



# Protection des données et nouvelle réglementation européenne (GDPR - RGPD)



Pierre Bugnon  
<https://www.linkedin.com/in/pierrebugnon/>

# | Les enjeux de la protection des données



# Ce que l'on aime pas voir ...

- Des données privées volées, et rapidement disponibles...



EMISSIONS • SUISSE • MONDE • ECONOMIE • CULTURE • REPÉRAGES WEB • AFFICHER PLUS

Genève Mise à jour le 19 janvier 2015



## Les données de la BCGE piratées sont plus sensibles qu'annoncé



Hacking à la banque Mise au Point / 10 min. / Le 18 janvier 2015

Montants d'hypothèques, salaires: des informations financières très sensibles figurent dans les données volées par des pirates à la Banque Cantonale de Genève. Celle-ci affirmait pourtant le contraire.



CDS Marine @CDSSmarine · Jan 12

As stated they would, **REX Mundi** post bank details of **#BCGE** customers - Reuters News Link: [cdsurl.co/BCGE3](https://cdsurl.co/BCGE3)



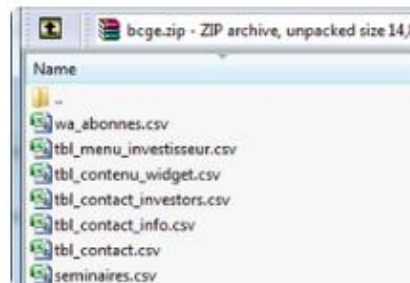
Rex Mundi @rexmundi14 · Jan 9

The **#BCGE** **#leak** is here, in all its glory:  
uplo [redacted]



Ptrace Security GmbH @ptracesecurity · Jan 12

Rex Mundi Hackers post stolen data from Swiss Bank **BCGE** **#cybercrime**  
**#databreach** **#infosec** **#hacking**



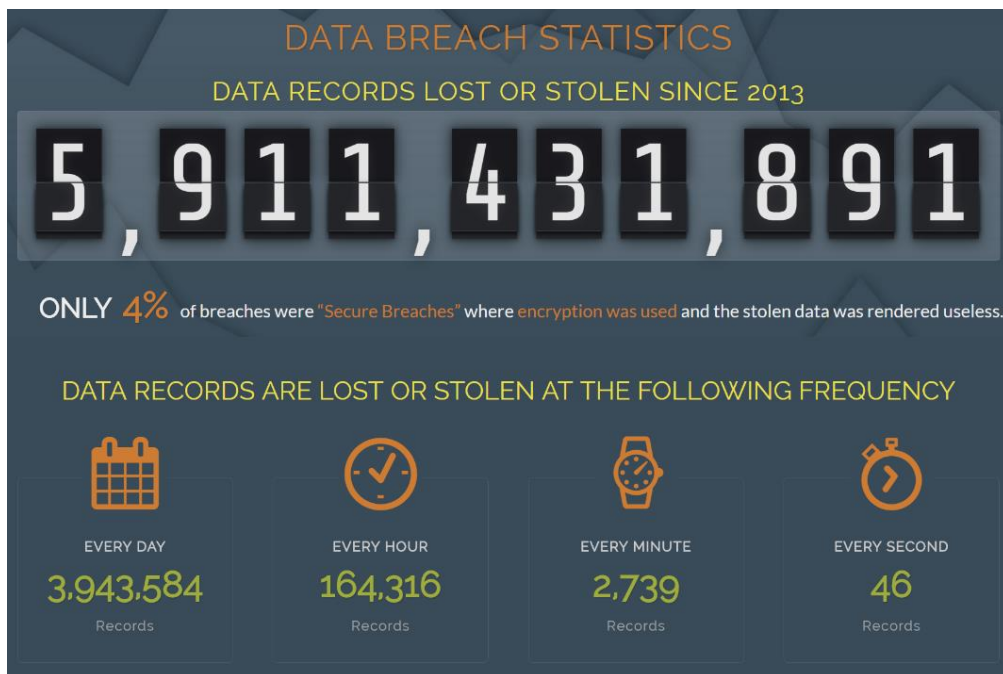
## Des données personnelles de policiers sur internet

