RGPD

Appréhender la démarche de mise en conformité RGPD pour vos entreprises.

Le RGPD…

C’est quoi ?

Que signifie-t-il pour votre Entreprise?

RGPD

En français: **RGPD:** **R**èglement **G**énéral à la **P**rotection des **D**onnées
En anglais: **GDPR:** **G**eneral **D**ata **P**rotection **R**egulation

Texte de référence européen en matière de protection des données personnelles pour les résidents de l'UE.

Applicable depuis le :

Objectifs:

- ✓ Redonner aux Citoyens Européens le contrôle sur leurs données personnelles en renforçant leurs Droits (Droit à la portabilité, Droit à l'oubli, Droit d'opposition…) et en leur donnant plus de visibilité sur les données transmises.
- ✓ Responsabiliser les Entreprises en renforçant la protection des données personnelles.
- ✓ Uniformiser la protection des données personnelles au sein de l'Union Européenne.

RGPD

Loi Informatique et Libertés

Régiment <u>déclaratif</u> des Traitements

Règlement Général à la Protection des Données

Délégué à la protection des données

Logique de <u>responsabilisation</u> des Traitements et de <u>justification de la protection</u> des données personnelles.

Les entreprises sont désormais pleinement responsables de la façon dont les données personnelles (Traitement existants, nouveaux Traitements) sont recueillies et exploitées.

RGPD

En bref…

99

Articles

11

Chapitres

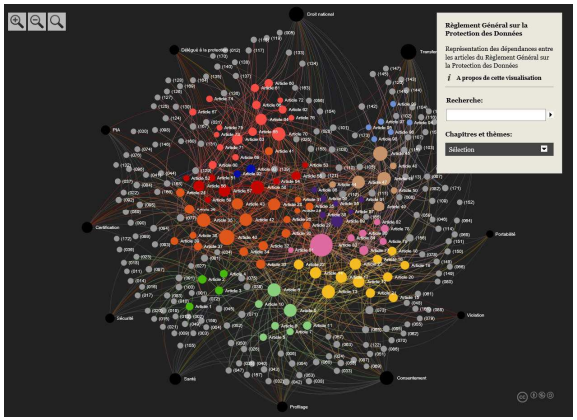
173

« Considérants »

≃200

Pages

Dataviz



https://www.cnil.fr/fr/reglement-europeen-protection-donnees/dataviz

1 (Article 32)

Parlant de Technologie

RGPD

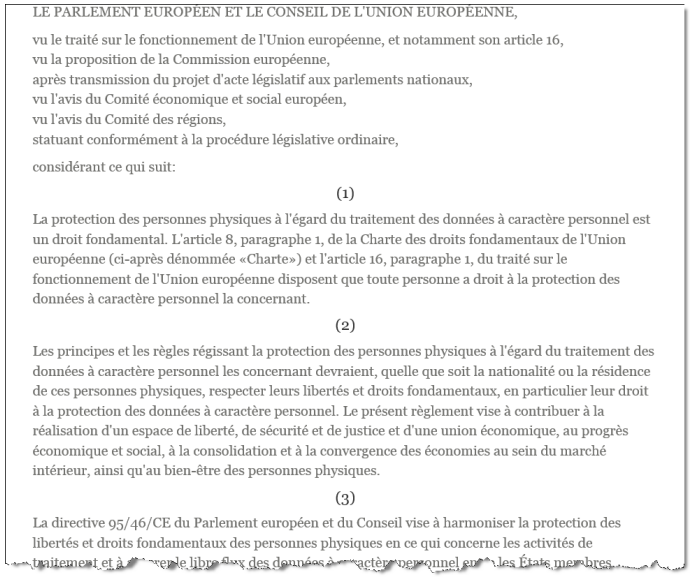
Quelle forme…

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

27 avril 2016

Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Sommaire



LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,
vu la proposition de la Commission européenne,
après transmission du projet d'acte législatif aux parlements nationaux,
vu l'avis du Comité économique et social européen,
vu l'avis du Comité des régions,
statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1)

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant.

(2)

Les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes physiques, respecter leurs libertés et droits fondamentaux, en particulier leur droit à la protection des données à caractère personnel. Le présent règlement vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques.

