Security for Data Scientists
Lecture 1

Pascal Lafourcade

LIMOS

UNIVERSITÉ Clermont Auvergne

November 2020

Notation

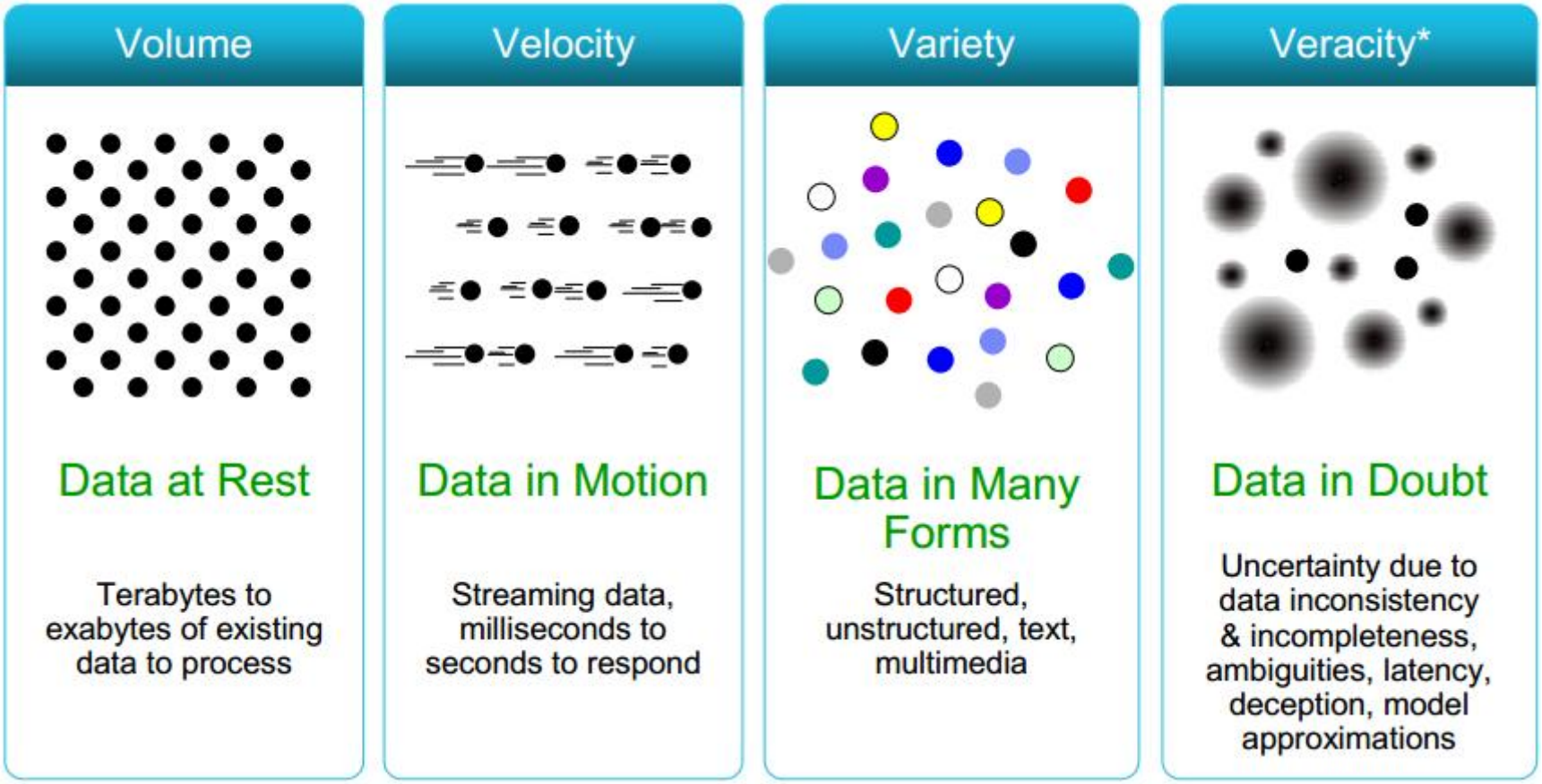
$2 \times$ 2h00 + 2h00 + 2h00 TP

Note = 70% Projet PIA + 30% TP

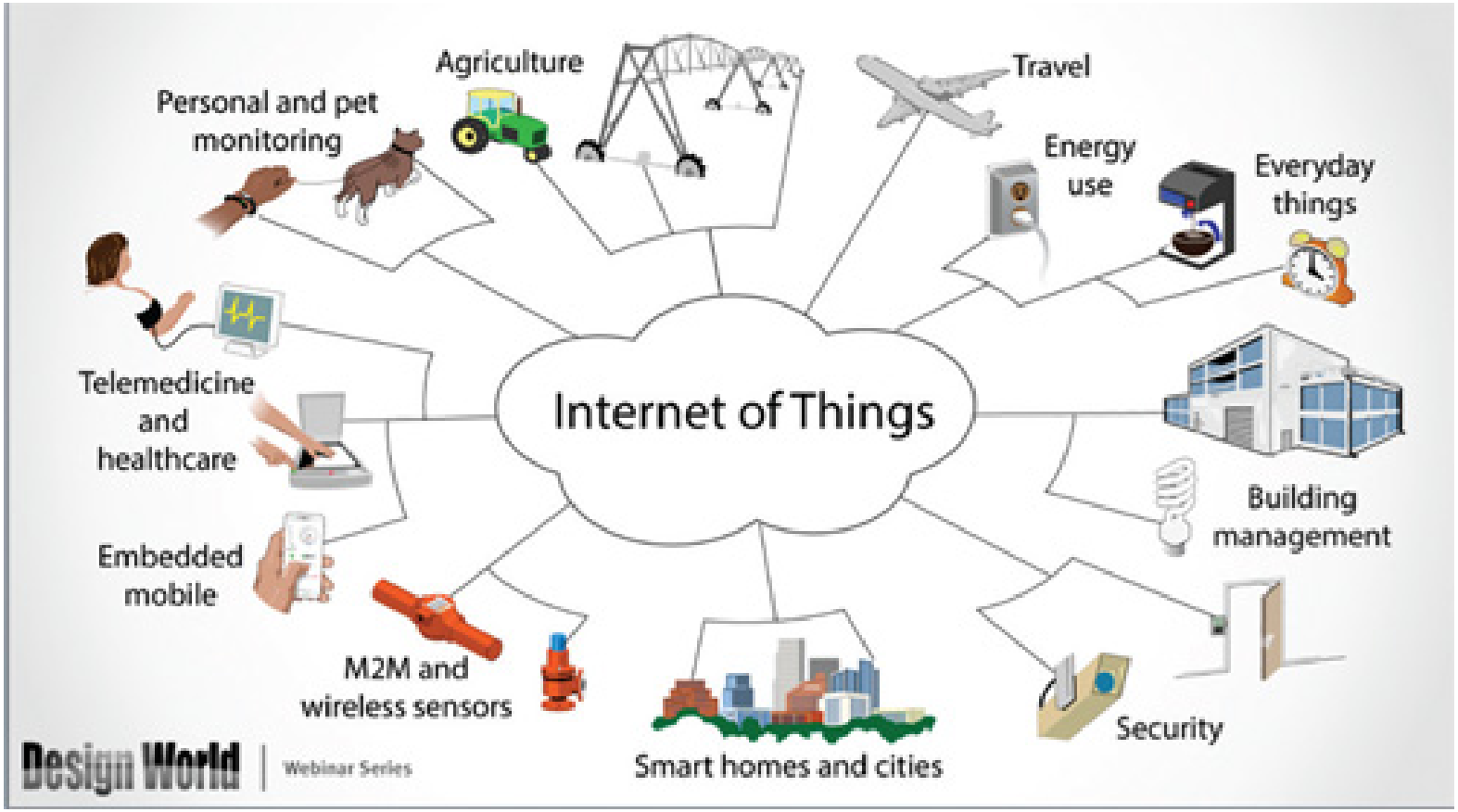
TP : python + REDIS + SSE

Outline

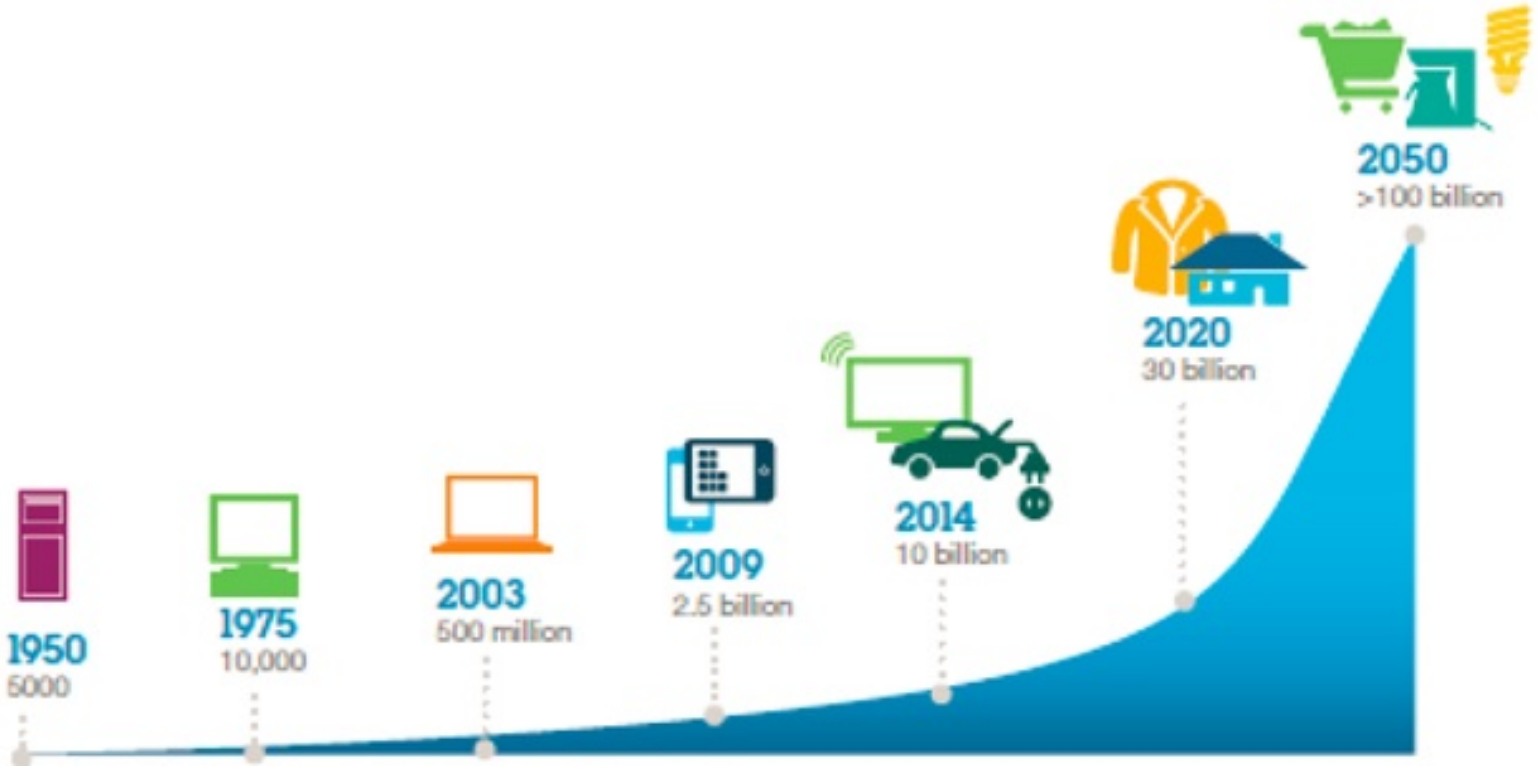
Big Data


Volume
Data at Rest
Terabytes to exabytes of existing data to process
Velocity
Data in Motion
Streaming data, milliseconds to seconds to respond
Variety
Data in Many Forms
Structured, unstructured, text, multimedia
Veracity*
Data in Doubt
Uncertainty due to data inconsistency & incompleteness, ambiguities, latency, deception, model approximations

IoT

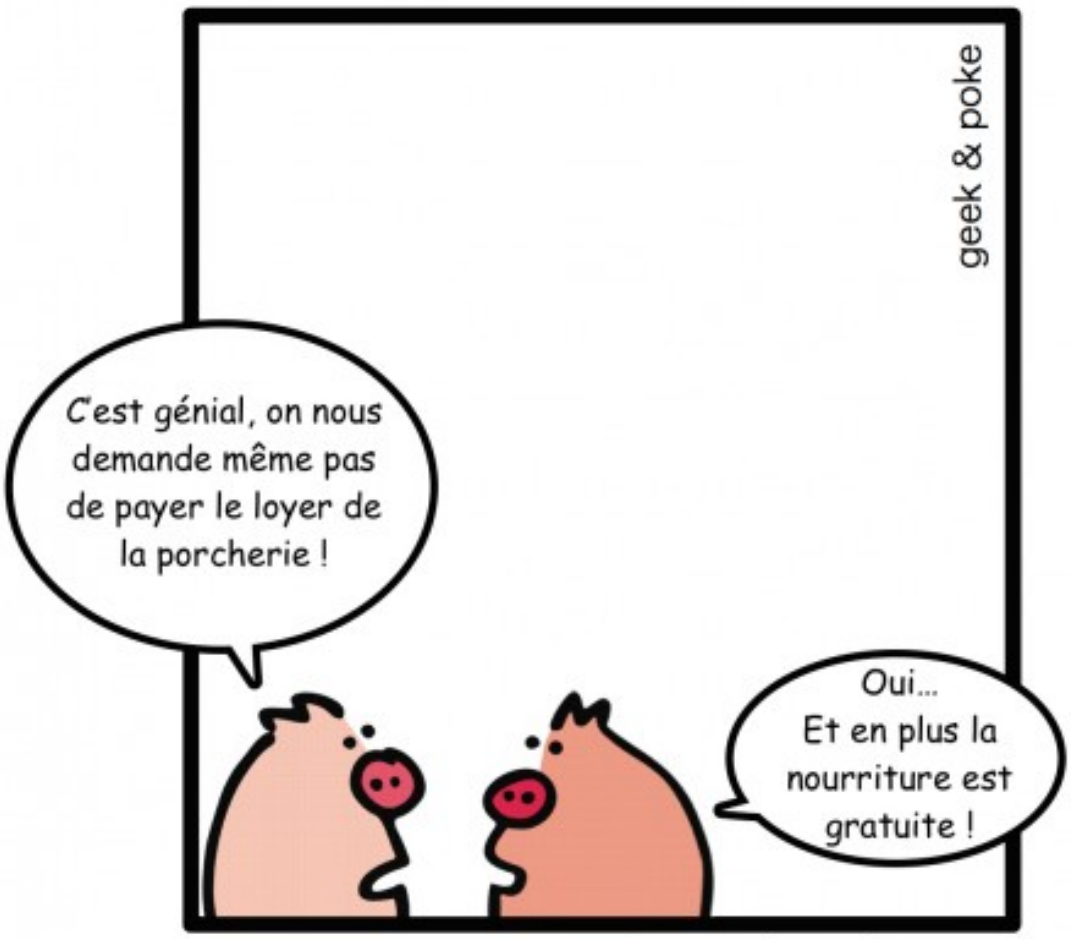

Internet of Things
Agriculture
Travel
Personal and pet monitoring
Energy use
Everyday things
Telemedicine and healthcare
Building management
Embedded mobile
M2M and wireless sensors
Smart homes and cities
Security
Design World
Webinar Series

IoT


1950
5000
1975
10,000
2003
500 million
2009
2.5 billion
2014
10 billion
2020
30 billion
2050
>100 billion

Big Data and Security

Free ?



Deux cochons discutant du modèle « gratuit »

Free ?

If it is free then you are the product

Data Privacy ?

Outline

CNIL créé en 1978

Commission nationale de l'informatique et des libertés

BUT

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

ANSSI créée le 7 juillet 2009.

STAD

Système de Traitement Automatisé de Données

"Tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité".

Aucune définition précise dans la loi

Dans les faits c'est presque tout :





3 acteurs

Utilisateur

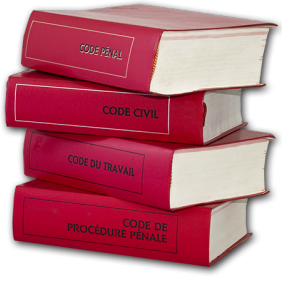
Responsable

Pirate

L'utilisateur

Droits

- D'accès : demander directement au responsable d'un fichier s'il détient l'intégralité de ces données
- De rectification
- D'opposition dêtre dans un fichier
- Déréférencement sur le web par rapport au nom et prénom



Le responsable

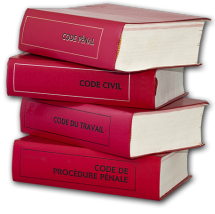
Et le sous-traitant via le contrat.