Mutuelle Générale de la Police / 5 pages / Par AFP, publié le 27/01/2015 à 13:51, mis à jour à 13:51

Paris - Les données personnelles de 112.000 policiers ont été mises en ligne sur internet via un fichier protégé par un code, un "incident inacceptable" a déclaré lundi à l'AFP



# Un phénomène en croissance



Juin 2016



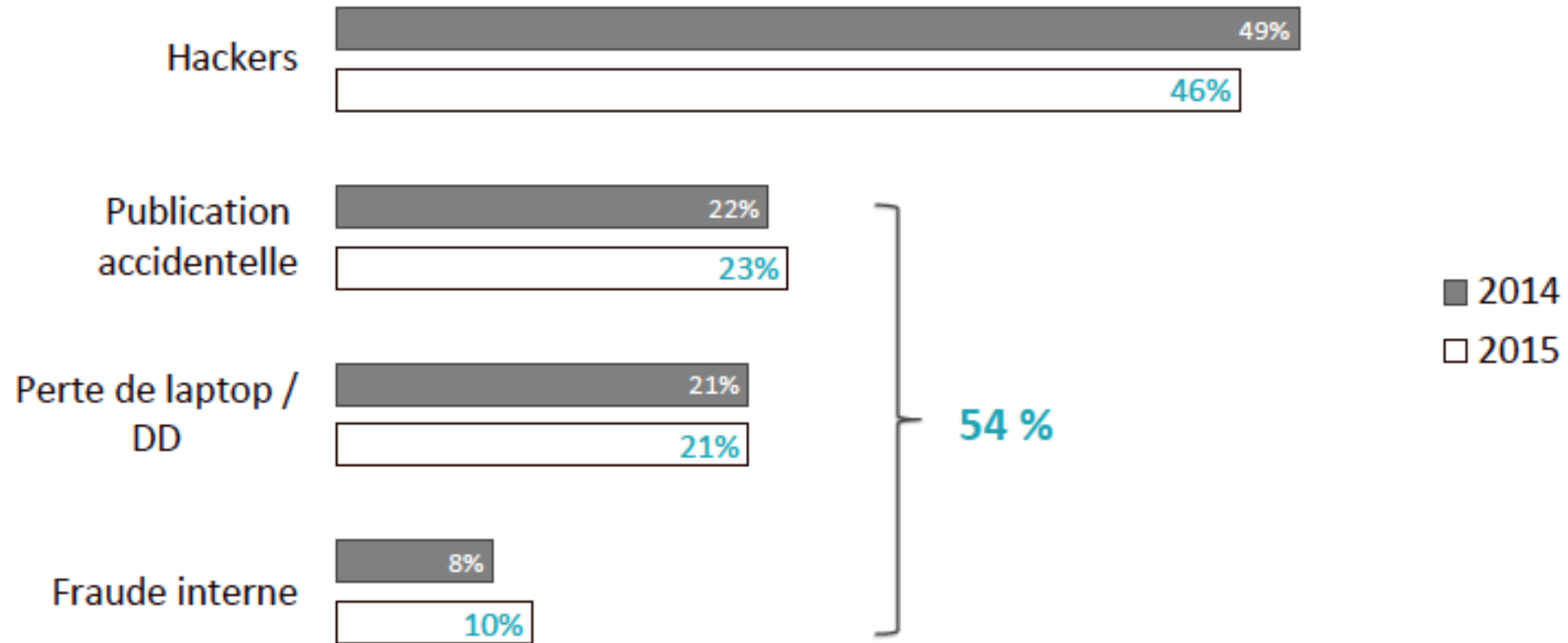
Octobre 2017

Source : <http://breachlevelindex.com/> (Gemalto)

