CLUB D'AFFAIRES ATLANTIQUE

RGPD

Quelle conformité ?
Qu'exige le règlement ?
Par où commencer ?

RÈGLEMENT GÉNÉRAL DE PROTECTION DES DONNÉES

Médéric GUERIN – PERINOVE
Certifié « Data Protection Officer »

PERINOVE

- Zoom sur les données personnelles
- Pourquoi le RGPD ? Enjeux & opportunités
- Etre en conformité, c'est quoi ?

La Data ?

La nouvelle ruée vers l'Or

Qu'est ce qu'une donnée personnelle ?

Art 4 du RGPD

Toute information se rapportant à une personne physique susceptible d'être identifiée directement ou indirectement

Quelle type d'information?

- **L'adresse IP d'un pc ou d'un smartphone** associée aux informations détenues par un fournisseur d'accès internet est susceptible de permettre d'identifier une personne
- Le numéro de sécurité sociale
- Le numéro d'immatriculation de la voiture personnelle
- …

Collecte de données

Formulaire en liane

Les données sensibles

Les données sensibles sont celles qui font apparaître, directement ou indirectement

- Les origines raciales ou ethniques d'une personne
- les opinions politiques, philosophiques ou religieuses d'une personne
- l'appartenance syndicale d'une personne
- des informations relatives à la santé d'une personne
- des Informations sexuelles relatives à une personne

La collecte et le traitement de ces données sont interdits sans le consentement préalable et explicite de la personne !

Les données sensibles

…

- données génétiques,
- données relatives aux infractions pénales, aux condamnations etc.,
- données comportant des appréciations sur les difficultés sociales des personnes,
- données biométriques

Sont interdits sauf : en cas de consentement préalable et explicite de la personne, de traitement d'une obligation ou de données rendues publiques par la personne

Les traitements de données

Principes des traitements de données

- licites,
- limitation de la finalité, explicite et légitime
- données minimisées, exactes et intègres,
- limitation de la conservation,
- confidentiels et sécurisés

Sous la responsabilité du Responsable de Traitement

- Annuaire du personnel
- Procédure de recrutement
- Vidéosurveillance
- Questionnaire qualité
- Dispositif d'écoute téléphonique
- Prospection commerciale par email
- Accès aux locaux par badge