Devoirs

- Déclarer les traitements de données personnelles
  5 ans & 300 000
- Prendre toutes précautions pour la sécurité des données selon
  - la nature des données
  - les risques présentés par le traitement

  5 ans & 300 000

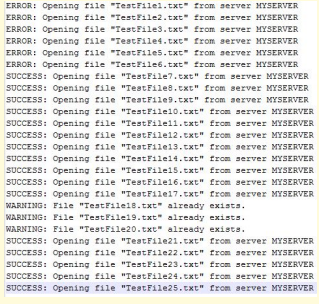
Lois informatique et libertés : Article 22 et Article 34.
Guide de la CNIL : La sécurité des données personnelles



Conservation des logs

LCEN 2004

- 1 an pour les logs (jurisprudence de la BNP Paribas)
- Décret 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne:
  - ip, url, protocole, date heure, nature de l'opération
  - éventuellement les données utilisateurs
  - éventuellement données bancaires
  - accédées dans le cadre d'une réquisition
  - conservées un an
  - données utilisateurs pendant un an après la clôture



Article 226-20 : les logs ont une date de péremption

Le pirate

Risques (STAD (Article 323-1))

- accès frauduleux ou maintien frauduleux de l'accès **2 ans & 60 000**
- suppression ou modification des données **3 ans & 100 000**
- si données à caractère personnel **5 ans & 150 000**
- altération du fonctionnement **5 ans et de 75 000**
- si données à caractère personnel **7 ans & 100 000**

Risques encourus

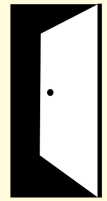
En pratique

- Atteintes aux intérêts fondamentaux de la nation (Sécurité nationale) Article 410-1 à 411-6
- Secret des communication pour l'autorité publique et FAI **3 ans et 45 000** Article 432-9
- Usurpation d'identité **5 ans et de 75 000** Article 434-23
- Importer, détenir, offrir ou mettre à disposition un moyen de commettre une infraction est puni

Sauf si

Pas de condamnation si

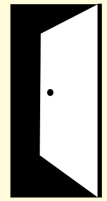
- aucune protection
- aucune mention de confidentialité
- accessible via les outils de navigation grand public
- même en cas de données nominatives



Sauf si

Pas de condamnation si

- aucune protection
- aucune mention de confidentialité
- accessible via les outils de navigation grand public
- même en cas de données nominatives