(3)

La directive 95/46/CE du Parlement européen et du Conseil vise à harmoniser la protection des libertés et droits fondamentaux des personnes physiques en ce qui concerne les activités de traitement et à [illegible] le libre flux des données à caractère personnel entre les États membres.

https://www.cnil.fr/fr/regelement-europeen-protection-donnees

Donnée personnelle

Définition: Une Donnée personnelle ou à caractère personnel est une Donnée qui permet de caractériser/identifier une personne physique.

Donnée personnelle

Nom / Prénom

Date de Naissance

Adresse postale

Identifiant d'équipement électronique

Information médias sociaux

Photographies

Collecte de données IoT

Adresse mail

Donnée personnelle sensible

Origine raciale ou ethnique

Orientations et préférences sexuelles

Opinions politiques, philosophiques ou religieuses

Adhésion syndicale

Santé

Donnée génétique / Biométrique

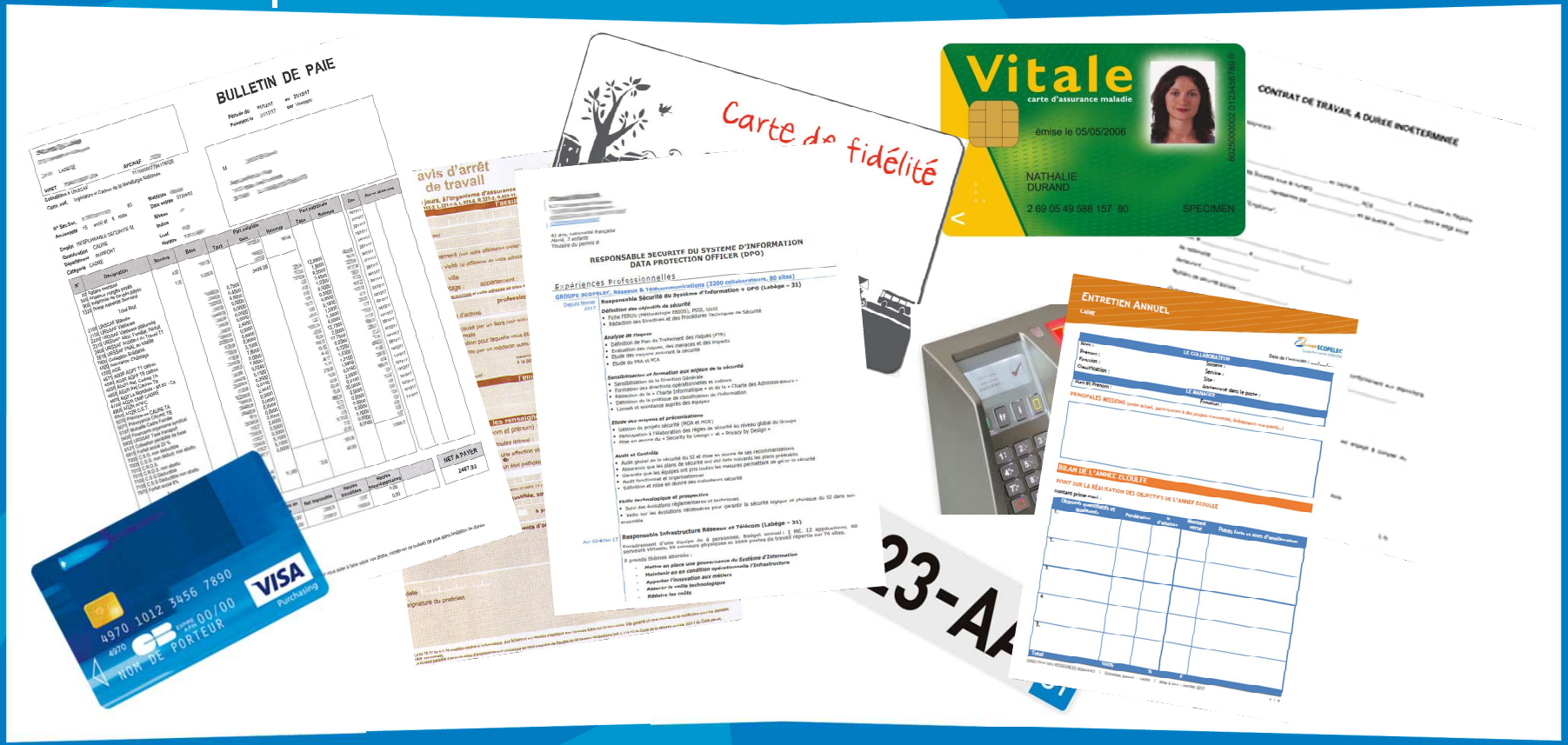
Séquences génétiques

Empreintes digitales

Reconnaissance faciale

Scan rétiniens

Donnée personnelle



Groupe SCOPELEC
La performance collective

Le RGPD…

A qui s’applique t-il ?