# Et tous les incidents ne sont pas anodins

Organization Breached	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location	Industry	Risk Score
JPMorgan Chase	83,000,000	08/27/14	Identity Theft	Malicious Outsider	United States	Financial	10.0
Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card	104,000,000	01/20/14	Identity Theft	Malicious Insider	South Korea	Financial	10.0
Target	110,000,000	11/04/13	Financial Access	Malicious Outsider	United States	Retail	10.0
Home Depot	109,000,000	09/02/14	Financial Access	Malicious Outsider	United States	Retail	10.0
MySpace	360,000,000	06/11/13	Account Access	Malicious Outsider	United States	Other	10.0
Anthem Insurance Companies (Anthem Blue Cross)	78,800,000	01/27/15	Identity Theft	State Sponsored	United States	Healthcare	10.0
Adult FriendFinder/Friend Finder Network/Cams/Penthouse/Stripshow/iCams	412,214,295	10/16/16	Account Access	Malicious Outsider	United States	Other	10.0
eBay	145,000,000	05/21/14	Identity Theft	Malicious Outsider	United States	Retail	10.0
Adobe Systems, Inc	152,000,000	09/18/13	Financial Access	Malicious Outsider	United States	Technology	10.0
CyberVor	1,200,000,000	08/05/14	Account Access	Malicious Outsider	Global	Technology	10.0

# Avec une certaine responsabilité des entreprises



Source: Internet Security Threat Report 2015, Symantec

# | Les réglementations



# Leur but

- Réglementer la collecte, l'utilisation, le stockage, la protection, la révélation « d'informations personnelles identifiables ».
- Un distinguo est fait quant aux obligations entre :
  - Les données « personnelles / RH / Clients » qui peuvent être exploités dans le respect de la réglementation.
  - Les données « sensibles » qui ne peuvent être exploitées excepté quelques cas :
    - Consentement explicite + base légale
    - Protègent un intérêt vital de la personne
    - Rendues publiques par la personne
    - Nécessaires pour démarche légale
- Suivant les réglementations, la nature des données personnelles et sensibles diffère.



# Actuellement sont en vigueur trois niveaux de lois

- National (Loi Française) avec la loi Informatique, fichiers et libertés de 1978, dont le respect est « assuré » par la CNIL.
- Européen avec des approches globales :
  - Data Protection Directive (95/46/EC) E-Privacy Directive (+ *amendement*)
  - Data Protection Directive (2006/24/EC)
  - Data Retention Directive.
- USA avec des lois sectorielles telles que l'HIPAA/HITECH (santé), GLBA/FCRA (finances), Children On-line Privacy Protection Act, etc. mais aussi des lois par état.

*L'approche globale de l'UE semble être le choix des autres pays dans le monde et la GDPR devrait en être "l'aboutissement".*

# Des lois dissuasives ?

- Probablement pas...

## Top 20 Government-imposed Data Privacy Fines Worldwide, 1999-2014 \*\*

Rank	Fined entity	Amount of fines and penalties	Year	Country	Privacy principles violated
1	Apple	\$32.5M	2014	U.S.	Choice and Consent
2	Google	\$22.5M	2012	U.S.	Collection
3	Google	\$17M	2013	U.S.	Collection and Notice
4	ChoicePoint	\$15M	2006	U.S.	Security
5	Hewlett-Packard	\$14,5M	2006	U.S.	Collection
6	LifeLock	\$12M	2010	U.S.	Accuracy, Security
7	TJ Maxx	\$9.8M	2009	U.S.	Security
8	Dish Network	\$6M	2009	U.S.	Choice and Consent
9	DirecTV	\$5.3M	2005	U.S.	Choice and Consent
10	HSBC	\$5M	2009	UK	Security
11	US Bancorp	\$5M	1999-2000	U.S.	Disclosure
12	Craftmatic	\$4.3	2007	U.S.	Choice and Consent
13	Cignet Health	\$4.3M	2011	U.S.	Access
14	Barclays Bank	\$3.8M	2013	U.S.	Use and Retention
15	Certegy Check Services	\$3.5M	2013	U.S.	Accuracy
16	Playdom	\$3M	2011	U.S.	Collection and Notice
17	The Broadcast Team	\$2.8M	2007	U.S.	Collection
18	Equifax, TransUnion and Experian	\$2.5M	2000	U.S.	Access
19	CVS Caremark	\$2.3M	2009	U.S.	Security and Disposal
20	Norwich Union Life	\$1.8M	2007	UK	Disclosure