Il est donc important de protéger ces données

Outline

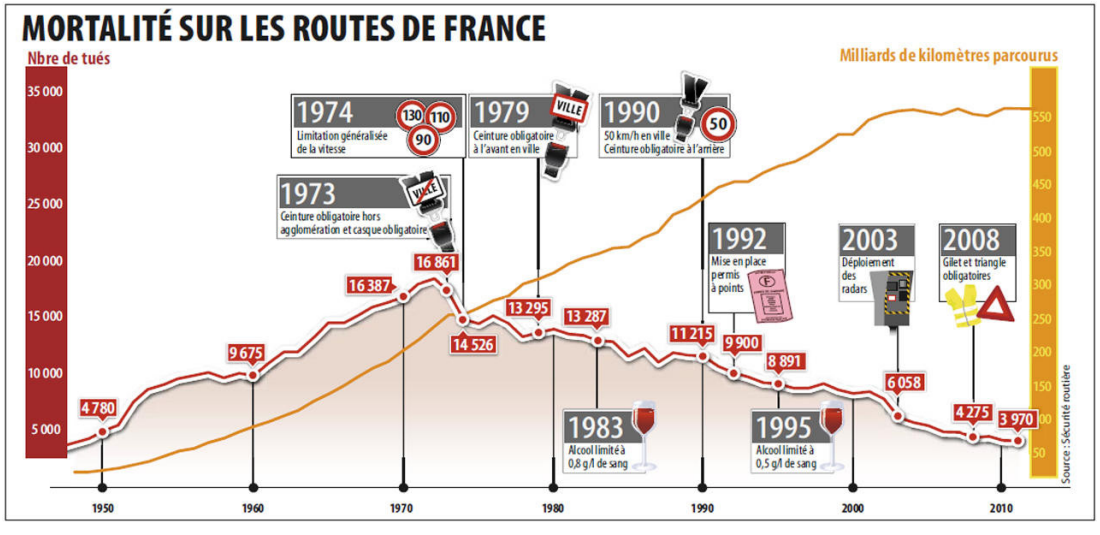

RIP


RIP


NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS 12


RIP


NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS 12


MORTALITÉ SUR LES ROUTES DE FRANCE
Nbre de tués
Milliards de kilomètres parcourus
35 000
30 000
25 000
20 000
15 000
10 000
5 000
550
500
450
400
350
300
250
200
150
100
50
1974
Limitation généralisée de la vitesse
130
110
90
1979
Ceinture obligatoire à l'avant en ville
VILLE
1990
50 km/h en ville
Ceinture obligatoire à l'arrière
50
1973
Ceinture obligatoire hors agglomération et casque obligatoire
VILLE
1992
Mise en place permis à points
2003
Déploiement des radars
2008
Gilet et triangle obligatoires
4 780
9 675
16 387
16 861
14 526
13 295
13 287
11 215
9 900
8 891
6 058
4 275
3 970
1983
Alcool limité à 0,8 g/l de sang
1995
Alcool limité à 0,5 g/l de sang
1950
1960
1970
1980
1990
2000
2010
Source : Sécurité routière

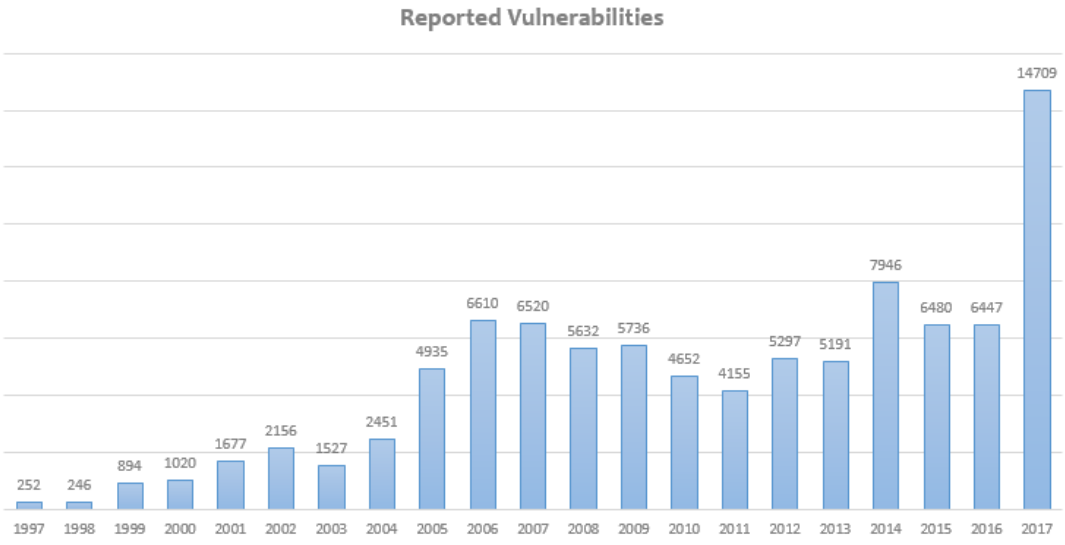
L'argus

Sanctions

20 millions

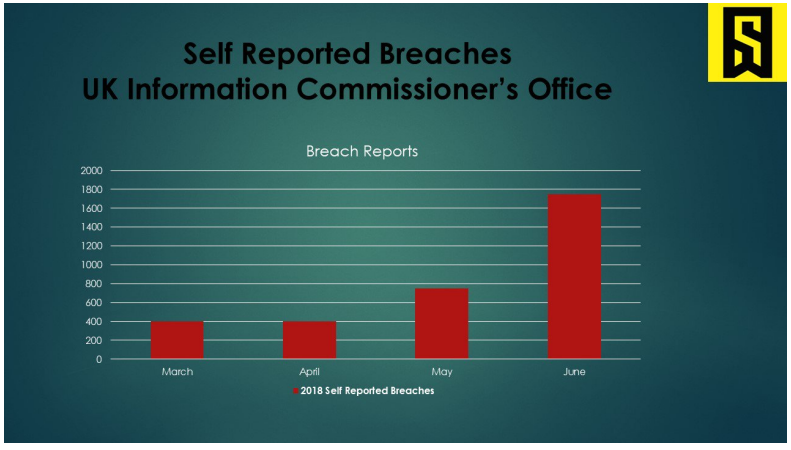
ou 4 %

En France la CNIL devient autorité de contrôle



Règlement Général sur la Protection des Données

GDPR : General Data Protection Regulation



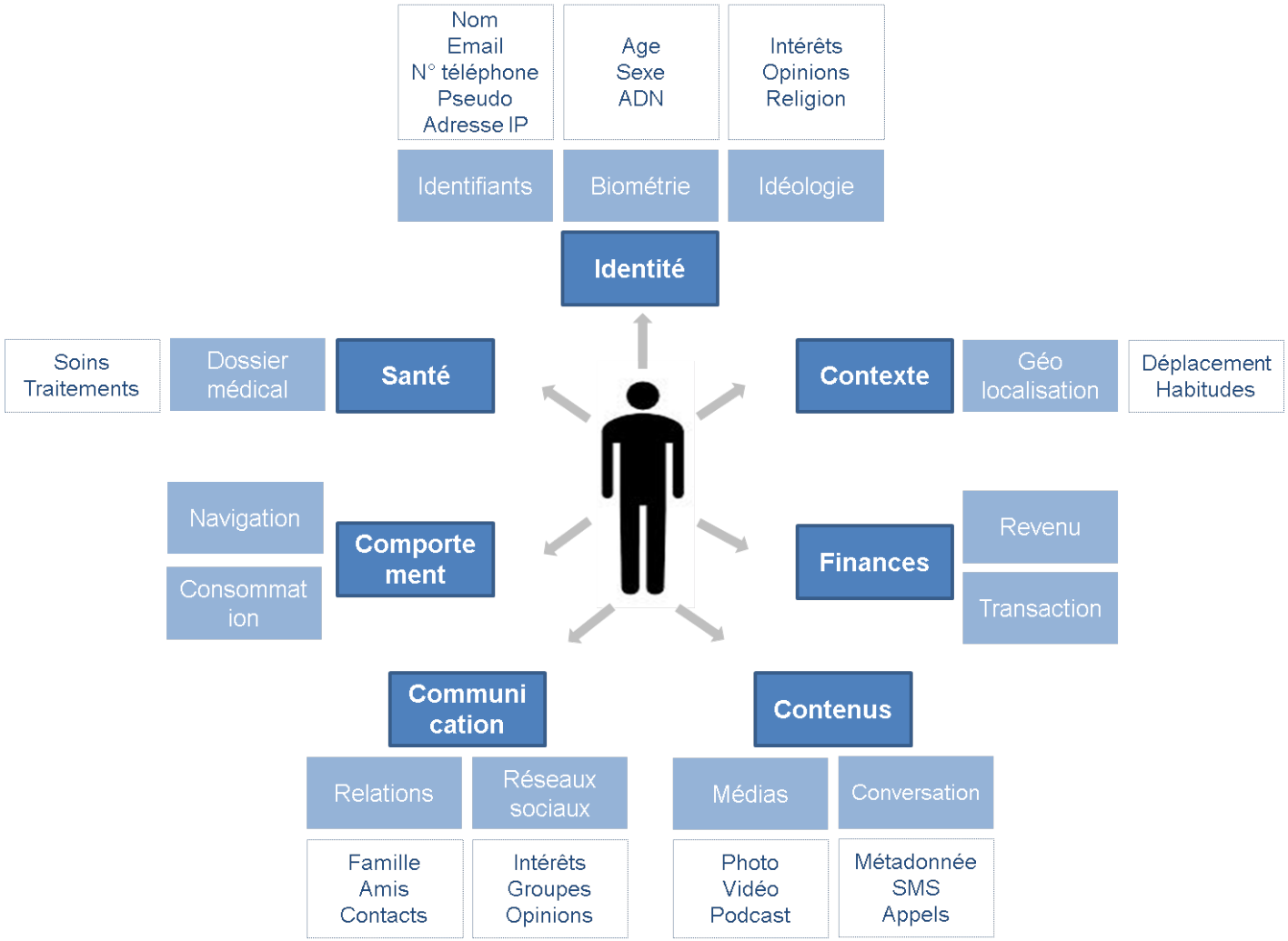
Qui est touché ?

TOUT LE MONDE !

5 types de données

1. neutres
2. personnelles
3. sensibles
4. pseudonymisées
5. anonymisées

Qu'est-ce qu'une donnée personnelle ?



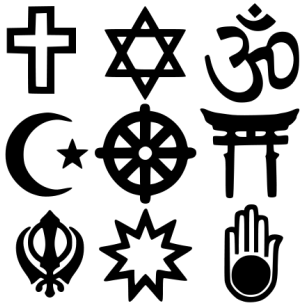
Toutes informations relatives à une personne physique qui peuvent être utilisées pour re-identifier la personne

Qu'est-ce qu'une donnée personnelle ?

Information qui permet d'identifier une personne physique, directement ou indirectement.

- un nom,
- une photographie,
- une adresse IP,
- un numéro de téléphone,
- un identifiant de connexion informatique,
- une adresse postale,
- une empreinte,
- un enregistrement vocal,
- un numéro de sécurité sociale,
- un mail, etc.

Qu'est-ce qu'une donnée personnelle **sensible**?



Collecte sans consentement préalable écrit, clair et explicite

Safe Harbor: 07 octobre 2015

- Invalidation par la Cour de Justice de l'Union européenne
- Une décision clé pour la protection des données,
- Quel niveau de protection des données personnelles transférées aux Etats-Unis ?