RGPD

Le RGPD s'applique à:

- ❑ Tous les Etats membres de l'UE y compris le Royaume-Uni (malgré le Brexit).
- ❑ Tous les organismes dans le monde qui collectent, stockent, traitent des données personnelles appartenant à des citoyens de l'**U**nion **E**uropéenne dont l'utilisation peut directement ou indirectement permettre de les identifier, c'est-à-dire:

- ✓ les acteurs économiques et sociaux européens (entreprises, associations, administrations, collectivités locales, syndicats d'entreprise)
- ✓ les Sous-traitants
- ✓ les Entreprises hors Union Européenne (GAFA) qui proposent des services et biens sur le marché européen

Le RGPD s'applique à toutes les structures publiques comme privées et ce quelle que soit leur taille.

RGPD

Les obligations du RGPD supposent qu'une Entreprise doit à tout moment savoir de quelles données elle dispose, leur localisation, l'objectif de leur collecte, leur mode de gestion, stockage, sécurisation, transfert et effacement.

Il s'agit de toutes les données détenues par l'Entreprise (Internes, externes, de passage).

Tous les Traitements (Traitement existants, nouveaux Traitements) de l'information doivent être conformes.

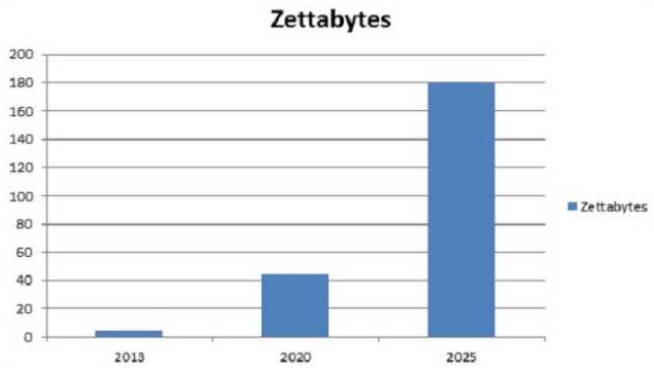
La CNIL, autorité de contrôle pour la France sera en mesure de contrôler les Entreprises.

RGPD

Le RGPD, c'est
renforcer la protection des données personnelles…

Mais pourquoi concrètement ?

Augmentation exponentielle des données



Source: IDC

1 ZB en 2011

4 ZB en 2013

44 ZB en 2020

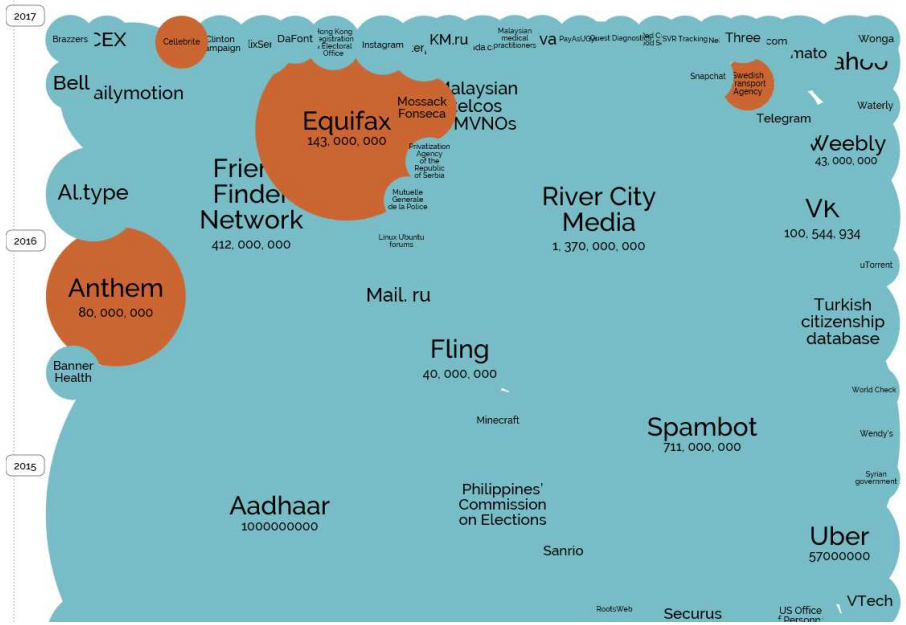
1ZB = 1^{21} octets = 1 000 000 000 000 000 000 000 octets

