DU CIL au DPO

Informatica

18 octobre 2016

Hélène LEGRAS / DPO Groupe AREVA
Vice Présidente de l'ADPO

Anthony COQUER / DPO Keolis
Membre de l'ADPO

Zoom sur les données personnelles

- Une sensibilité accrue de la protection des données personnelles, avec le développement des nouvelles technologies
- à l'origine →
  - du règlement communautaire adopté le 14 avril 2016
  - De la loi Lemaire N° 2016-1321 pour une république numérique (adoptée en 1ère lecture à l'Assemblée Nationale le 22 juillet 2016 et au Sénat le 28 septembre 2016 – parue au Journal Officiel le 7 octobre 2016).

AREVA

Un sujet au cœur de l'actualité

données de près de 1,3 million de clients dont leurs nom, prénom, date de naissance, adresse électronique et numéro de téléphone fixe ou mobile

La société ORANGE sanctionnée pour défaut de sécurité des données dans le cadre de campagnes marketing

25 août 2014

un avertissement public

Publication sur Legifrance et sur le site de la CNIL

A la suite d'une faille de sécurité concernant les données de plus d'un million de clients, la CNIL a effectué un contrôle au sein de la société ORANGE et de ses prestataires. Des lacunes de sécurité ayant été identifiées, la formation restreinte prononce un avertissement public.

Un manquement à l'obligation
non excessif des données

La délégation a été informée que la société met à disposition de ses magasins un outil national de gestion des clients pour lesquels une facture a été éditée. Le service après vente (ci-après « le SAV ») utilise le menu « intervention » de cet outil pour gérer les réparations.

A cet égard, la délégation a constaté, dans le menu « intervention » la présence de 5 828 commentaires non pertinents, comme par exemple « CLIENT TRES AGRESSIF », « N'A PAS DE CERVEAU », « LE CLIENT EST CHIANT », « CLIENT TRES CON », « LA CLIENTE EST UNE GROSSE CONNASSE QUI SE CROIT TOUT PERMIS », « CLIENT CASSE COUILLE », « FOLLE », « FORT ACCENT AFRICAIN », « CLIENTE DE CONFESSION JUIVE », « CLIENTE AVEC PROBLEME CARDIAQUE », « CLIENTE A UNE MALADIE NEUROLOGIQUE », « CLIENT ALCOOLIQUE », « ME PASSE SON

2

Un règlement communautaire qui voit le jour

- On a pu l'appeler l'arlésienne !
- Le Groupe de Travail G29 avait adopté, lors de sa séance plénière des 22 et 23 mars 2012, un avis sur les propositions de réforme présentées par la Commission Européenne le 25 janvier 2012.
- Il remplacera la Directive européenne de 1995 et sur de nombreux points la Loi informatique et Libertés française
- **Adoption par Parlement européen le 14 avril 2016**
- **Publication le 4 mai 2016 au JO de l'UE.**
- **Entrée en vigueur le 25 mai 2016**

- **Les entreprises ont une période transitoire de 2 ans pour se mettre en conformité**
- **Eté 2018, période où les CNIL européennes pourront faire leurs 1ers contrôles**

AREVA

28 pays : 28 législations : --→
1 règlement communautaire

28 pays en avril 2016 :

l'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, la Croatie, le Danemark, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lituanie, la Lettonie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Roumanie, le Royaume-Uni, la Slovaquie, la Slovénie et la Suède

Le G29 va devenir « European Data Protection Board » « Comité Européen de la Protection des données »

AREVA

Une évolution juridique

- La loi française 2004-801 du 6 août 2004 et son décret d'application n°2005-1309 du 20 octobre 2005 permettent de nommer des Correspondants Informatique et Libertés

- Le règlement communautaire adopté à Bruxelles uniformise et harmonise les règlementations des 28 pays d'Europe : le Data Protection Officer est consacré !

AREVA

Du CIL au DPO

- **Le Correspondant Informatique et Libertés est facultatif**

- **Le Data Protection Officer / Délégué à la Protection des Données est obligatoire dans certains cas**