PERINOVE

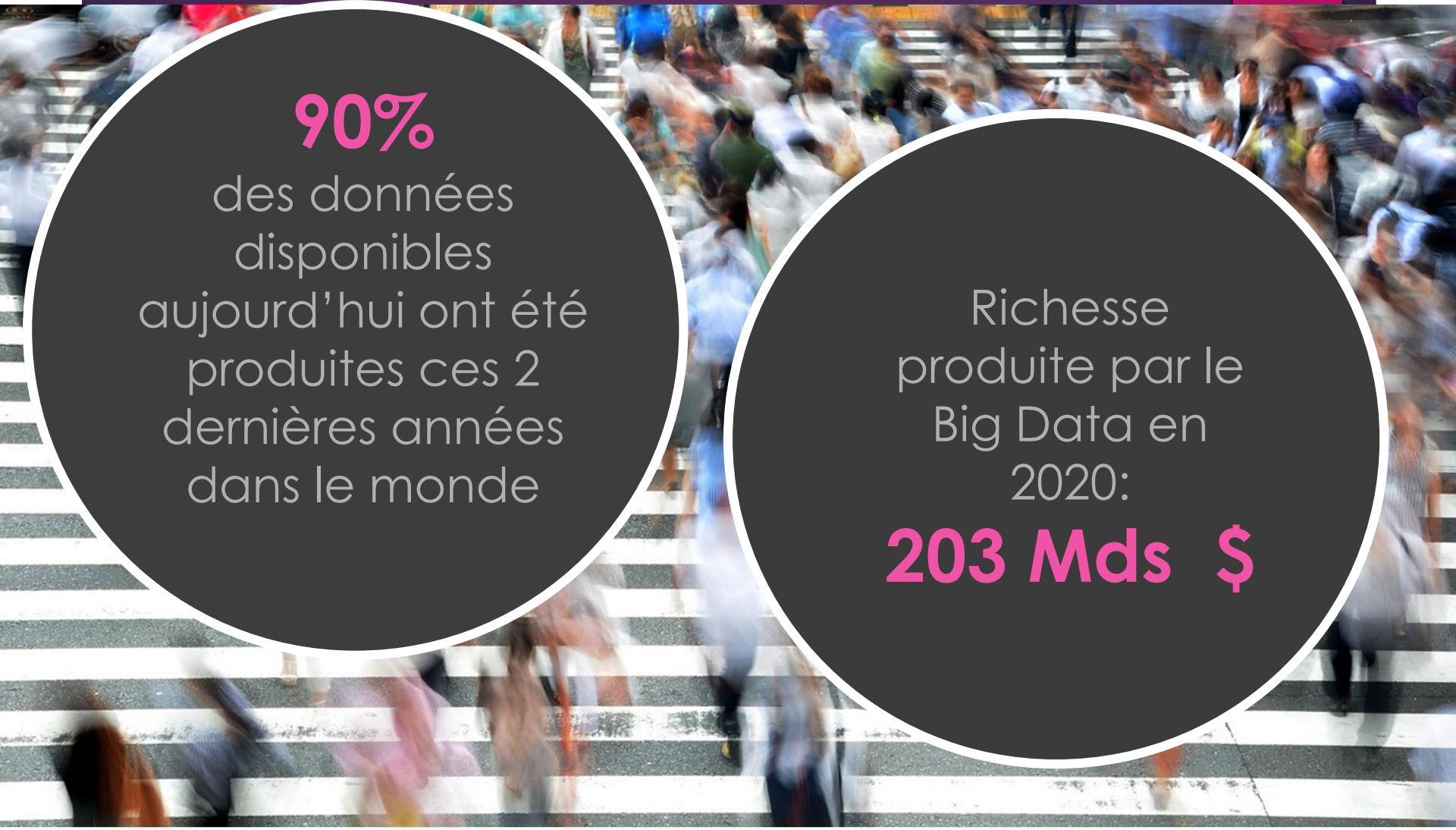
La donnée dans l'Entreprise

vos fichiers clients particuliers,
adhérents, salariés, etc

Le patrimoine informationnel de votre entreprise à protéger

Pourquoi le RGPD ?

- Règlement européen 2016/679 du 27 Avril 2016
- Droit fondamental mais non absolu
- Le règlement ne doit pas être adapté à la loi français et s'applique directement (prioritairement à la loi)
- Le RGDP laisse de la place à des précisions des états



90%
des données disponibles aujourd'hui ont été produites ces 2 dernières années dans le monde

Richesse produite par le Big Data en 2020:
203 Mds $

Contexte actuel

- Nouvelles technologies
- Cyberattaques à répétition
- Externalisation informatique (données hébergées chez prestataires en Inde / Afrique)
- Cloud computing : hébergement de données sur des supports de stockage géographiquement mouvants

60%

des attaques et vols de données ont concerné une PME en 2017

Source : Ministère de l'Intérieur

Réaction du législateur européen

- canaliser le flux d'informations
- assurer la protection de la vie privée dans l'univers digital

Application du RGPD

TPE/PME, start up, sociétés du CAC 40, banques, assurances, cybermarchands, SSII, fournisseurs de services SaaS, éditeurs d'applications mobiles ou autres dispositifs connectés, syndicats, C.E, associations, etc

- à tous les secteurs d'activités,
- public ou privé,
- quelle que soit la taille de l'organisation,
- dès lors que des citoyens européens sont concernés

Objectifs du RGPD

Responsabiliser davantage les entreprises en développant l'auto-contrôle

Uniformiser au niveau européen la réglementation sur la protection des données

Renforcer le droit des personnes

- Droits d'accès aux données traitées et aux finalités du traitement
- Droit de rectification
- Droit d'opposition
- Droit contre le traitement automatisée et le profilage
- Droit à la limitation du traitement
- Droit à la portabilité du traitement
- Droit à l'oubli

Renforcer le relationnel client

LA CONFIANCE

Une meilleure image grâce aux CERTIFICATIONS de la CNIL

Avantage concurrentiel

Opportunité de DIFFERNCIATION

Comment faire? Par quoi commencer?

