 à 15h50 | laisser un avis

La semaine dernière, les responsables du site Internet de la Commission nationale de l'informatique et des libertés (Cnil) on été alertés d'une vulnérabilité sur leur site Web. La faille de type Cross-Site Scripting, connue aussi sous le nom de XSS, aurait pu être exploitée par des individus malveillants pour accéder à certaines parties du site.



La découverte du bug revient à deux internautes français, Romain et Jérôme, alors qu'ils surfaient sur l'espace agenda du site de la Cnil. « *D'abord, avec l'apparition d'une page d'erreur,* explique Romain, *Je n'ai rien tapé de particulier. Juste une* [illegible] *souhaitais* [illegible] par le ser [illegible] informatic [illegible]

Actualités > Sécurité

Une faille sur le site des correspondants Cnil

Un internaute a pu accéder à des données personnelles normalement sécurisées sur le site des correspondants Cnil. Elles n'ont pas été exploitées, mais le site a tenu à prévenir la Commission.

Arnaud Devillard | 01net | le 05/01/10 à 15h16 | 3 réactions

Tweet

Un site Internet qui protège mal ses données personnelles, cela fait déjà mauvais effet. Mais quand il s'agit du site de l'Association des correspondants informatique et libertés, c'est le comble ! C'est pourtant la mésaventure qu'a connue l'Association française des correspondants aux données personnelles (AFCDP), révélée par un article un peu nébuleux du *Canard Enchaîné* du 30 décembre 2009.

- La question n'est pas de savoir SI nous allons connaître un incident nous obligeant à notifier, **mais QUAND**

- Il faut donc **S'Y PREPARER**

- Et qui, **MIEUX QUE LE CIL**, est pertinent pour lancer un tel sujet ?