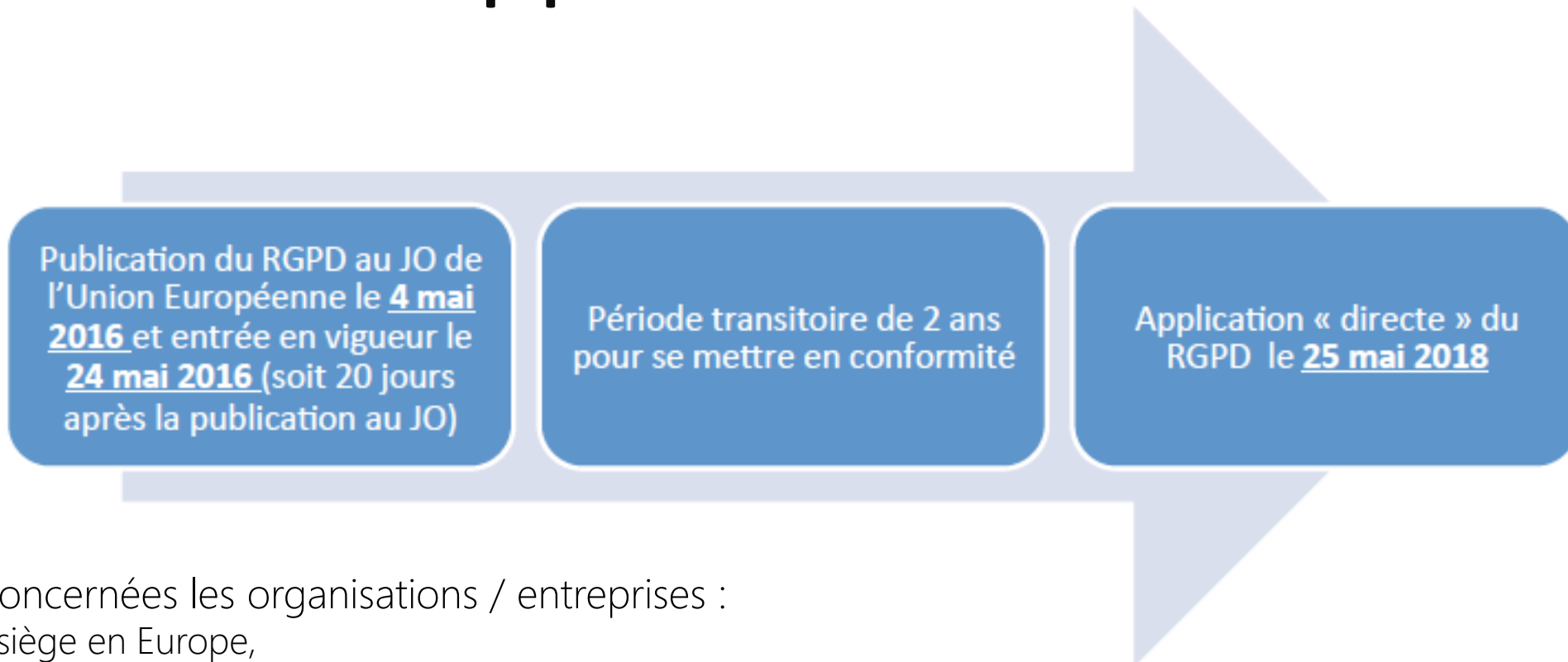
\*\*SOURCE IAPP 17 FEB 2014

A close-up photograph of a right hand holding a silver and black ballpoint pen, poised to write on a white, lined notebook. The background is a soft, out-of-focus white.