Les premières étapes

PERINOVE

La CNIL : Une démarche en 6 étapes

- **Désigner** un pilote
- **Cartographier** les traitements
- **Prioriser** les actions
- **Gérer** les risques
- **Organiser** les processus
- **Documenter** la conformité

1 Je renseigne le **Registre des Traitements**

2 Je **recense** et je **documente** des protections simples

3 Je **sensibilise** mes collaborateurs

Puis je **Désigne** un pilote (DPO ou non)

La Base du RGPD : le Registre des Traitements

Le REGISTRE DES TRAITEMENTS

Le registre doit être vu comme un outil du principe d'«accountability» c'est-à-dire de responsabilité inscrit à l'article 30 du RGPD

Cela implique notamment que le responsable du traitement soit à même de pouvoir démontrer la conformité des activités de traitement.

Exemple de Registre des Traitements

	Identification du traitement				Acteurs	Finalité du traitement	Transferts hors UE ?	Données sensibles ?
1								
2	Nom / sigle	N° / REF	Date de création	Dernière mise à jour	Responsable du traitement	Finalité principale	Oui /non	Oui/non
3								
4	Fichier clients	1	08 03 2015	10 03 2018	Mr DUPONT, Dirigeant	Gestion adminsitrative et comme	non	non
5								
6	Mise en ligne sur le site internet de l'entreprise du trombinoscope de l'équipe commerciale	2	10 0					
7								
8								
9								
10								
11								
12								
13								
14								
15								

Fiche de registre ref-000

Description du traitement	
Nom / sigle	
N° / REF	ref-000
Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	V
Responsable du traitement				
Délégué à la protection des données				
Représentant				
Responsable(s) conjoint(s)				

Finalité(s) du traitement effectué	
Finalité principale	
Sous-finalité 1	
Sous-finalité 2	
Sous-finalité 3	
Sous-finalité 4	
Sous-finalité 5	

Mesures de sécurité	
Mesures de sécurité techniques	
Mesures de sécurité organisationnelles	

Catégories de données personnelles concernées	Description	Délai d'effa
Etat civil, identité, données d'identification, images...		
Vie personnelle (habitudes de vie, situation familiale, etc.)		
Informations d'ordre économique et financier (revenus, situation financière,		
Données de connexion (adress IP, logs, etc.)		

[A télécharger sur le site de la CNIL]

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Authentifier les utilisateurs

- Définissez un identifiant (login) unique à chaque utilisateur
- Adoptez une politique de mot de passe utilisateur conforme aux recommandations de la CNIL
- Obligez l'utilisateur à changer son mot de passe après réinitialisation
- Limitez le nombre de tentatives d'accès à un compte