- **POURQUOI ATTENDRE ?** C'est un chantier de plusieurs années

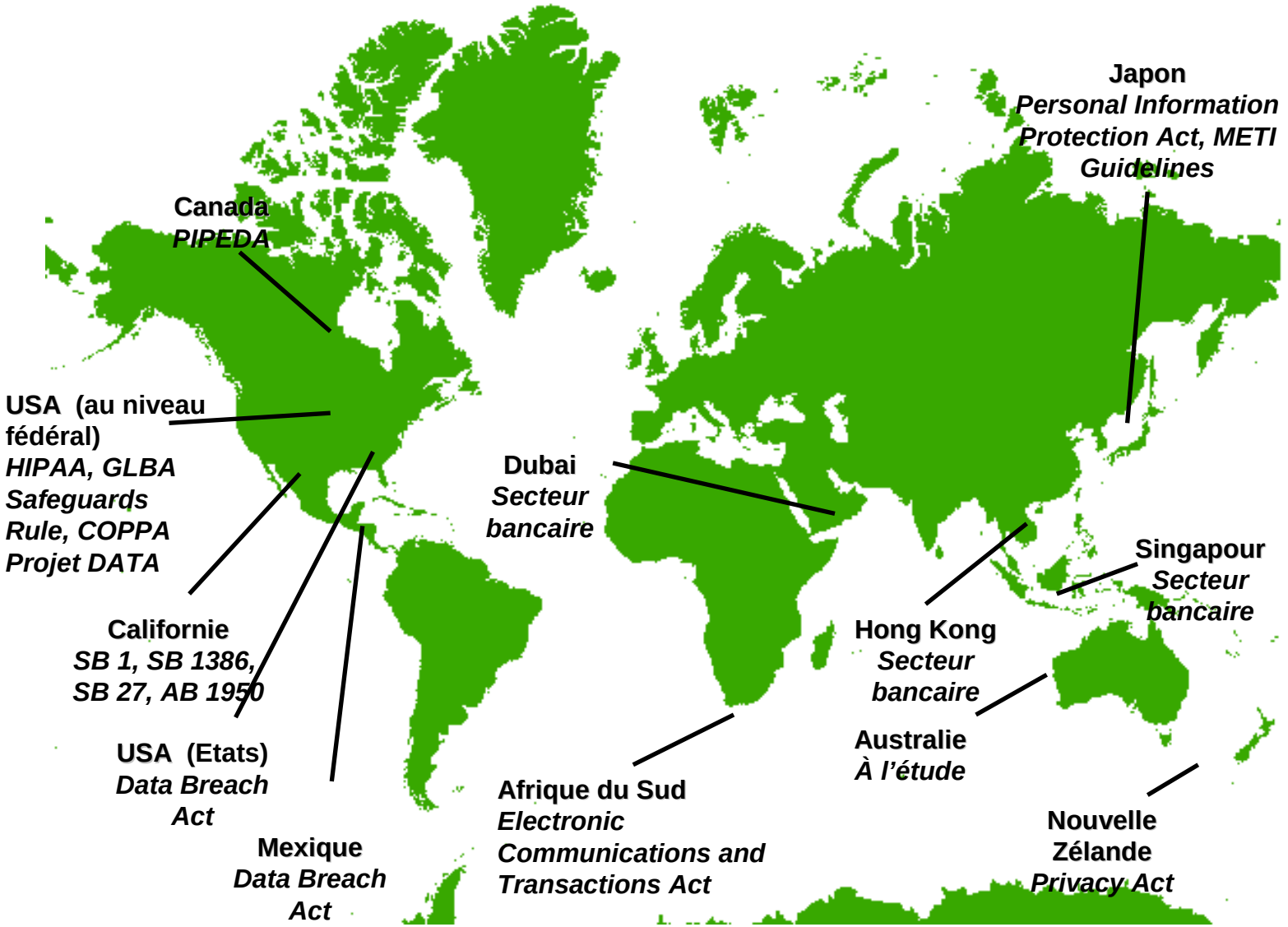
Travaux de l'AFCDP

- Présentation devant l'OSSIR en décembre 2009
- **Groupe AFCDP « Notification des violations aux traitements de données à caractère personnel »**
- Conférence inaugurale au Palais du Luxembourg 23 mars 2010
- Auditions de *Chief Privacy Officer* américains
- Audition du Chef de l'expertise technique de la CNIL
- Groupe « Notification » sur AGORA AFCDP

Ne pas confondre…

- La Proposition de loi Détraigne-Escoffier - 23 mars 2010
- Ce qui se fait à l'étranger hors UE : USA (2003), Canada, Mexique, etc.
- Ce qui se fait en Europe : Allemagne (2009)
- Le Paquet Telecom (ne concerne que les Opérateurs et les FAI) – 21 août 2011
- Le Projet de Règlement européen – 25 janvier 2012