= 1 000 Milliard de GB

= 152 Million d'années de vidéos HD

RGPD

Augmentation exponentielle des fuites de données



Groupe SCOPELEC
La performance collective

RGPD

- ✓ Augmentation du volume de données
- ✓ Augmentation du nombre d'utilisateurs d'Internet
- ✓ Augmentation des fuites de données
- ✓ Augmentation des menaces

Se prémunir des fuites d'informations

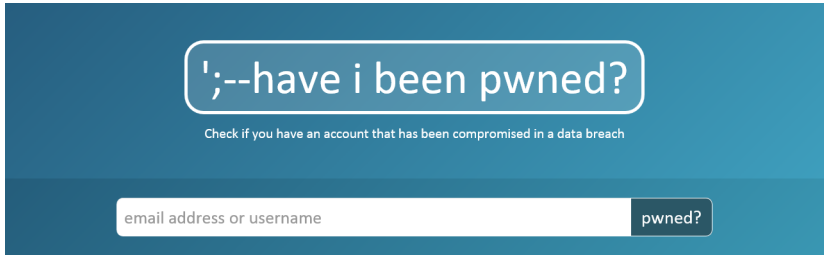
Protéger les Utilisateurs/Citoyens

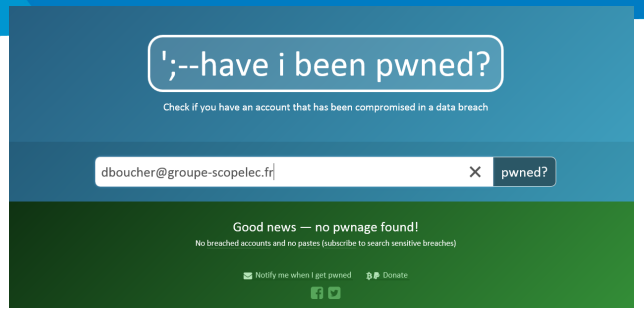
Leur divulgation ou leur mauvaise utilisation pourrait porter atteinte aux droits et libertés des personnes ou à leur vie privée.

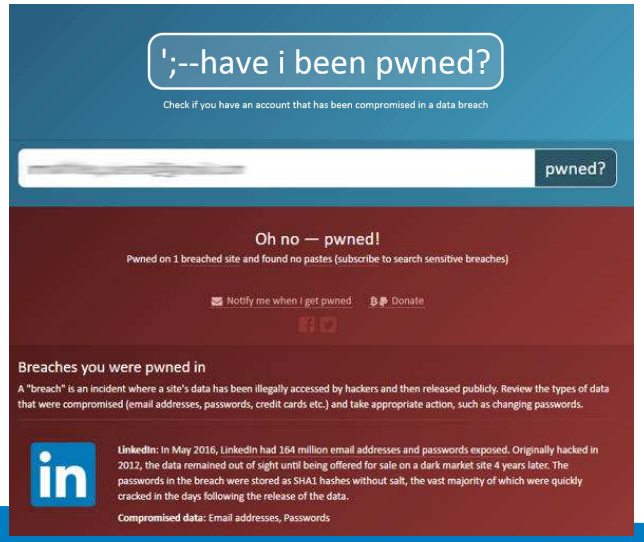
Faites le test...

Vérifiez si vos données ont été piratées

Le site « **Have I been pwned** » vérifie si votre email est concerné par l'une des Cyberattaques recensées par le site et ayant pu engendrer la violation de vos données personnelles.