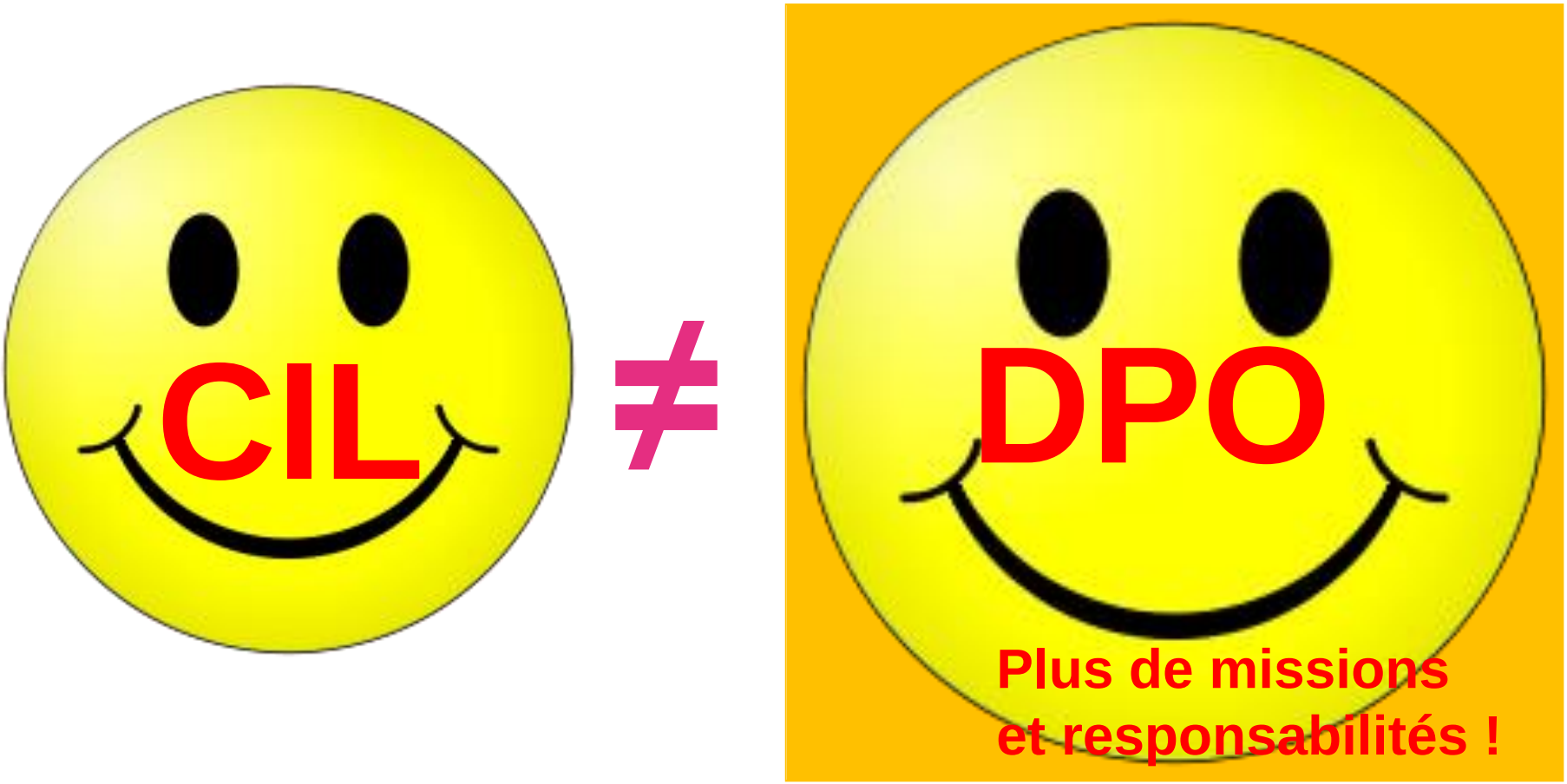
AREVA

DPO obligatoire

L'article 37 du règlement prévoit la désignation du délégué à la protection des données → Obligatoire dans les cas suivants :

- le traitement est effectué par une autorité publique ou un organisme public
- les activités de base du responsable du traitement ou du sous-traitant exigent un suivi régulier et systématique à grande échelle des personnes concernées
- les activités de base du responsable du traitement ou du sous-traitant traitement à grande échelle de catégories particulières de données visées à l'article 9 (données sensibles) et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 (Traitement ne nécessitant pas l'identification de la personne).