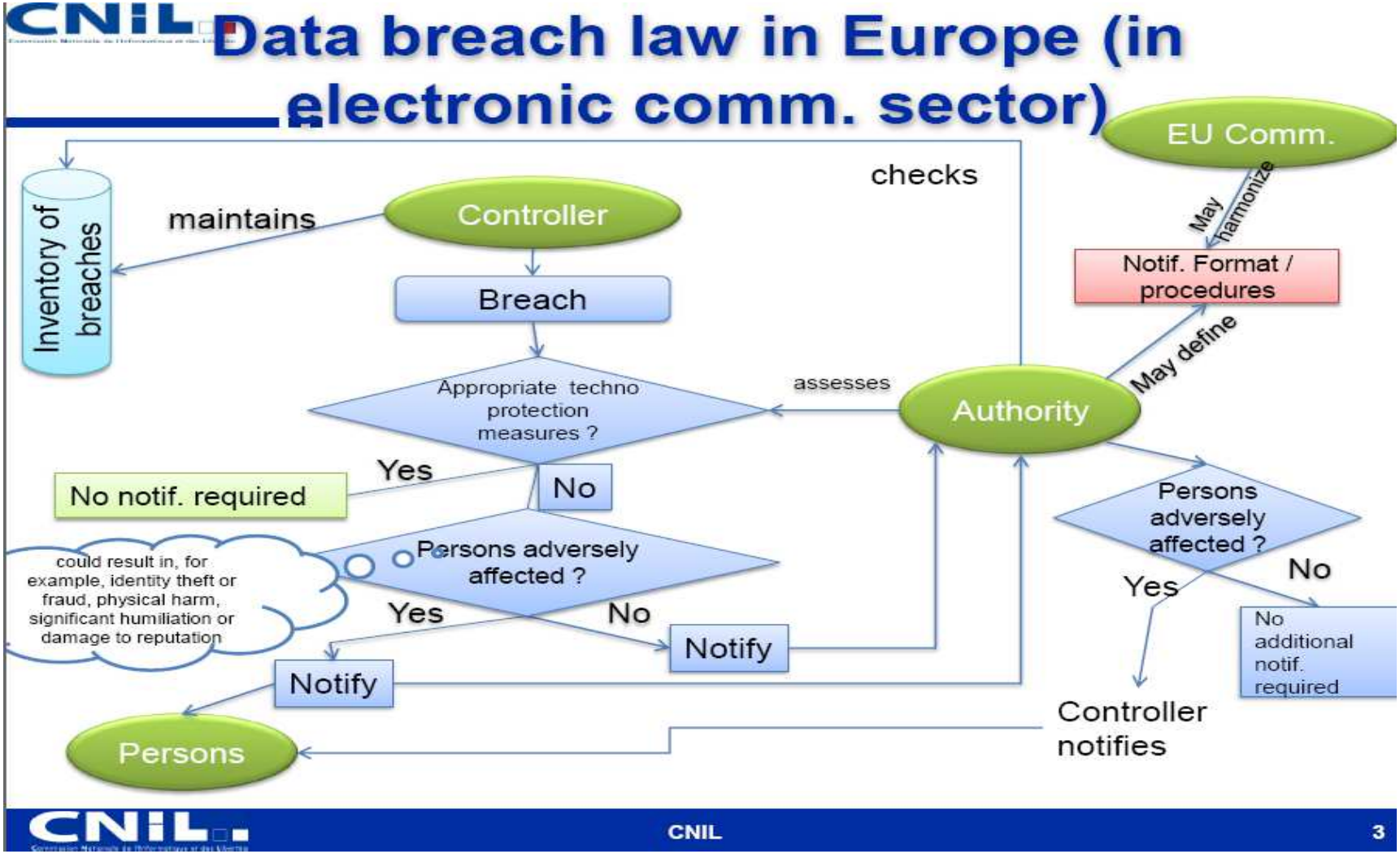
Etranger (hors UE)



Allemagne : Loi Fédérale sur la protection des données personnelles (article 42a)

- Le responsable de traitement doit informer les personnes dont les données personnelles sensibles auraient été divulguées à des tiers non autorisés.
- Les données concernées sont : 1. des données relatives à la race, l'appartenance ethnique ; les opinions politiques, philosophiques ou religieuses ; les orientations sexuelles ; l'appartenance syndicale ; les données de santé. 2. les données soumises au secret professionnel. 3. les données relatives à des infractions ou des condamnations. 4. les données bancaires relatives aux comptes ou cartes de paiement.
- La communication doit intervenir dès que les mesures conservatoires ont été prises.
- La personne concernée doit être informée sur la nature de la compromission et bénéficier de conseils sur les mesures à mettre en œuvre pour limiter les conséquences de la divulgation.
- L'autorité de contrôle compétente doit également être informée, en particulier sur les impacts de la compromission et sur les mesures correctives apportées.

Ordonnance du 21 août 2011



Le rôle pivot du CIL (du DPO)

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)

A traiter…

- Qu'est-ce qu'une violation ?
- Quels sont les critères de notification ?
- Qui prendra la décision de notifier ?
- Suivant quelle méthode objectiverons-nous le risque pour les personnes ?
- Qui décidera de la rapidité avec laquelle nous notifierons ?
- Comment sera sélectionné le media de notification aux personnes ?
- Qui signera la lettre ?
- La lettre comprendra-t-elle des excuses ?
- Qui répondra aux journalistes ? Aux syndicats ? Aux Actionnaires ?
- Qui gérera la relation avec la CNIL ?
- Nous ferons-nous aider ?
- Devons-nous prévoir une assurance ?
- Devons-nous mettre en place des mesures techniques et procédurales ?
- Devons-nous d'ores et déjà introduire un chapitre dans nos contrats de Cloud computing ?
- Que doit-on faire des « near miss » ? Etc.