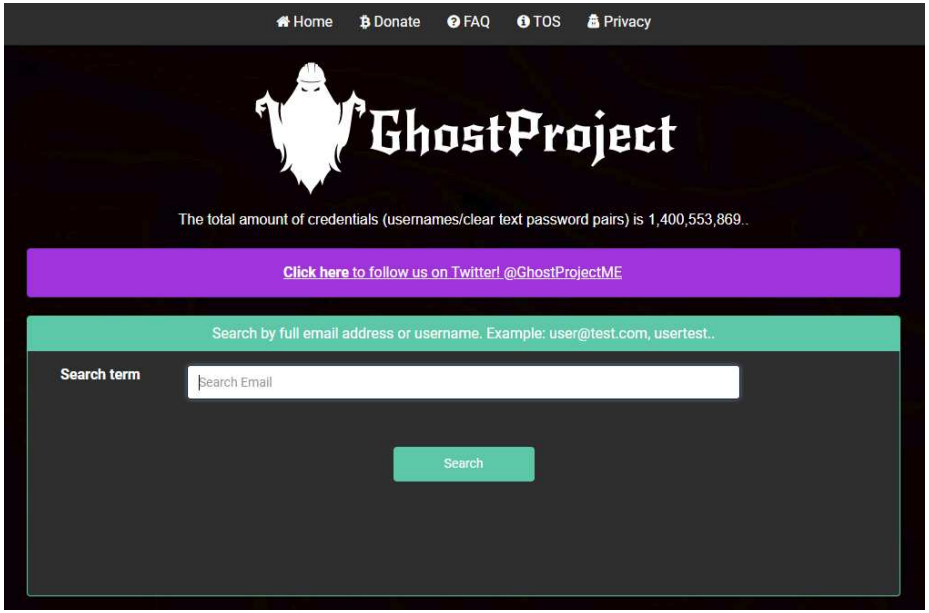




https://haveibeenpwned.com

Faites le test…

Retrouver le mot de passe d'un compte Mail



Quels sont les devoirs de l'Entreprise en cas de fuites ou de violations des données personnelles ?

- ✓ En référer à la CNIL (autorité de contrôle pour la France) dans les 72h00 (Art. 33)
- ✓ Notifier obligatoirement les incidents de sécurité ainsi que les atteintes aux Salariés de l'Entreprise en cas de risque d'atteinte à la protection de leur vie privée en lui apportant les explications nécessaires.
- ✓ Apporter une remédiation.

Que se passe t-il en cas de non-conformité du Règlement ?

→ **Amende Administrative**
(4% du CA annuel pour les Entreprises, 20 millions d'€ minimum pour les Administrations.

→ **Amende au tribunal pénal**

→ **Eventuels dommages et intérêts**
Si une plainte a été déposée.

Effets collatéraux:

- ✓ Vols de données Business
- ✓ Perte de parts de marchés
- ✓ Dégâts pour l'image de marque

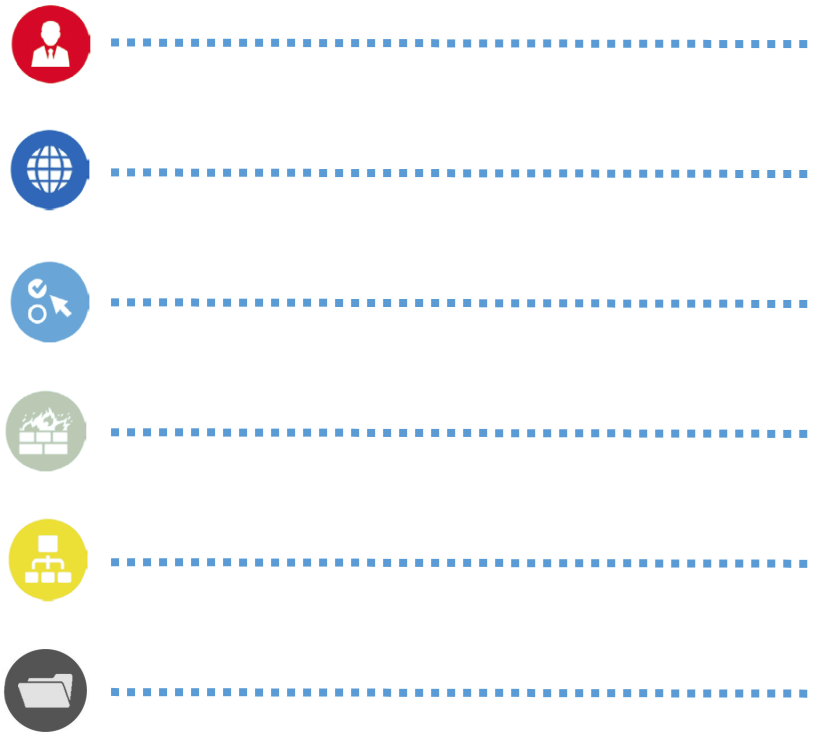
**Sur le plan pénal, la responsabilité en matière de RGPD est allouée…
au CHEF D'ENTREPRISE.**