Safe Harbor: 07 octobre 2015

- Invalidation par la Cour de Justice de l'Union européenne
- Une décision clé pour la protection des données,
- Quel niveau de protection des données personnelles transférées aux Etats-Unis ?

Règlement Général sur la Protection des Données (RGPD)
Règlement no 2016/679 adopté le **27 avril 2016**.
Mise en application le **25 mai 2018**.

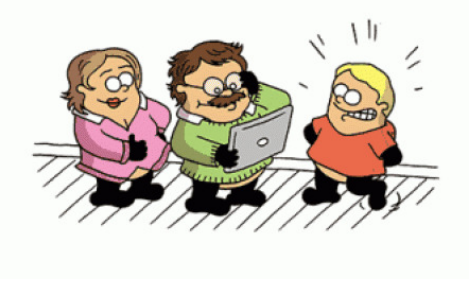
Plus de droits pour vos données !

Sanction

Plus de transparence

Droit à l'oubli

Guichet unique



Protection des mineurs

Portabilité

Objectifs?

Renforcer la transparence:

- Quelles données sont collectées?
- Dans quels buts?
- Pour combien de temps?

Faciliter l'exercice des droits

- droit à la rectification
- droit à la portabilité : récupération et communication à un autre traitement
- droit à l'oubli : suppression de données personnelles
  - dès qu'elles ne sont plus nécessaires au traitement
  - dès que le consentement de l'utilisateur a été retiré
  - dès que la personne s'y oppose

Règles d'or de la CNIL

1. Licéité du traitement
2. Finalité du traitement
3. Pertinence et proportionnalité des données; principe de minimisation
4. Conservation limitée des données
5. Exactitude, intégrité et confidentialité des données : principe de sécurité
6. Renforcement de la transaparence et exercice des doits facilité

Nouveautés

RESPONSABILITATION de TOUS les acteurs !
Outils de la confirmité

- Registre des traitements
- Registre sous-traitant
- Analyse d'impact PIA (CNIL)

Archivage et RGPD : à des fins statistiques.

Principes

Tous responsables et tous auditables
Privacy by design
Security by default
DPO (Data Protection Officer)

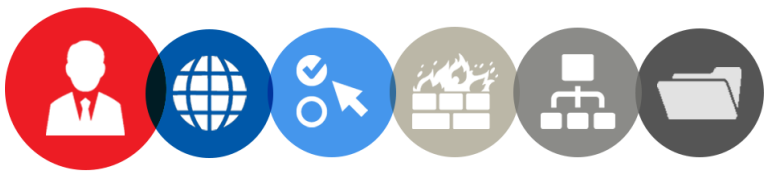
- conformité au RGPD
- Point de contact avec les autorités

Analyse d'impact (PIA: Privacy Impact Assessment)

RPGD : en 6 étapes @CNIL

1. Désigner un pilote
2. Cartographier
3. Prioriser
4. Gérer les risques
5. Organiser
6. Documenter

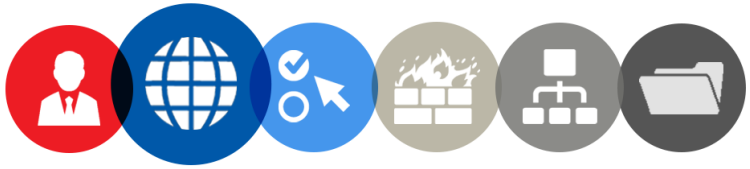
Étape 1 : Désigner un pilote



Délégué à la protection des données

Mission d'information, de conseil et de contrôle en interne.
Conformité au RGPD.

Étape 2 : Cartographier

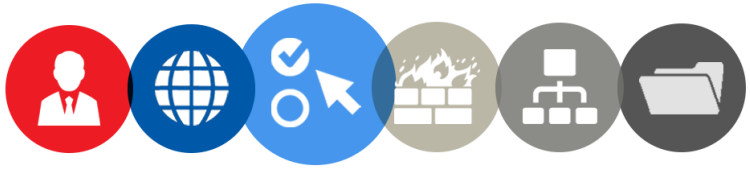


Tenir une documentation interne complète sur leurs traitements de données personnelles

- Catégories les données traitées
- Recenser précisement vos traitements de données personnelles (**Registre des traitements**)
- Lister les objectifs
- Identifier les acteurs
- Identifier les flux des données

But : Assurer que ces traitements respectent bien le règlement.

Étape 3 : Prioriser



1. Collecter et traiter **que les données nécessaires**.
2. **Base juridique du traitement** : consentement de la personne, contrat, obligation légale ...
3. Révisez vos **mentions d'information** : articles 12, 13 et 14: droits de la personne concernée : Transparence, Information et Transitivité
4. Vérifier vos **sous-traitants** et clause des contrats
5. Prévoyez les **modalités d'exercice des droits** des personnes concernées : droit d'accès, de rectification, droit à la portabilité, retrait du consentement...
6. Vérifiez les **mesures de sécurité** mises en place.

Étape 3 : VIGILANCE, des **types** de données

- origine prétendument **raciale ou ethnique**, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale,
- la **santé** ou l'orientation sexuelle,
- génétiques ou **biométriques**,
- infraction ou de condamnation **pénale**,
- sur les **mineurs**.

Étape 3 : VIGILANCE, votre traitement

- la surveillance **systématique** à grande échelle d'une zone accessible au public
- l'évaluation **systématique** et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

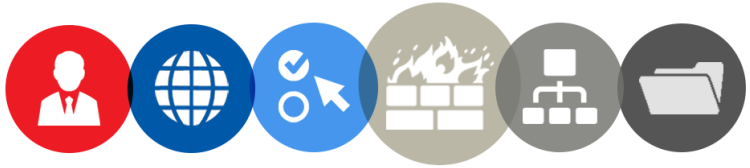
Étape 3 : VIGILANCE **transfert** des données hors UE

- Vérifiez que le pays vers lequel vous transférez les données est reconnu comme adéquat par la Commission européenne ;
- Dans le cas contraire, encadrez vos transferts.

Étape 4 : Gérer les risques

Privacy Impact Assessment (PIA)

Data protection impact assessment



- Principes et droits fondamentaux, **non négociables**, de la loi
- Gestion des **risques sur la vie privée** des personnes concernées, pour déterminer les mesures techniques et d'organisation pour protéger les données personnelles.

Un PIA contient :

- Une **description** du traitement étudié et de ses **finalités**.
- Une **évaluation de la nécessité et de la proportionnalité** des opérations de traitement au regard des finalités
- Une **évaluation des risques** pour les droits et libertés des personnes, les mesures envisagées pour faire face aux risques.

Étape 4 : Qui participe au PIA?

- **Le responsable de traitement** : valide et applique le PIA.
- **Le délégué à la protection des données** : élabore le plan d'action et se charge de vérifier son exécution ;
- **Le(s) sous-traitant(s)** : fournit les informations nécessaires à l'élaboration du PIA ;
- **Les métiers (RSSI, maîtrise d'ouvrage, maîtrise d'œuvre)** : aident à la réalisation du PIA en fournissant les éléments adéquats ;
- **Les personnes concernées** : donnent leurs avis sur le traitement.

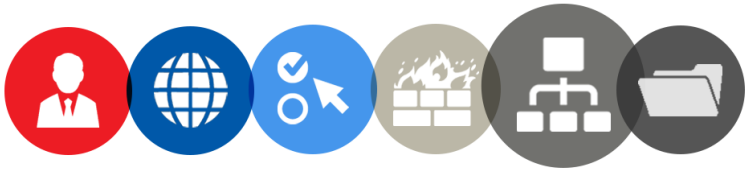
Étape 4 : **PIA obligatoire** Art. 35

Pour tout traitement susceptible d'engendrer des **risques élevés** pour les droits et libertés des personnes concernées.

1. Evaluation ou notation;
2. Décision automatisée avec effet juridique significatif;
3. Surveillance systématique ;
4. Données sensibles ou données à caractère hautement
5. Données personnelles traitées à grande échelle ;
6. Croisement d'ensembles de données ;
7. Données concernant des personnes vulnérables ;
8. Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
9. Exclusion du bénéfice d'un droit, d'un service ou contrat.

Si **au moins 2 de ces critères**, alors faire un PIA.

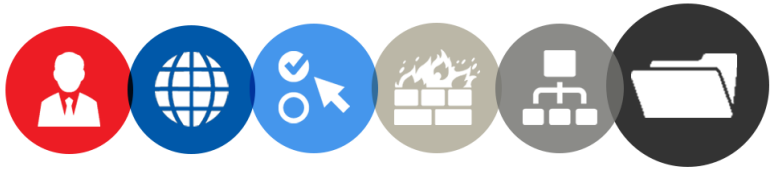
Étape 5 : Organiser



- Protection des données personnelles **dès la conception**
- **Sensibiliser et d'organiser la remontée d'information**
- Traiter les **réclamations et les demandes** des personnes concernées quand à l'exercice de leurs droits
- **Anticiper les violations de données**, dans les 72 heures aux autorités et personnes concernées

Étape 6 : Documenter

Prouver la conformité = Avoir la documentation nécessaire



- Traitements
- Information des personnes
- Contrat pour les acteurs

Étape 6 : Documenter les traitements

- Le **registre des traitements** (pour les responsables de traitements) ou des **catégories d'activités de traitements** (pour les sous-traitants)
- **PIA** pour les traitements à risque
- L'**encadrement des transferts** de données hors de l'Union européenne.

Étape 6 : Documenter l'information

- Les **mentions d'information**
- Les modèles de **recueil du consentement** des personnes concernées,
- Les procédures **mises en place** pour l'exercice des droits

Étape 6 : Documenter les contrats

- Les **contrats avec les sous-traitants**
- Les **procédures internes** en cas de violations de données
- Les **preuves** que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

Objectif

Responsabilisation de tous les acteurs impliqués dans le traitement des données personnlles dès lors qu'elle concernent des résidents européens.

- Obligation de transparence et traçabilité
  - Contrtat écrit entre les acteurs
  - Autorisation écrite des traitement
  - Démontrer le respect de vos obligations
  - Ternir un **registre des traitements**
- Protection by design et by default (paramètres, accès, purge)
- Obligation de garantir la sécurité des données traitées
- Obligation d'assistance, d'alerte et de conseil (immédiate)

Registre des catégories d'activités de traitement

- nom et les coordonnées de chaque client
- le nom et les coordonnées de chaque sous-traitant
- le nom et les coordonnées du délégué à la protection des données
- les catégories de traitements effectués
- les transferts de données hors UE
- une description générale des mesures de sécurité techniques et organisationnelles que vous mettez en place

Qui est touché ?