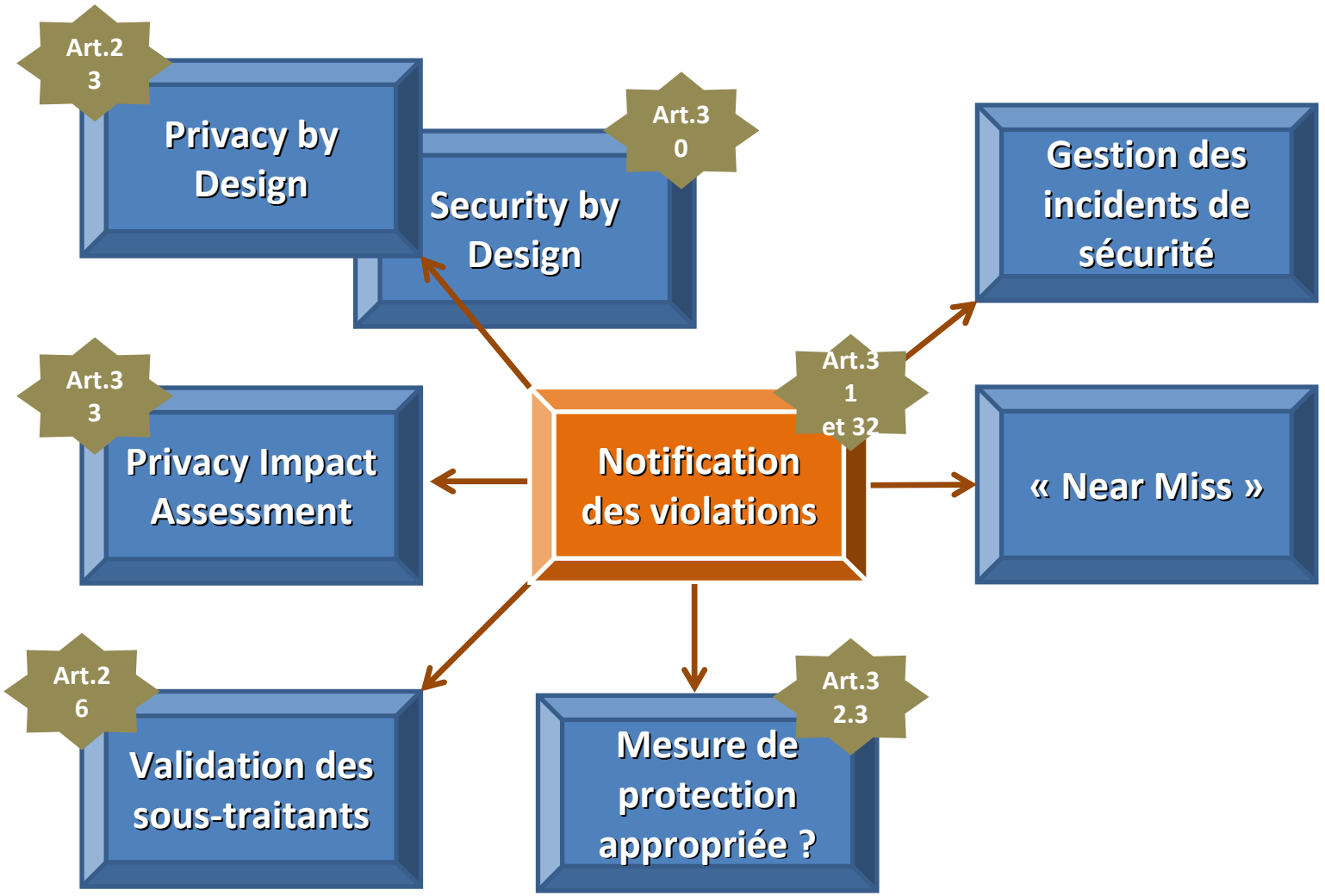
Propositions CEDPO auprès de la Commission européenne

CEDPO propose que le DPO joue un plus grand rôle dans la gestion des éventuelles notifications de violations :

- Analyse de l'incident par le DPO ;
- Prise en compte du contexte ;
- Objectivation de la criticité et évaluation des risques pour les personnes ;
- Conseil au responsable du traitement ;
  - Notification à l'Autorité ;
  - Notification à l'Autorité et aux personnes concernées ;
  - ou Documentation de l'incident ;
- Amélioration (Privacy by Design, PIA, procédures, sensibilisation, etc.)

La responsabilité reste sur le Responsable de traitement.

Boucles d'amélioration



(Source : Commissariat à la protection de la vie privée du Canada)