Le RGPD…

Comment procéder pour que votre Entreprise soit en conformité avec le RGPD ?

Se préparer en 6 étapes

CNIL.



ETAPE 1
DESIGNER UN PILOTE

ETAPE 2
CARTOGRAPHIER LES TRAITEMENTS DE DONNEES PERSONNELLES

ETAPE 3
PRIORISER LES ACTIONS

ETAPE 4
GERER LES RISQUES

ETAPE 5
ORGANISER LES PROCESSUS INTERNES

ETAPE 6
DOCUMENTER LA CONFORMITE

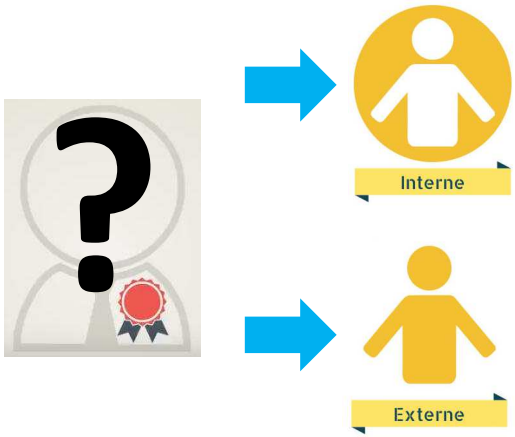
Groupe SCOPELEC
La performance collective

RGPD

ETAPE 1: Désigner un pilote (1/3)

Nomination du DPO

C'est le Chef d'orchestre de la conformité en matière de protection des données au sein de son Organisation.



OBLIGATOIRE POUR (Art.37):

- Les Organismes Publics (Mairie, Ministère)
- Les Organisations avec des activités nécessitant la surveillance à grandes échelle des personnes (compagnie d'assurance, de banque…)
- Les Organisations traitant des données « sensibles » (hôpital, site de rencontre…)

Contexte: ≥ 250 Salariés

ETAPE 1: Désigner un pilote (2/3)

Le Responsable de Traitement (RT)

Rôle: Il est le référent du traitement des données à caractère personnel au sein de son Organisation. C'est le Responsable légal d'un point de vue juridique.

Le RT doit:

- Avoir un niveau hiérarchique suffisant pour « décliner » ses données personnelles.
- S'assurer de leur bonne sécurisation.
- Donner les accès et les contrôler.
- Etablir une liste de personnes autorisés à les manipuler.

RGPD

ETAPE 1: Désigner un pilote (3/3)

1. Formation au DPO, DSI, RSSI, Responsable Qualité

2. Formation/Sensibilisation en COMEX/CODIR

3. Formation aux Services / Tronc commun + Adaptation métier (Services RH, Juridique, Marketing, Commercial,…)

En continu

ETAPE 2: Cartographier vos traitements de données personnelles (1/3)

1. REGISTRE DES ACTIVITES DE TRAITEMENT

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	**Nom :** Cliquez ici. **Prénom :** Cliquez ici. **Adresse :** Cliquez ici. **CP :** Cliquez ici. **Ville :** Cliquez ici. **Téléphone :** Cliquez ici. **Adresse de messagerie :** Cliquez ici.
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	**Nom :** Cliquez ici. **Prénom :** Cliquez ici. **Société (si DPO externe) :** Cliquez ici. **Adresse :** Cliquez ici. **CP :** Cliquez ici. **Ville :** Cliquez ici. **Téléphone :** Cliquez ici. **Adresse de messagerie :** Cliquez ici.