# La GDPR / RGPD

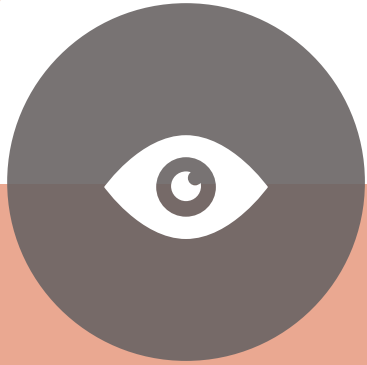
*Evolutions et conséquences*

# L'échéance approche



- Et sont concernées les organisations / entreprises :
  - avec un siège en Europe,
  - ou offrant des prestations / produits à des résidents de l'UE,
  - ou traitant des données de résidents de l'UE
- Avec un peu de souplesse pour les entreprises de moins de 250 employés ne traitant pas de données sensibles.

# Quels sont les principaux changements qu'induit le GDPR ?



## Protection de la vie privée

Les individus sont en droit de :

- Accéder à leurs données à caractère personnel
- Rectifier les erreurs dans leurs données à caractère personnel
- Supprimer leurs données à caractère personnel
- S'opposer au traitement de leurs données à caractère personnel
- Exporter leurs données à caractère personnel



## Contrôles et notifications

- Exigences de sécurité strictes
- Obligation de signaler tout piratage
- Consentement **approprié pour le traitement des données**
- Confidentialité
- Conservation des documents



## Politiques transparentes

Politiques transparentes et facilement accessibles concernant :

- Avis de collecte de données
- Avis de traitement
- Informations sur le traitement
- Conservation/suppression des données