La métamorphose du CIL en DPO

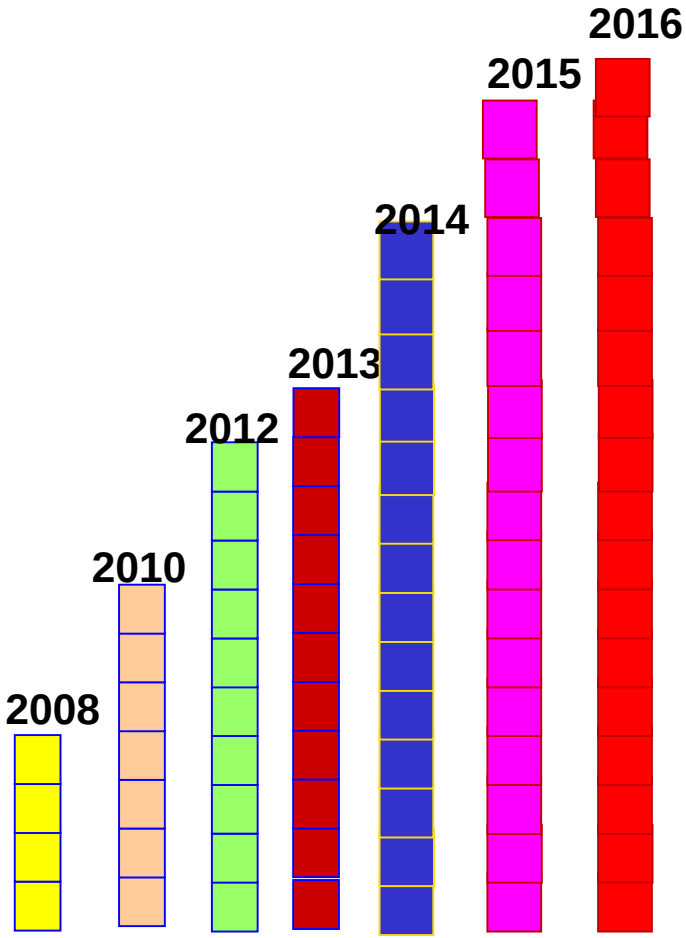


Le DPO sera associé de manière appropriée et en temps utile à toutes les questions touchant à la protection des données personnelles