Je recense/documente des protections simples

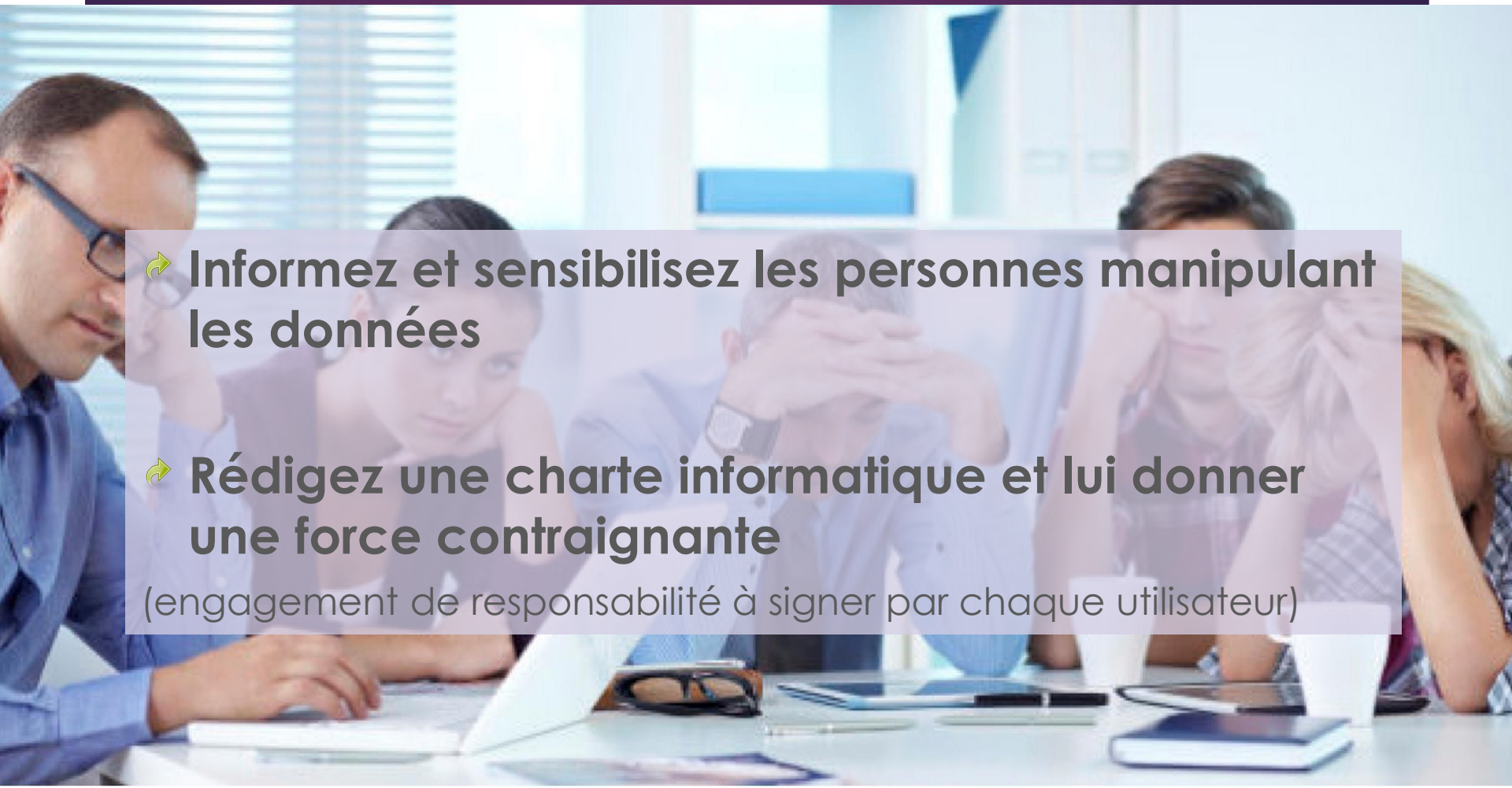
Gérer les habilitations

- Définissez des profils d'habilitation
- Supprimez les permissions d'accès obsolètes
- Réaliser une revue annuelle des habilitations

Sécuriser les postes de travail

- Prévoyez une procédure de verrouillage automatique de session
- Utilisez des antivirus régulièrement mis à jour
- Installez un « pare-feu » (firewall) logiciel

3 - Je sensibilise mes collaborateurs



- **Informez et sensibilisez les personnes manipulant les données**
- **Rédigez une charte informatique et lui donner une force contraignante**

(engagement de responsabilité à signer par chaque utilisateur)

La CNIL : Une démarche en 6 étapes

- **Désigner** un pilote
- **Cartographier** les traitements
- **Prioriser** les actions
- **Gérer** les risques
- **Organiser** les processus
- **Documenter** la conformité

1 Je renseigne le **Registre des Traitements**

2 Je **recense** et je **documente** des protections simples

3 Je **sensibilise** mes collaborateurs

Puis je **Désigne** un pilote (DPO ou non)

