Atelier informatique - La réglementation européenne et la protection des données personnelles

- Marguerite Brac de la Perrière (Cabinet Bensoussan)
- Olivier Pantaléo (Provadys)

10/10/2017

provadys

Information Security

RGPD et conformité

Accompagnement pour la conformité à la protection des DCP pour le secteur des Laboratoires de Biologie Médicale

26/09/2017

provadys

LEXING ALAIN BENSOUSSAN AVOCATS

sfil Société Française d'Informatique de Laboratoire

Sommaire

1 Avant propos

LES FAITS

Panorama : attaques croissantes et impactantes

Des hackers plus efficaces

- des hackers organisés
- des méthodes perfectionnistes
- des attaques diversifiées

Des enjeux et intérêts croissants

- des motivations financières
- des motivations idéologiques
- des motivations stratégiques

Des entreprises vulnérables

Forte dépendance des SI

Manque de préparation aux attaques

3,7 Milliards d'€
coût 2015 en France - figurant dans le Top 10 des pays où la cyber criminalité est la plus active

80 %
des organisations adhérentes au CESIN ont été ciblées en 2016

+ 30% (monde)
+ 50% (France)
Attaques 2014 – 2015

255 jours
durée moyenne d'une compromission

80%
de la cybercriminalité est liée à des bandes organisées transfrontalières et représente un coût financier plus important que les coûts combinés des trafics de cocaïne, marijuana et héroïne.
(Interpol)

1500 attaques
Fraudes au Président - depuis 2012
450 Millions d'€ détournés en France en 2015

Données à caractère personnel
Données les plus volées en 2015
2018 Nouvelle législation

+260%
de Ransomware en France en 2015
(5ème rang mondial)

35 %
des incidents sont générés par les collaborateurs

68% des entreprises
ont fait l'objet d'au moins une
cyber-attaque au cours
des 24 derniers mois.

50% des attaques concernent
les TPE-PME

Le saviez-vous ?

2 Enjeux de la réforme

Contexte et objectif

UN RÈGLEMENT EUROPÉEN

- Objectif : Mettre la protection des données personnelles des citoyens au cœur des organisations
- Application: 25 mai 2018
- Zone: les 28 pays de l'Union Européenne
- Scope: tous les traitements de données personnelles en cours et à venir

Une approche REPRESSIVE

- Suppression d'un système de déclaration préalable (déclaration « CNIL ») vs un programme d'autorégulation intégrant une approche par les risques
- Sanctions dissuasives :
  - Manquements mineurs : 10 M€ jusqu'à 2% du chiffre d'affaire annuel mondial
  - Manquements majeurs : 20 M€ jusqu'à 4% du chiffre d'affaire annuel mondial

Rappel

Qu’est ce qu’une donnée à caractère personnel?

« toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d’identification ou à un ou plusieurs éléments qui lui sont propres ».

En pratique? Nom, prénom, email, n° téléphone, adresse, n° carte d’identité, une photo, adresse IP, n° unique de device ...

Qu’est ce qu’un traitement de donnée à caractère personnel?

« toute opération ou tout ensemble d'opérations portant sur des données personnelles, quel que soit le procédé utilisé, et notamment : la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction »

En pratique? Collecte, gestion, stockage, transfert, suppression, accès …

Qui ?

Tout individu « personne physique »
En pratique? patients, partenaires, salariés, intérimaires, prestataires, fournisseurs…

Contexte et objectif

Points majeurs

- **Un principe *d'Accountability* à déployer pour tous nos traitements**
  Le LBM doit pouvoir démontrer la conformité de ses opérations avec le Règlement
- **Des moyens techniques et organisationnels à mettre en place**
  (DPO, tenue de registre, PIA, Privacy/Protection by design & by default)
- Un nouveau régime de responsabilité à encadrer avec nos prestataires
- Le renforcement du droit des personnes
- **Un régime répressif** : 4% CA mondial pourra être réclamé en cas de non respect du règlement

Un principe directeur et quatre piliers

Protection des citoyens et de leurs données

Protéger les données des citoyens de l'Union Européenne, garantir les droits des personnes concernées par les données collectées.