TOUT LE MONDE !

- les prestataires de services informatiques
- les agences de marketing ou de communication
- tout organisme offrant un service ou une prestation
- Un organisme public ou une association

qui traite les données personnelles.

Sanctions

Jusqu'à 10 ou 20 millions d'euros, ou 2% ou 4% du chiffre d'affaires annuel mondial de l'exercice précédent.
En France la CNIL devient autorité de contrôle

Sanctions pour le sous-traitant

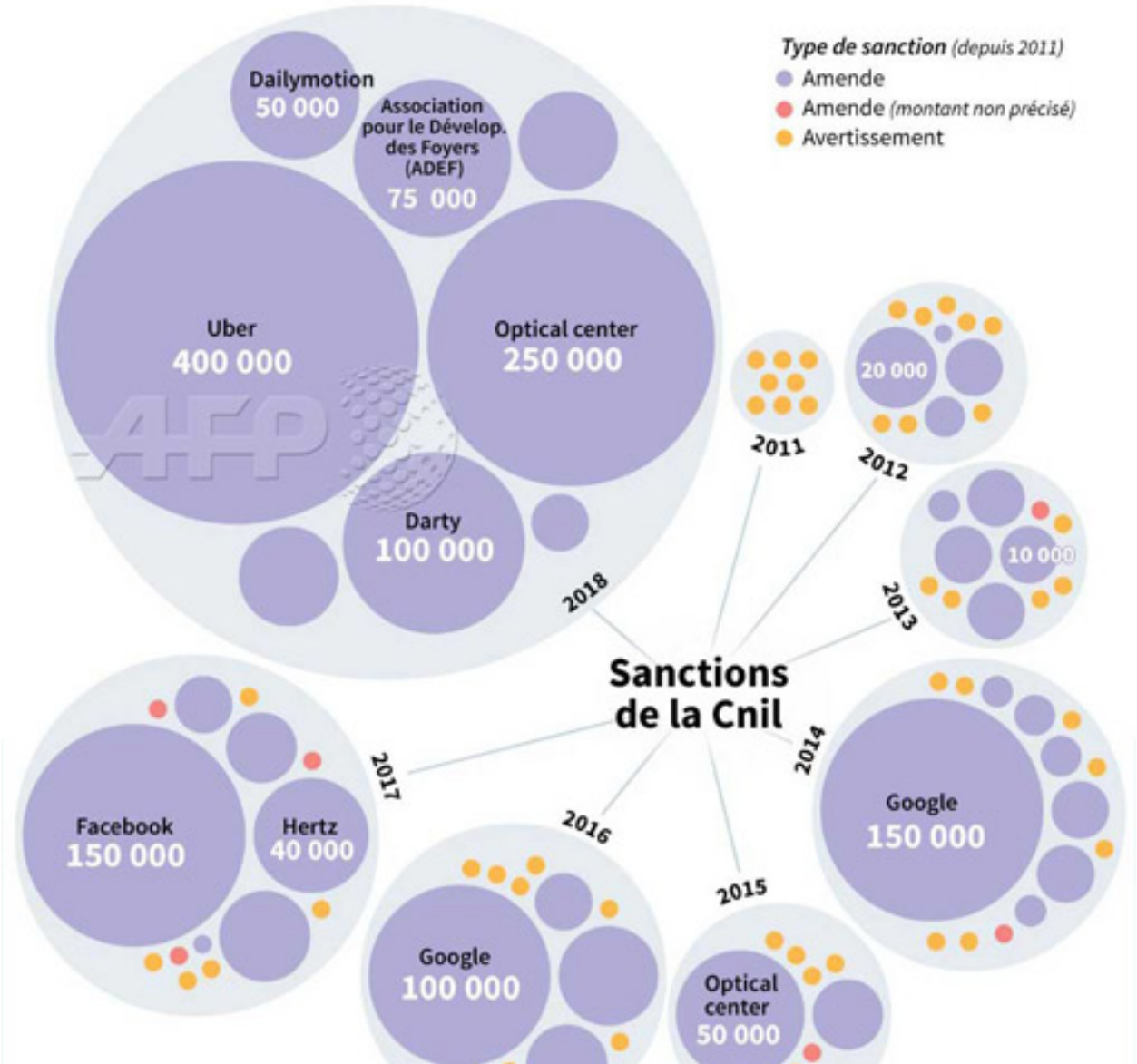
- si vous agissez en dehors des instructions licites de votre client ou contrairement à ces instructions ;
- si vous n'aidez pas votre client à respecter ses obligations
- si vous ne mettez pas à la disposition de votre client les informations permettant de démontrer le respect des obligations ou pour permettre la réalisation d'audits
- si vous n'informez pas votre client qu'une instruction constituerait une violation du règlement européen
- si vous sous-traitez sans autorisation préalable de votre client
- si vous fait es appel à un sous-traitant qui ne présente pas de garanties suffisantes
- si vous ne désignez pas un délégué à la protection des données
- si vous ne tenez pas de registre des catégories d'activités de traitement

Bilan après 6 mois

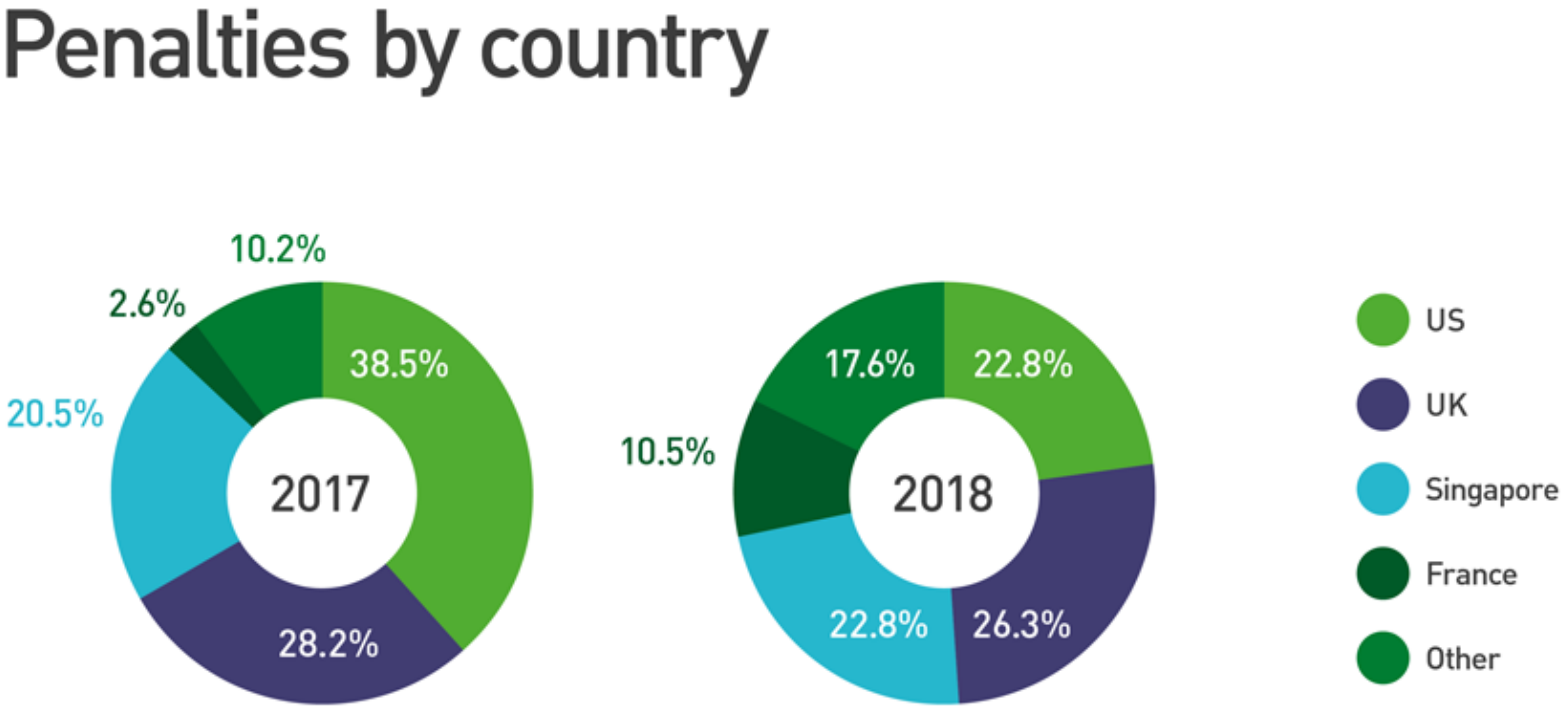
- 32 000 organismes ont 1 DPO: 15000 DPO contre 5000 CIL
- 100 notifications de violations, environ 7 par jour
- 7 millions de visites sur le site de la CNIL
- 130 000 téléchargements du PIA de la CNIL
- 9 700 plaintes
- plus de 345 plaintes transfrontalières
- Conception d'un MOOC

24 Juillet 2018 : Sanction de 50 000 € de la CNIL à l'encontre de la société DAILYMOTION, mot de passe stocké en clair temporairement.
15 Aout 2018 : Sanction de 30 000 € par la CNIL à l'encontre de l'Office Public de l'Habitat de Rennes Métropole
L'amende (50 Millions €) infligée par la CNIL à Google : le manque de transparence, le manque d'information adéquate, l'absence de consentement explicite préalablement recueilli.