Nouveautés du RGPD

Désignation d'un DPO / DPD

Renforcement des droits des personnes et preuve du consentement renforcée

Actions collectives

Privacy by design

Accountability ou documenter sa conformité

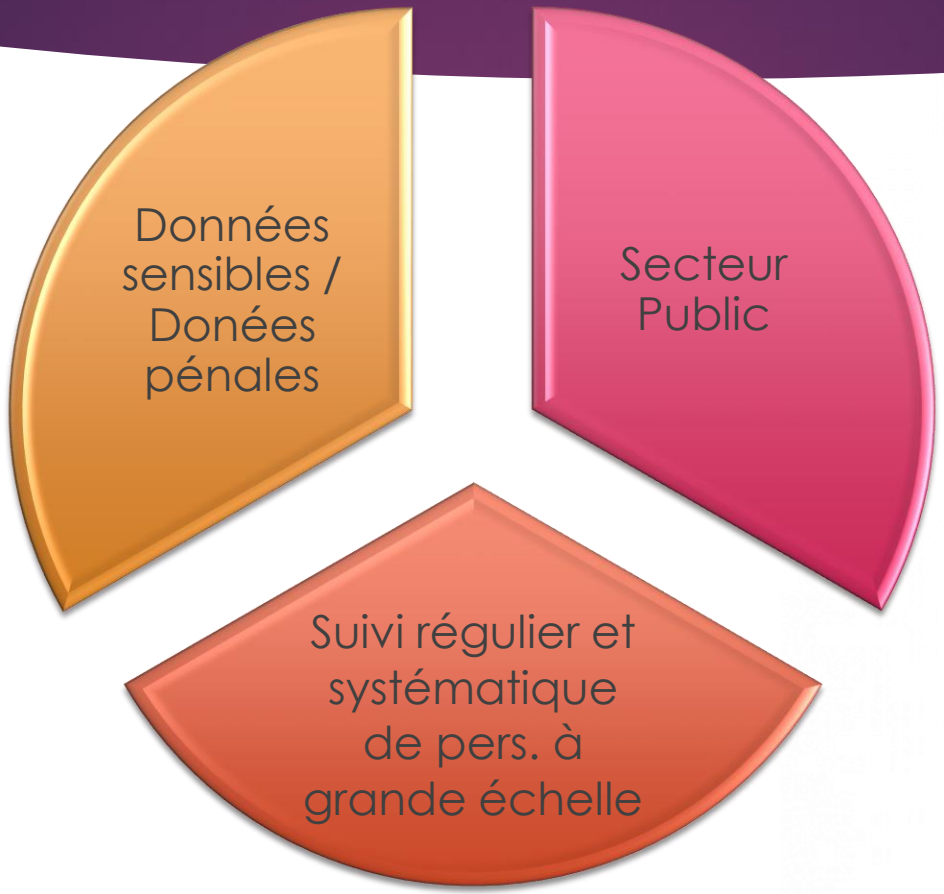
Sécurité et notification des failles de sécurité dans les 72h

La co-responsabilité avec le sous traitant

Intensification des sanctions

Le DPO (Data Protection Officer**)** ou **DPD** (Délégué à la Protection des Données)
Désignation obligatoire du DPD ou DPO sous certaines conditions

Le DPO – Une obligation si …



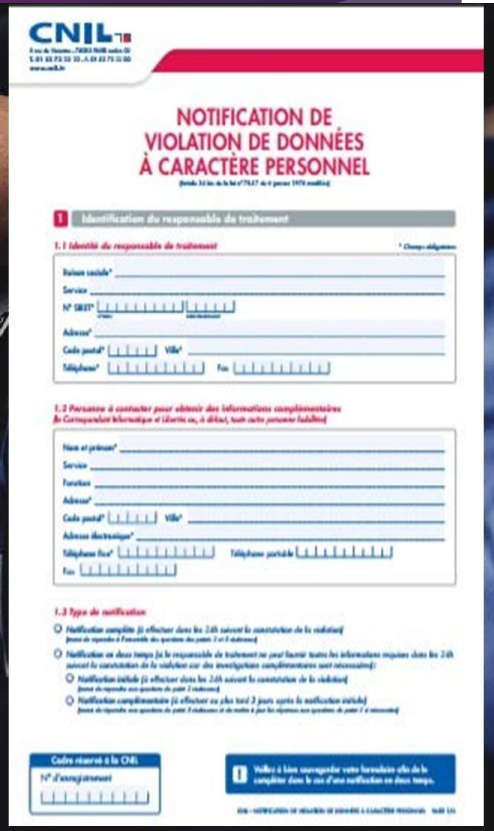
Le DPO – Son rôle

Mission d'information, de conseil et de contrôle.