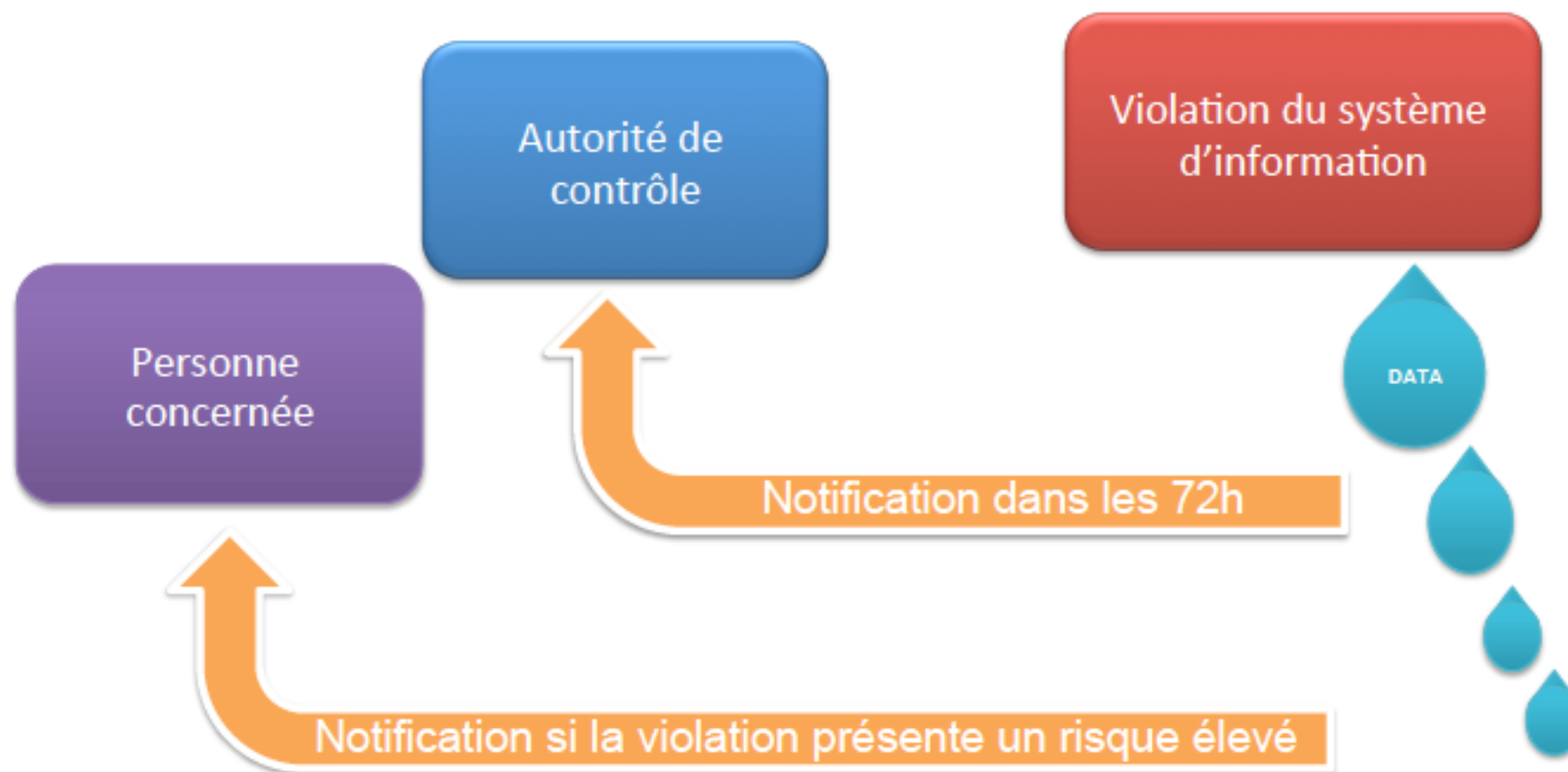
## Informatique et formation

Nécessité d'investir dans :

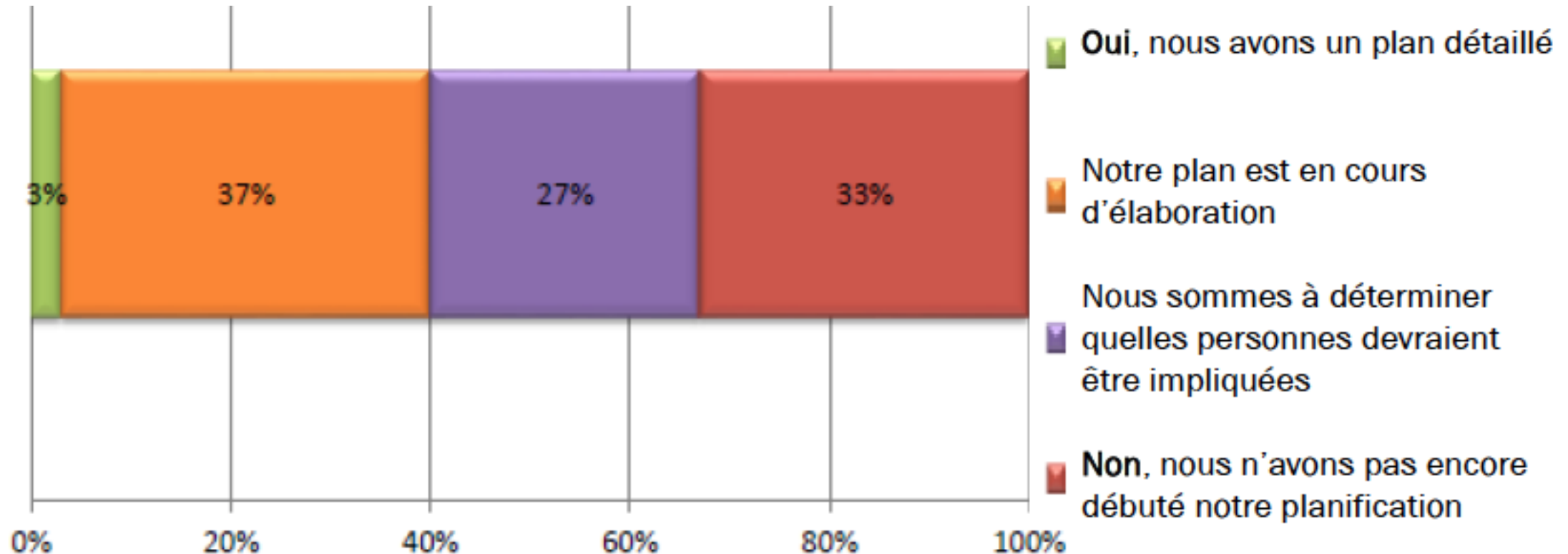
- Formation des employés et du personnel responsable de la confidentialité
- Politiques de données
- Préposé à la protection des données
- **Contrat fournisseurs/sous-traitants**