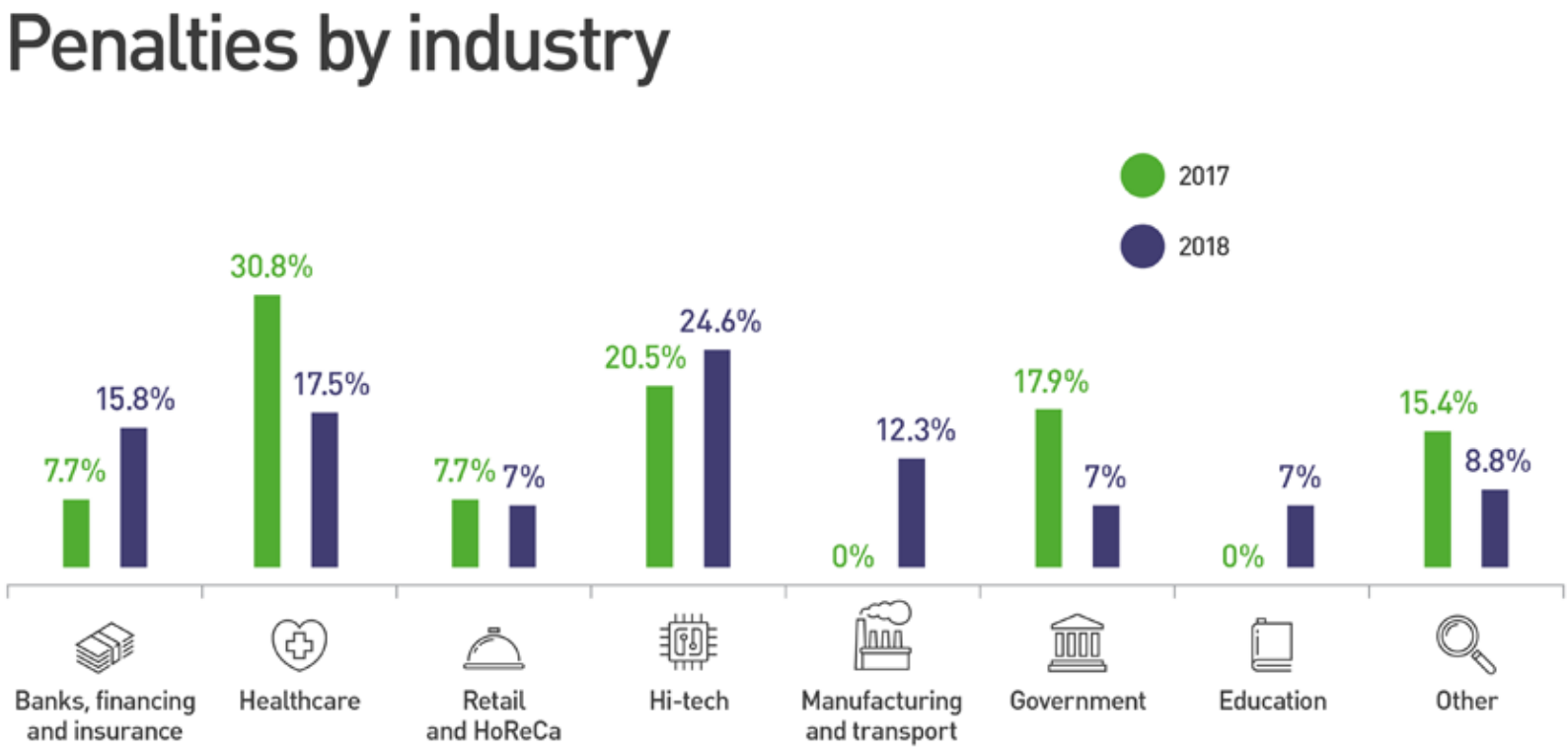
Sanctions de la CNIL



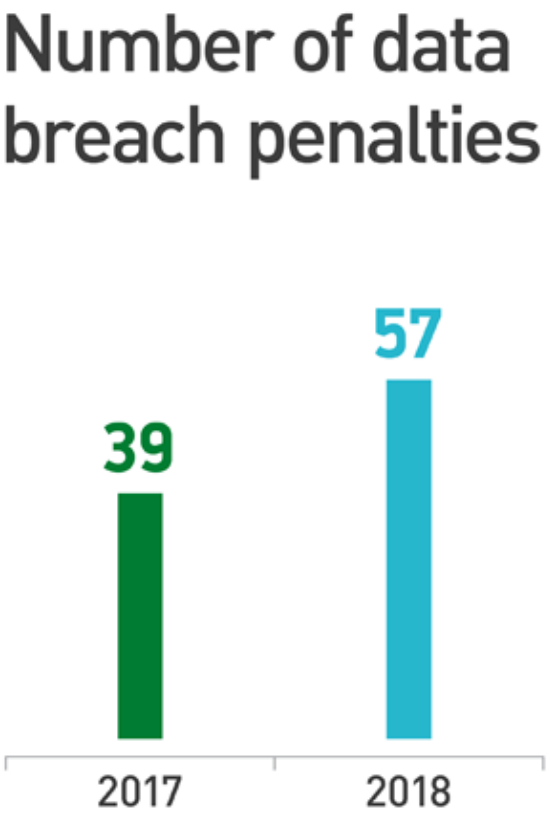
Par pays

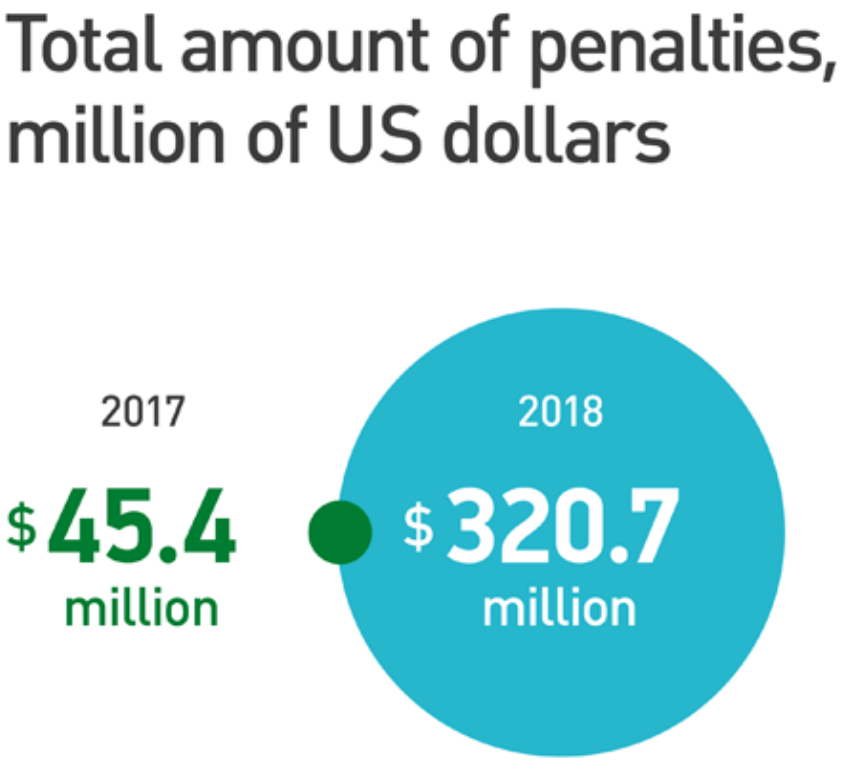

Penalties by country
10.2%
2.6%
38.5%
20.5%
2017
28.2%
17.6%
22.8%
10.5%
2018
22.8%
26.3%
US
UK
Singapore
France
Other