- Externe, interne ou mutualisé
- Ne dois pas être Resp. de Traitements
- Interface avec la CNIL, indépendant
- Conseil, alerte, recommande, forme
- Désigné sur la base d'une lettre de mission par le Resp. Traitement
- Affectation de ressources humaines et financières suffisantes
- Associé en amont à toutes les questions relatives aux Données Personnelles

Obligation de notification des violations de données personnelles - Art 33 RGPD

- Destruction
- Perte
- Altération
- Divulgation
- Accès non autorisé à des données personnelles, de manière accidentelle ou illicite


CNIL

NOTIFICATION DE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

1 Identification du responsable de traitement

1.1 Identité du responsable de traitement

1.2 Personne à contacter pour obtenir des informations complémentaires

1.3 Type de notification

Cadre réservé à la CNIL

N° d'enregistrement

Formulaire de notifications de la CNIL

Protéger vos données

93% des entreprises ayant perdu leurs données ou l'accès à celles-ci pendant 10 jours ou plus, ont fait faillite dans l'année suivant la catastrophe.

En 2017, **1 entreprise sur 3** a déjà subi un incident ou une panne qui a nécessité le déclenchement d'un **plan de reprise d'activité**

Sauvegarder et prévoir la continuité d'activité

Effectuez des sauvegardes régulières
Stockez les supports de sauvegarde dans un endroit sûr (pas forcement au bureau)

Protéger vos données

Archiver vos données…
de manière sécurisée

Détruisez les archives obsolètes de manière sécurisée
Investissez dans un broyeur de document

Utiliser des fonctions cryptographiques
Utilisez des algorithmes, des logiciels et des bibliothèques reconnues,
Conservez les secrets et les clés cryptographiques de manière sécurisée

Responsabilité partagée entre le responsable du traitement et le sous-traitant

Uniformisation des obligations pesant sur les responsables de traitements et les sous-traitants

Le Sous traitant,

- A une obligation de conseil // client
- Doit maintenir un registre des traitements de données
- Désigne un Délégué à la protection des données (ex-CIL)
- Sa responsabilité est engagée en cas de violation de DP par exemple

Des sanctions renforcées !

2% du C.A annuel mondial ou 10M€

- défaut de tenue d'un registre des traitements,
- défaut d'étude d'impact sur la vie privée en cas de données sensibles (orientations sexuelles, politiques, informations médicales…),
- défaut d'annonce suite à une faille décelée, et problèmes de sécurité.

4% du C.A annuel mondial ou 20 M€

- défaut de consentement,
- traitements de données illégaux,
- non-respect des droits des personnes,
- manque de prudence lors des transferts transfrontaliers de données

1er Bilan après 4 mois

+ 742 notifications de violation

concernant 33 millions de personnes en France et ailleurs

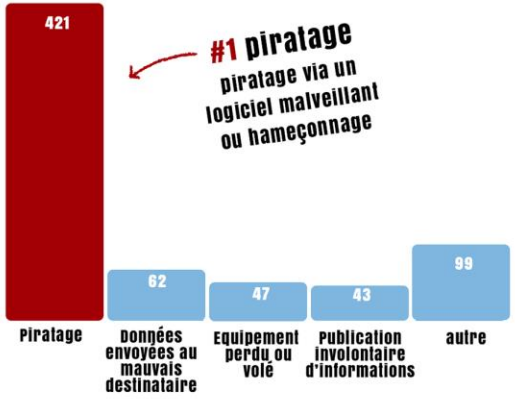
Problèmes rencontrés

1. Hôtellerie
2. sciences techniques
3. commerces auto-moto
4. information communication
5. finance assurances

185 notifications

« Notre prestataire de réservation a subi une violation de données. Il m'a averti que mon hôtel figurait dans la liste des victimes. Il m'a rappelé le contexte et conseillé de signaler cette violation auprès de la CNIL dans un délai de 72h. Il a mis en place une hotline et nous a envoyé une lettre type pour informer les clients qui figurent dans la base piratée. »