PIA ou EIVP

Évaluer les impacts sur la vie privée des personnes concernées

Security by Default

Assurer à tous les niveaux et dans les contrats que les données bénéficient du niveau de protection adéquat

Privacy by Design

S'assurer, dès la conception des traitements, que seules les données strictement nécessaires sont collectées et manipulées

Accountability

Maintenir la conformité et s'assurer de sa capacité à démontrer la conformité ainsi que son amélioration continue. Démontrer à travers des contrôles et de la documentation la maitrise de la protection des données à caractère personnel

2

Présentation du code de conduite et du PIAF appliqués au secteur d'activité des LBM

Composition

- **Composition du code de conduite**
  - Présentation du document
  - Présentation des modalités de validation par l'autorité de contrôle lors de l'adoption et des modifications ultérieures
  - Identification de l'organisme réalisant le suivi du code de conduite et des modalités de contrôles obligatoires
  - Présentation du cadre légal applicable au LBM
  - Présentation des exigences juridiques et techniques communes à toutes les activités des LBM
  - Description des processus communs à tous les LBM et les exigences juridiques et techniques qui s'appliquent par processus métiers

Composition

- **Composition du PIAF**
  - Présentation de la méthodologie d'analyse d'impact sur la vie privée à destination des LBM afin :
  - De faciliter la sélection et la valorisation des risques sur la vie privée sur la base des risques partagés par tous les LBM
  - D'identifier les risques sur la vie privée spécifiques aux LBM

Composition

- **Associés au code de conduite et au PIAF**

  → Une mallette opérationnelle :

  - Les référentiels, textes de lois, décrets avec explications de texte
  - Exemples de contrats,
  - Fiches types de recueil de consentement,
  - …

Qu’est ce que le PIA ?

Qu’est ce qu’un PIA :

- Un processus permettant de :
  - évaluer la nécessité et la proportionnalité ;
  - gérer les risques sur les droits et libertés.
- Un outil pour bâtir sa conformité et la démontrer

Sur quoi un DPIA porte-t-il ?

- Un traitement (généralement)
- Des traitements similaires
  - Traitements identiques mis en œuvre par plusieurs responsables de traitements (RT)
  - Traitements partagés par plusieurs RT
  - Traitements similaires en termes de finalités, fonctionnalités, risques, technologies, etc.

Quels traitements font l'objet d’’un PIA :

- Tous ceux créés après mai 2018
- Ceux créés avant, dès qu’ils changent après mai 2018
  - Contexte : finalité, fonctionnalités, etc.
  - Composants des risques : données, supports des données, sources de risques, impacts potentiels, menaces

À quel moment du cycle de vie d’un traitement un PIA doit-il être mené ?

- Avant la mise en œuvre du traitement
- Principe de Privacy by design

Qu'est ce qu'une analyse d'impact (PIA) ?

Identifier l'impact sur la vie privée des personnes concernées, dont on manipule les données, en cas de faille de sécurité

- Le risque correspond à l'IMPACT sur la vie privée des personnes concernées.

- L'impact est estimé selon deux critères :
  - La difficulté à identifier la personne concernée à partir des données à caractère personnel disponibles.

  Question : Quels moyens doivent être mis en œuvre pour identifier la personne concernées avec les données à caractère personnel en notre possession ?

  - Le caractère préjudiciable de la violation sur les personnes concernées.

  Question : quelle est la conséquence potentielle de la violation ? (sur la base d'une échelle identifiée)

-> L'impact est d'autant plus considéré comme critique en raison de la typologie de données, les données de santé et du secret médical.