AREVA

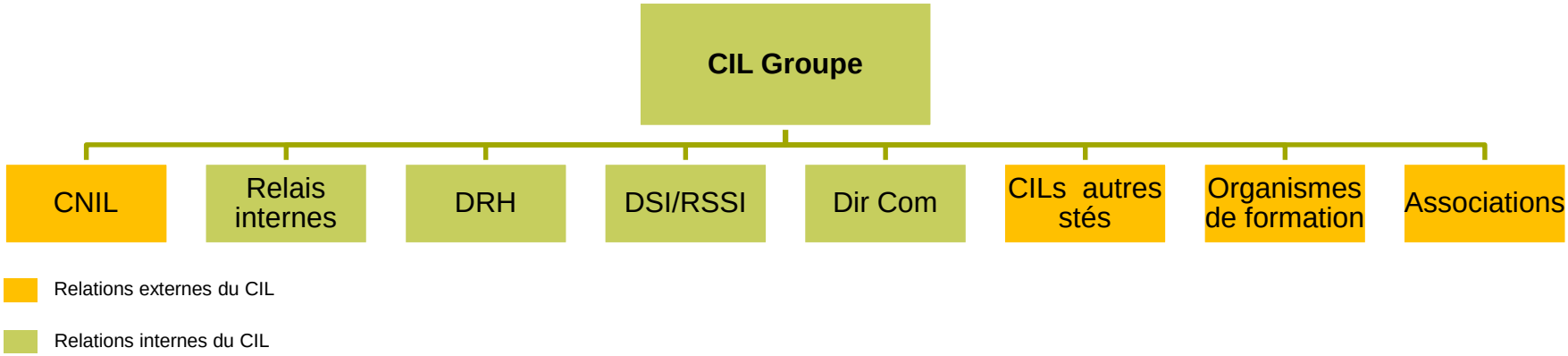
Des CILs / DPO éclectiques

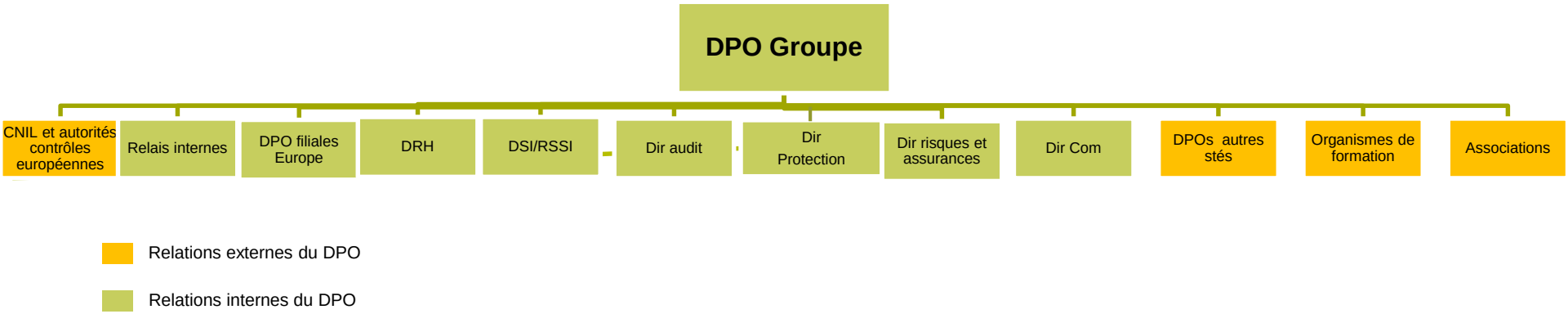
- Juristes, DSI, RSSI, Auditeurs, Commerciaux, Risk managers, Avocats, CIL externes
- Un métier reconnu : un code Rome K1903, « Défense et conseil juridique »
- Un métier récent en évolution constante
  - 2008 : 4 000 organismes ont désigné des correspondants en
  - 2010 : 7 000
  - Fin 2012 : 10 543
  - Fin avril 2013 : 11 000
  - Décembre 2014 : 14 300
  - Décembre 2015 : 16 300
  - Septembre 2016 : 17 500
  - Et demain : le CIL deviendra DPO, en 2018
  - L'**I**nternational **A**ssociation of **P**rivacy **P**rofessionals estime que ce règlement devrait créer 28 000 emplois en Europe



AREVA

Un réseau interne et externe indispensable





AREVA

Le profil

- Le CIL doit connaître son entreprise, l'informatique et le droit. Il est choisi par son entreprise et sa désignation est notifiée à la CNIL. Aucune compétence n'est spécifiée dans la loi de 2004 et le décret de 2005.

- Le DPO sera désigné sur la base de ses qualités professionnelles, de sa connaissance de la législation et des pratiques en matière de protection des données.

AREVA

Autorité de contrôle
la CNIL en France

Le CIL avait des rapports privilégiés avec la CNIL.

Le DPO :

- coopère avec l'autorité de contrôle ;
- fait office de point de contact pour l'autorité de contrôle

Du régime déclaratif à la démarche conformité

- Le CIL veille à la licéité des traitements
- Il répertorie les traitements de données personnelles
- Il forme aux « bonnes pratiques informatique et libertés »
- Il donne des conseils, émet des recommandations, donne d'éventuelles alertes

- le DPO veillera toujours à la licéité des traitements mais Incitera à l'utilisation de la pseudonymisation
- Véritable acteur de la conformité, il fait de l' »accountability » (prouver la conformité), du «Privacy by design » (respect de la protection des données dès la conception) , « Security by default » (sécurité par défaut) et fait des études d'impact pour les traitements à risques

AREVA

La documentation des traitements

Le CIL tient un registre des traitements automatisés de données personnelles

Le DPO tient la documentation des traitements :

- Registre (le RGPD prévoit que ce soit le RT qui le tienne),
- Cahier des charges,
- Spécifications,….

Les droits des personnes

La personne dont les données sont collectées et traitées a des droits

- d'information
- d'accès
- à rectification
- d'opposition s'il est légitime
- à suppression

- Le Délégué à la Protection des Données veillera à ce que ces droits soient toujours respectés
- Le droit à l'effacement et à l'oubli est consacré
- Le DPO veillera à ce que le consentement soit donné par un acte positif clair….. de façon libre, spécifique, éclairée, explicite.

AREVA

La sécurité

Le CIL veille à la sécurité et à la confidentialité des données et empêche qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès

En plus de l'obligation de sécurité, le DPO devra signaler les « violations de données à caractère personnel » dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance.

Indispensable collaboration

DPO/DSI et RSSI

AREVA

La responsabilité

Le CIL est un irresponsable pénal.

C'est le responsable de traitement qui est responsable.

Le sous-traitant n'est responsable que s'il excède les missions confiées par le RT.

Le RT reste le responsable pénal

Voir dans la pratique l'éventuelle responsabilité du DPO, qui doit contrôler la conformité

Le sous-traitant devient responsable

AREVA

Les sanctions

- Sanction pécuniaire qui peut atteindre 150 000 € lors du premier manquement constaté et 300 000 € ou 5% du chiffre d'affaire hors taxes du dernier exercice s'il s'agit d'une entreprise dans la limite de 300 000 €.
- Cette sanction pécuniaire peut être rendue publique ; la formation contentieuse peut également ordonner l'insertion de sa décision dans la presse, aux frais de l'organisme sanctionné.

- Sanction pécuniaire fortement augmentée : **4% du chiffre d'affaires mondial, ou 20 millions d'euros**
- Et toujours la publicité de cette sanction qui porte atteinte à l'image de marque de l'entreprise !

AREVA