Tony D.
Gérant d'un hôtel

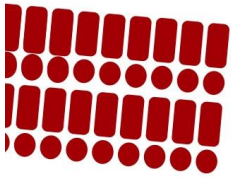


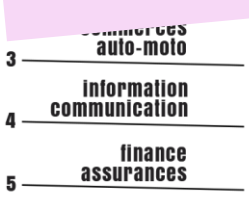
Source CNIL – 1er Oct. 2018

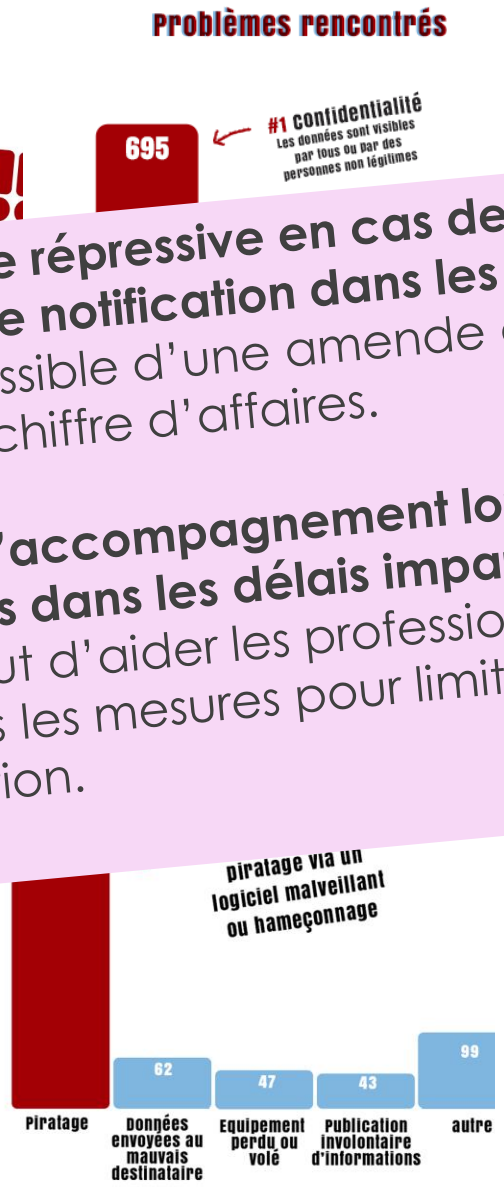
1er Bilan après

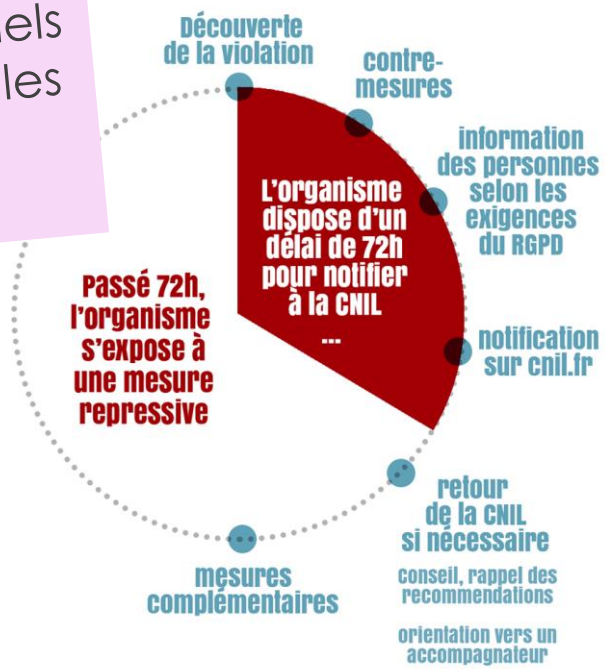
La CNIL adopte une approche répressive en cas de non-respect de l'obligation de notification dans les 72h. Ce manquement est passible d'une amende de 10 millions d'euros ou 2% du chiffre d'affaires.

En revanche, elle privilégie l'accompagnement lors de la réception des notifications dans les délais impartis, une approche qui a pour but d'aider les professionnels concernés à prendre toutes les mesures pour limiter les conséquences d'une violation.









Source CNIL – 1er Oct. 2018

Merci

Médéric GUERIN
06 81 97 18 67
mguerin@perinove.fr
PERINOVE