3 Démarche de mise en conformité

Une démarche en trois temps

1. **Elaboration du code de conduite**

2. **Elaboration du PIAF**

3. **LBM Pilote : Déploiement**

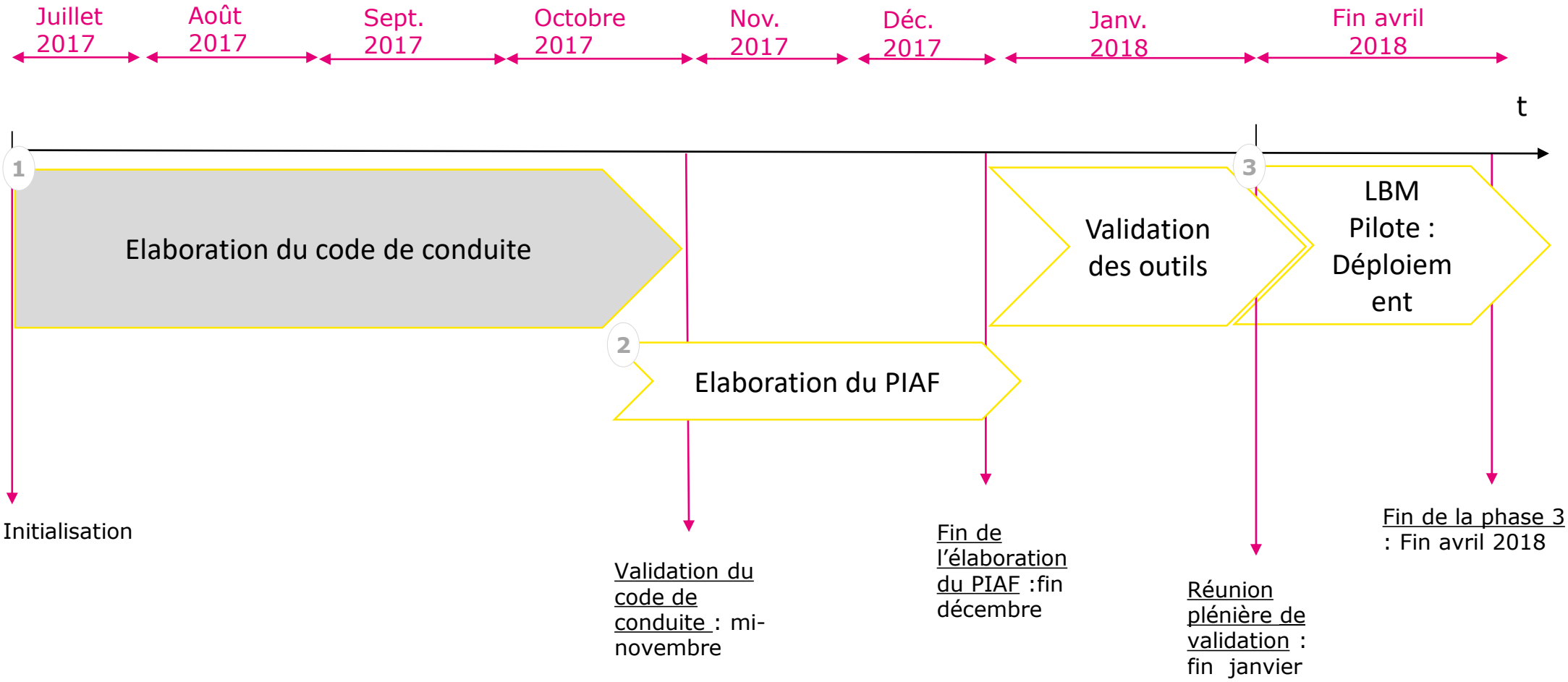
Périmètre considéré dans la définition du code de conduite et du PIAF pour les LBM

- **Périmètre des personnes concernées**

→ Focus sur les données à caractère personnel des patients

→ Exclusion des données à caractère personnel des fonctions supports (Ressources Humaines, Comptabilité…).

Planning


Juillet 2017
Août 2017
Sept. 2017
Octobre 2017
Nov. 2017
Déc. 2017
Janv. 2018
Fin avril 2018
t
1
Elaboration du code de conduite
2
Elaboration du PIAF
3
Validation des outils
LBM Pilote : Déploiement
Initialisation
Validation du code de conduite : mi-novembre
Fin de l'élaboration du PIAF :fin décembre
Réunion plénière de validation : fin janvier
Fin de la phase 3 : Fin avril 2018

MERCI

provadys.com