# Que faire en cas de problème ?



# Et globalement les entreprises sont loin d'être prêtes ...



*Dimensional research – Sponsored by : DELL*  
*Septembre 2016*

# Avec des sanctions significatives

Loi Informatique et  
Libertés : sanctions  
maximales de 150 000  
€ (voire 300 000 € en  
cas de réitération)



RGPD : sanctions allant  
jusqu'à 20 millions  
d'euros ou jusqu'à 4 %  
du CA annuel mondial

# Des solutions avec Microsoft Azure



# Premier exemple : Microsoft 365 et GDPR

## Identifier où resident les données

- Office 365 Advanced Security Management / EMS Cloud App Security
- Office 365 eDiscovery / Advanced eDiscovery
- EMS Azure Information Protection

## Classifier et Protéger les données

- Office 365 Data Loss Prevention
- Office 365 Legal In-place Hold
- Message encryption – at rest & in transit
- EMS Intune
- Office 365 Advanced Security Management / EMS Cloud App Security
- EMS Azure Information Protection
- Windows Information Protection

## Contrôler les accès

- Office 365 Customer Lockbox
- EMS Azure Active Directory Premium
- EMS Azure Active Directory Privileged Identity Management

## Identifier les brèches et agir

- Office 365 Advanced Threat Protection
- Office 365 Advanced Security Management / EMS Cloud App Security
- EMS Advanced Threat Analytics
- EMS Azure Active Directory Identity Protection
- Windows Advanced Threat Protection & Windows Information Protection



# Deuxième exemple : la sauvegarde et protection des données avec Azure

## Azure Site Recovery

Reprise  
d'activité



Protégez vos applications de temps d'indisponibilité en les répliquant sur Azure

Extension de  
datacenter



Etendez votre datacenter dans Azure et profitez des services Cloud disponibles

## Azure Backup

Backup  
d'entreprise



Sauvegardez des données sur site vers le cloud. Remplacez la sauvegarde sur cassette et restez conforme

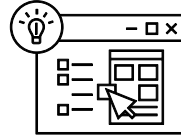
Backup IaaS



Protégez vos investissements cloud en assurant la protection des VM

# Ressources

## Microsoft Trust Center



<https://Microsoft.com/GDPR>

<https://aka.ms/gdprwhitepaper>

<https://aka.ms/emsgdprwhitepaper>

<https://aka.ms/gdprebook>

<https://aka.ms/gdprpartners>

- Cloud Security Practice Development Playbook
- GDPR Assessment
- GDPR Detailed Assessment
- GDPR Activity Hub
- Demos :

<https://demos.microsoft.com/materials;searchKeyword=GDPR>