Par industries

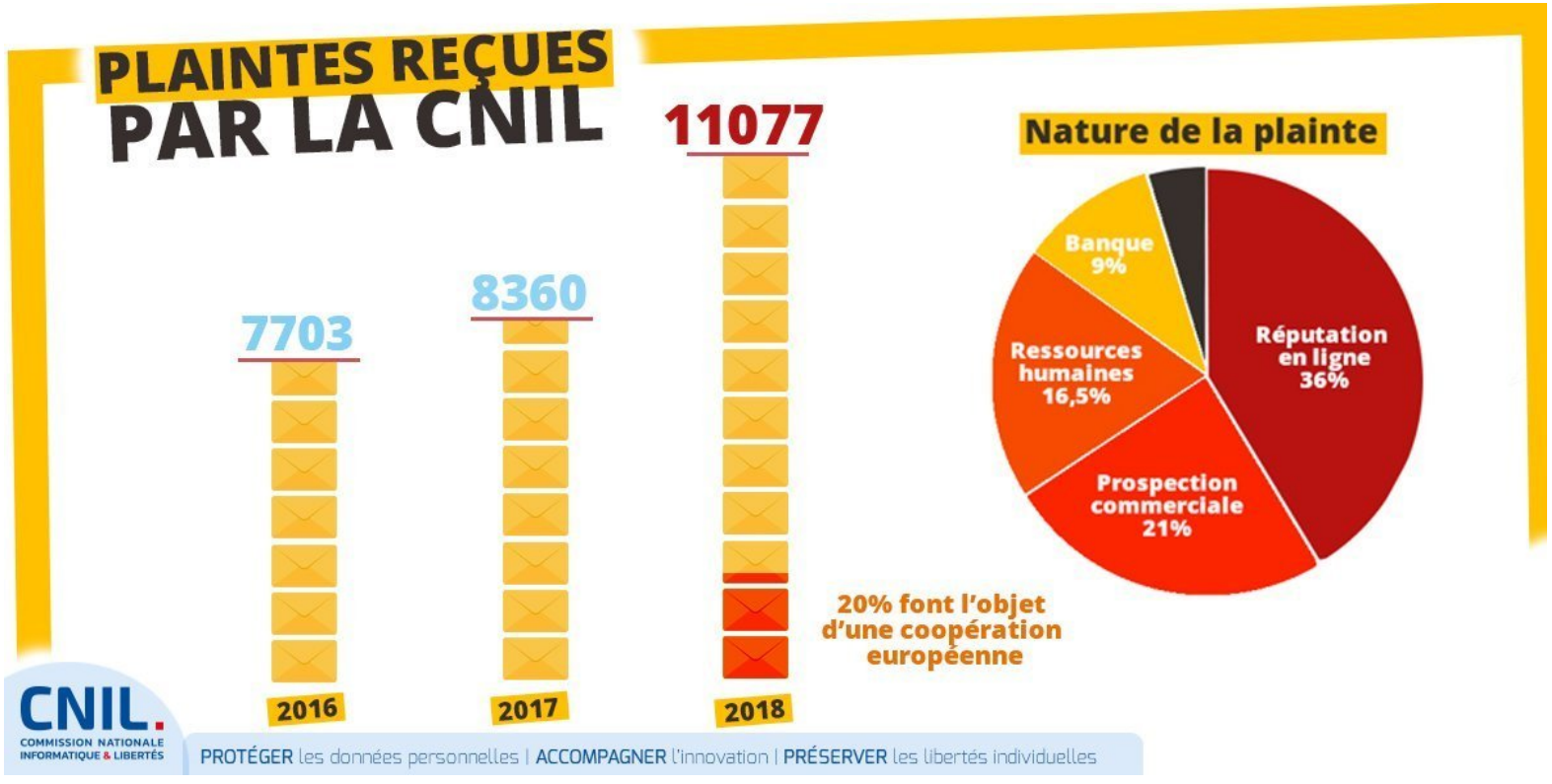


Évolution


Number of data breach penalties
39
57
2017
2018

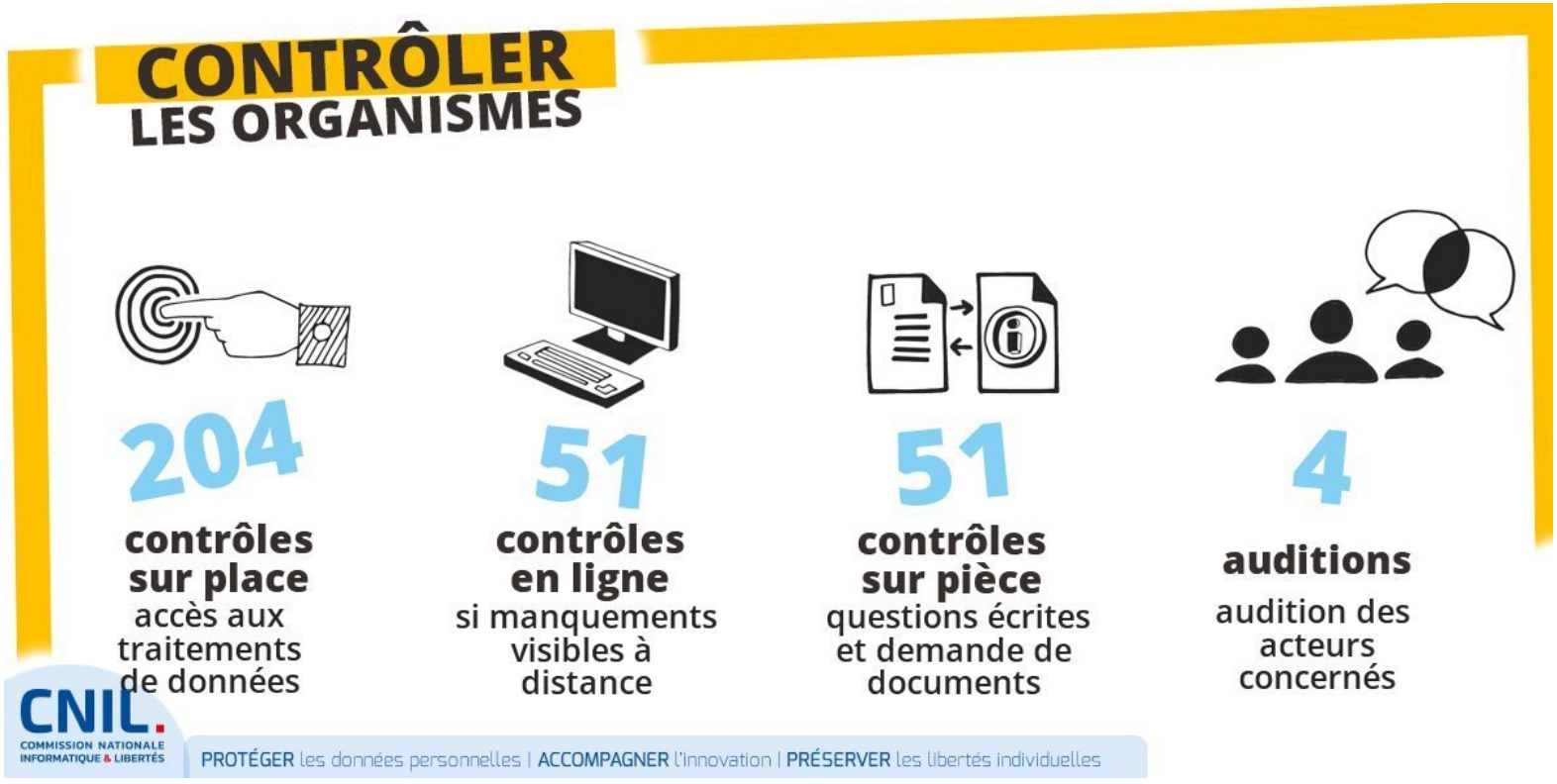

Total amount of penalties, million of US dollars
2017
$45.4 million
2018
$320.7 million

Plaintes déposées 2018

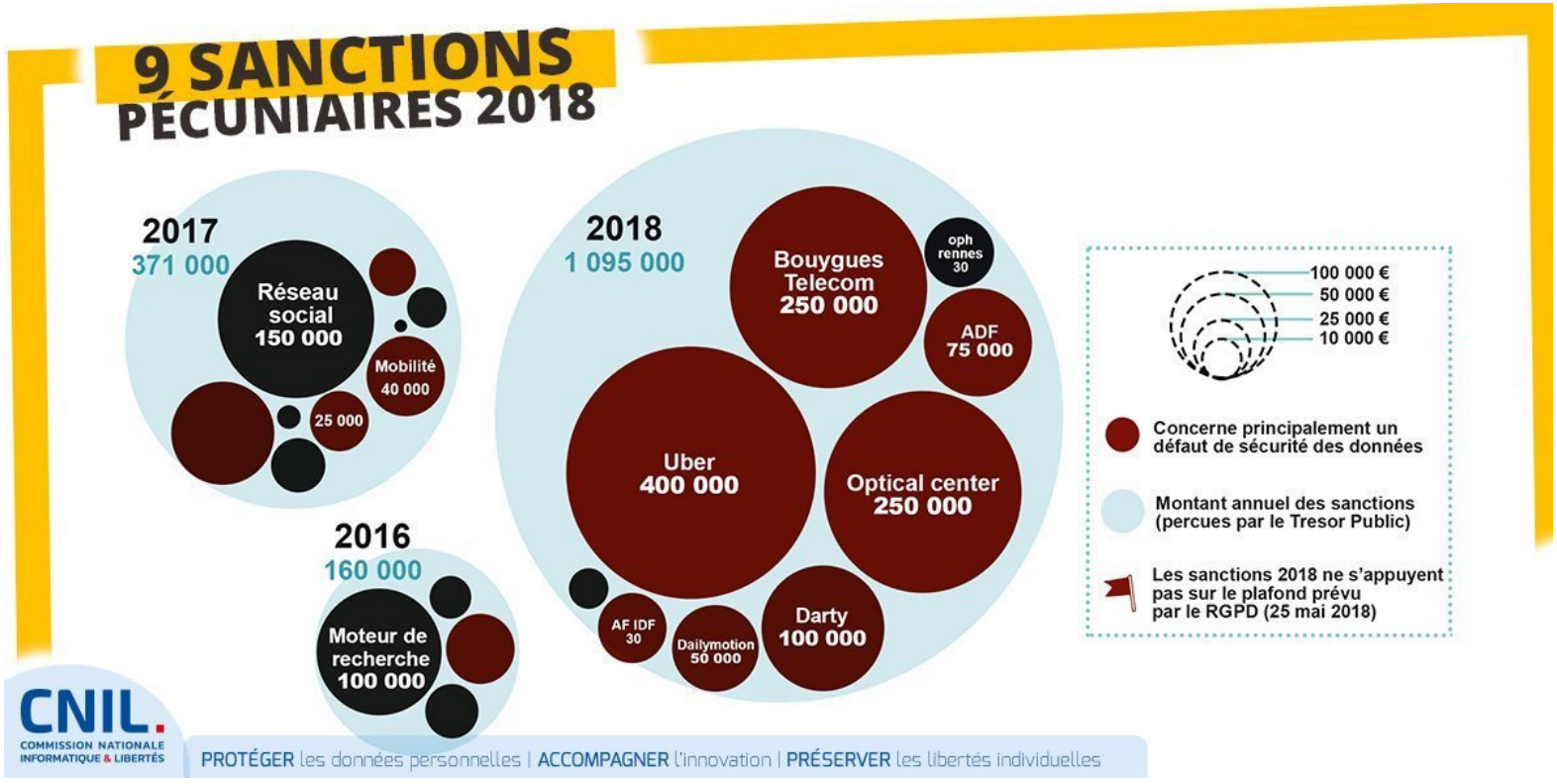


Tendances 2018

Contrôles 2018



Sanctions 2018



1 an après

"70 % des Français se disent aujourd'hui plus sensibles aux problématiques de protection des données."

- 2 044 notifications de violation de données en France
- 89 271 au niveau européen ;
- Plus de 19 000 DPO désignés par plus de 53 000 organismes
- Plus de 8,1 millions de visites depuis un an cnil.fr

4 Croyances sur le RGPD par Florence BONNET

I. La probabilité de faire l'objet d'un contrôle de la CNIL est faible

- obligation de notifier et de communiquer les violations de données personnelles à l'autorité et aux personnes concernées le cas échéant.
- toute personne a le droit de réclamer auprès d'une autorité de contrôle et d'exercer son droit d'obtenir réparation.

4 Croyances sur le RGPD par Florence BONNET

II. En cas de contrôle, il suffira de collaborer avec la CNIL et de faire preuve de réactivité pour éviter une sanction

Absence de mesures élémentaires de sécurité = non-conformité.

- Mise en ligne d'un site sans test
- Exposition aux données sans authentification (mot de passe suffisamment robustes)
- Ne doivent pas être conservés ou transmis en clair mais de manière sécurisée
- Les connexions et flux de données doivent être sécurisés
- Les connexions à une plateforme des paiements doivent être tracés
- Le dispositif de communication bluetooth doit être sécurisé
- La connexion à distance doit être sécurisée (VPN, IP)
- Les données les sensibles doivent être conservées et sécurisées
- Le chiffrement doit être à l'état de l'art ! Pas de MD5 !

4 Croyances sur le RGPD par Florence BONNET

II.

- Protection du secret : le sel doit être conservé dans un espace distinct de celui où sont stockés les mots de passe ;
- Les numéros de carte bancaire ne doivent pas être conservés en clair avec les cryptogrammes .
- Les accès aux données doivent être strictement limités aux seules personnes ayant besoin d'en connaitre
- il appartient au responsable de traitement, d'adapter les conditions d'usage de ce logiciel à sa propre population

4 Croyances sur le RGPD par Florence BONNET

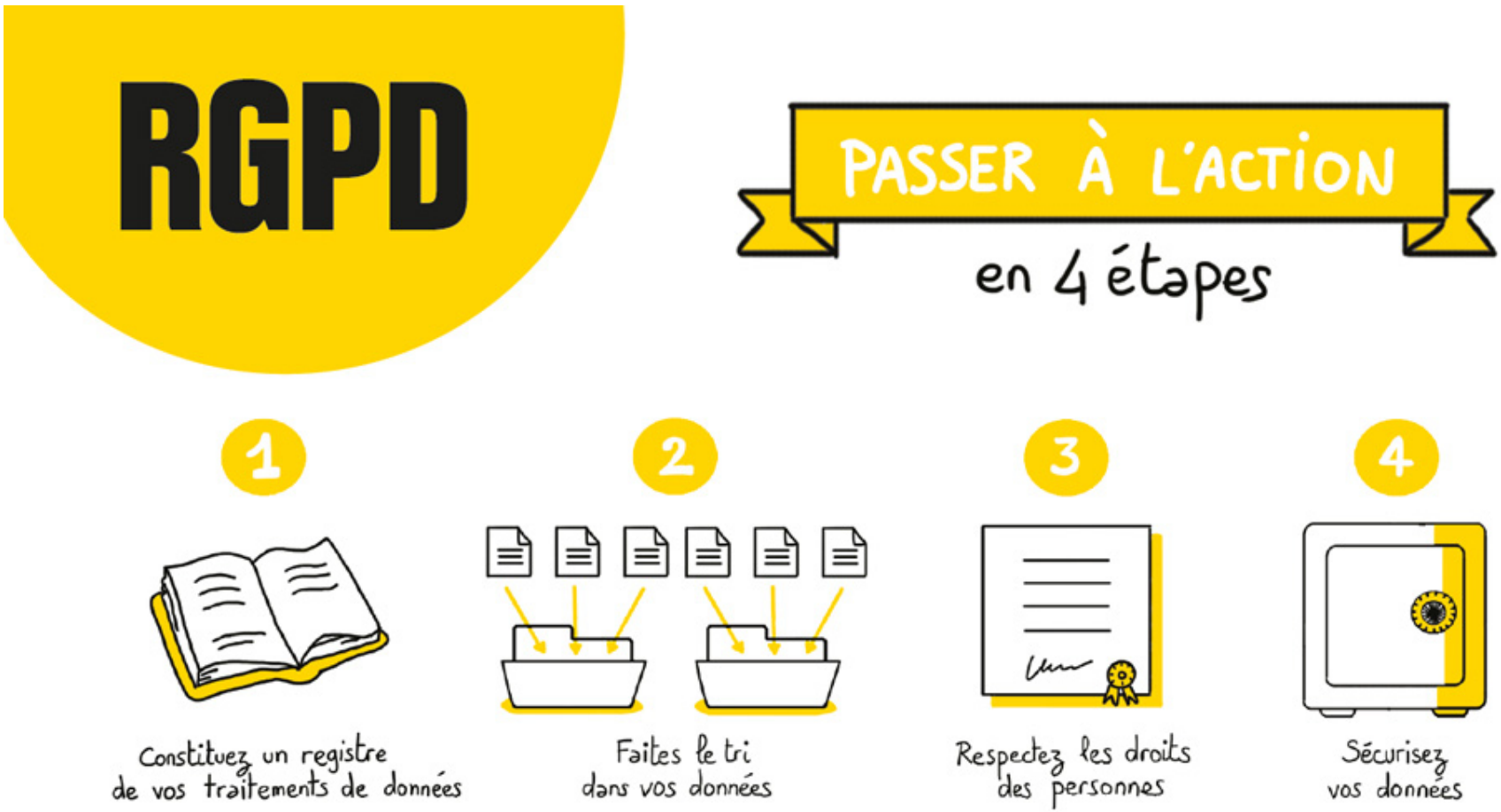
III. Se croire à l'abri parce qu'il existe forcément une politique de sécurité dans l'entreprise

- il est vain pour la société de chercher à se dégager de sa responsabilité en invoquant de supposées procédures préventives en la matière (procédure sécurité conforme ISO 27001, exigences du Règlement CRBF 97-02)

4 Croyances sur le RGPD par Florence BONNET

IV. c'est le sous-traitant qui sera responsable

- Il convient de tracer et de documenter les échanges avec le prestataire
- L'intervention d'un prestataire crée une responsabilité supplémentaire de contrôle effectif des agissements du prestataire et des solutions utilisées par ce dernier.
- La prestation de service doit obligatoirement faire l'objet d'un contrat encadrant les obligations du sous-traitant en matière de sécurité et de confidentialité des données à caractère personnel


RGPD
PASSER À L'ACTION
en 4 étapes
1
Constituez un registre de vos traitements de données
2
Faites le tri dans vos données
3
Respectez les droits des personnes
4
Sécurisez vos données

Note: 70%

Faire un PIA pour votre entreprise ou une partie de votre entreprise.

Outline

Démarche

Publiée en octobre 2005 et révisée en 2013.

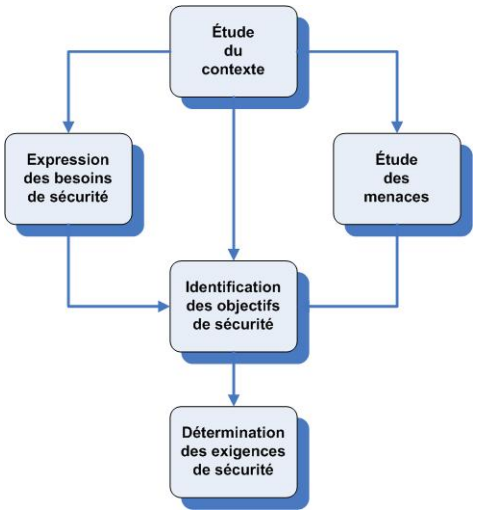
1. Phase d'établissement
2. Phase d'implémentation
3. Phase de maintien
4. Phase d'amélioration

SMSI : Système de management de la sécurité de l'information

Phase d'établissement (PLAN)

1. Définir la politique et le périmètre du SMSI
2. Identifier et évaluer les risques liés à la sécurité et élaborer la politique de sécurité (EBIOS)
3. Traiter le risque et identifier le risque résiduel par un plan de gestion (Évitement, réduction, transfert, acceptation)
4. Choisir les mesures de sécurité à mettre en place

EBIOS



1. Identifier les actifs ;
2. Identifier les personnes responsables ;
3. Identifier les vulnérabilités ;
4. Identifier les menaces ;
5. Identifier leurs impacts sur les actifs à défendre ;
6. Évaluer la vraisemblance ou potentialité du risque ;
7. Estimer les niveaux de risque, fonction de leur potentialité et de leur impact.

Phase d'implémentation (DO)

1. Établir un plan de traitement des risques
2. Déployer les mesures de sécurité
3. Générer des indicateurs:
   - De performance pour savoir si les mesures de sécurité sont efficaces
   - De conformité qui permettent de savoir si le SMSI est conforme à ses spécifications
4. Former et sensibiliser le personnel

Phase de maintien (Check)

Gérer le SMSI au quotidien et à détecter les incidents

- Le contrôle interne (s'assurer en permanence que les processus fonctionnent normalement)
- Les audits internes (vérifier la conformité et l'efficacité du système de management.
- Les revues (ou réexamens) qui garantissent périodiquement l'adéquation du SMSI avec son environnement.

Phase d'amélioration (Act)

Actions correctives, préventives ou d'amélioration pour les incidents et écarts constatés lors de la phase Check.

Outline

Ethique

éthique = (Larousse) Ensemble des principes moraux qui sont à la base de la conduite de quelqu'un.
Science de la morale / un art du comportement.

2 principes s'imposent (Jérôme Béranger)

1. L'information est agrégée en connaissance, mais cette connaissance est une connaissance pratique, finalisée dans l'action. C'est moins un savoir qu'un savoir-utiliser.
2. A une description de processus on préfèrera une description d'état. L'enjeu de l'éthique, est le passage d'un état de savoirs complexes, désorganisés et flous vers un état de savoirs simples, structurés et orientés vers une fin.

Les données médicales

4 principes par Tom Beauchamp et James Childress, Principles of Biomedical Ethics (2001).

1. bienfaisance avec deux règles précises :
   - elle doit être bénéfique,
   - et elle doit être utile (avoir un rapport coût-bénéfice positif)
2. l'autonomie : le fait qu'une personne se donne à elle-même sa règle de conduite. Ce principe vise à la participation du patient au processus de décision
3. la "non-malfaisance" : éviter le mal à celui dont on a la responsabilité, lui épargner préjudices ou souffrances qui n'auraient pas de sens pour lui
4. la justice : notion d'égalité et d'équité.

Problème

Le système impose des règles d'attribution et d'accès à l'information qui diffèrent en fonction du statut. La dissymétrie de connaissances est discriminante et remet en cause la transparence de l'information.
Quelle est leur utilisation et diffusion ?
$\Rightarrow$ La simplification des données transmises entraîne un usage et un accès plus efficace, avec une meilleure saisie et une plus grande sécurité. Elle aboutit en revanche à une moins bonne intégrité des données.
De ce fait, la hiérarchisation des données simplifie le travail des divers utilisateurs, mais induit une plus grande complexité technique pour le concepteur du système d'information.

Se questionner

- quels sont les objectifs, les buts, les enjeux et le sens de cette étape ?
- Quelles données vais-je utiliser ?
- Des données partielles ou totales ?
- Comment vais-je les utiliser ?
- À quel endroit ? Auprès de quels utilisateurs ?
- Plus globalement, comment exploiter l'ensemble hétérogène des données accumulées et stockées dans un système d'information ?
- Quelle sera sa pertinence par rapport à ma situation ?
- Cela ne va-t-il pas dénaturer la valeur informative initiale ?
- L'intégrité du message final sera-t-elle conservée ?

Outline

A retenir

- Contexte
- Cadre juridique
- Réglementation
- RGPD

Bruce Schneier

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."