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités
Activité 1	Cliquez ici. ex. Gestion de la paie
Activité 2	Cliquez ici. ex. Gestion des prospects
Activité 3	Cliquez ici. ex. Gestion des fournisseurs
Activité 4	Cliquez ici. ex. Vente en ligne
Activité 5	Cliquez ici. ex. Sécurisation des locaux

https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

ETAPE 2: Cartographier vos traitements de données personnelles (2/3)

2. FICHE DE REGISTRE DE L'ACTIVITE

Pour chaque traitement de données personnelles, posez-vous les questions suivantes :

Acteurs internes ou externes traitant les données

Catégorie des données traitées

Finalité du Traitement

Lieu où les données sont hébergées

Durée de conservation des données (Cycle de vie)

Mesures de sécurité mises en œuvre pour minimiser les risques d'accès non autorisés aux données

https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

1 TRAITEMENT = 1 FINALITÉ

RGPD

ETAPE 2: Cartographier vos traitements de données personnelles (3/3)

3. La Cartographie des risques sur les accès non autorisés aux Données à caractère personnel et donc l'impact sur la vie privée des personnes concernées (Macro)

4. L'identification des non-conformités:
   - ✓ Revue documentaire (charte informatique, PSSI, politique d'archivage des données, formulaires de consentement,…)
   - ✓ Evaluations de la conformité au RGPD

PLAN D'ACTION

ETAPE 3: Prioriser les actions

Priorisation et identification des actions à mener pour se conformer aux obligations actuelles et à venir:

- → Court terme
- → Moyen terme
- → Long terme

ETAPE 4: Gérer les risques

EIVP: **E**tude d'**I**mpact sur la **V**ie **P**rivée ou PIA: **P**rivacy **I**mpact **A**ssessment

Relatif à la protection des données et obligatoire pour les traitements les plus risqués.

→ En fonction de la Cartographie des risques vue lors de l'Etape 2

Mise en œuvre:

- Organisationnelle (Désignation des RT,…)
- Juridique (Validation des documents,…)
- Des solutions Techniques (Chiffrement, Droits d'accès, Supervision, Sauvegarde, Traçage des accès…)

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

RGPD

ARTICLE 32 RGPD

Sécurité du traitement des données à caractère personnel
Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque,...

La CNIL, autorité de contrôle se base sur le Guide d'hygiène Informatique établi par l'ANSSI.
Ce guide établi 42 règles d'hygiène à respecter afin d'assurer la protection des données personnelles.

12 REGLES A SUIVRE IMPERATIVEMENT POUR ÊTRE CONFORME AU RGPD.

RGPD

ETAPE 5: Organiser les processus internes (1/5)

1. **<u>Accompagnements</u>**:
   - **Consultant Sécurité**

   → Chef de Projet Sécurité: Cartographie des risques, EIVP, consentements,…

   - **Juriste spécialisé**

   → C'est le rédacteur. Il analyse les Contrats SST, Clients, Travail, les CGV, CGU.

   - **Avocat**

   → Le Valideur du plan d'action. Peut intervenir en cas de contrôle de la CNIL.

ETAPE 5: Organiser les processus internes (2/5)

2. **Recueil du consentement**: Elément-clé de la conformité des traitements mis en œuvre puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement portant sur leurs données personnelles.

Remarques:

- 1 finalité de traitement = 1 consentement
- 1 seul consentement est nécessaire si plusieurs traitements ont la même finalité.

→ On ne peut donc pas demander un consentement pour un but trop large, trop vague.

ETAPE 5: Organiser les processus internes (4/5)

Exemple pratique de consentement « Acte positif clair et univoque »:

Lors d'un salon professionnel, vous organisez un concours et demandez aux participants de glisser leur carte professionnelle dans une urne.

→ **C'est bien un acte positif clair et univoque.**

Cela signifie l'accord de la personne à figurer sur la liste pour être candidat aux prix offerts dans le cadre de ce concours.

MAIS

Cela ne signifie pas que vous pouvez utiliser ses données personnelles pour d'autres finalités (Marketing, envoi de Newsletter,…).

UNE SEULE FINALITÉ PAR CONSENTEMENT !!!

ETAPE 5: Organiser les processus internes (5/5)

3. **<u>Garantir le droit des personnes</u>**:
- Le Droit à la portabilité des données
- Le Droit à l'effacement (Le Droit à l'oubli numérique)
- Le Droit d'opposition

RGPD

ETAPE 6: Documenter la conformité

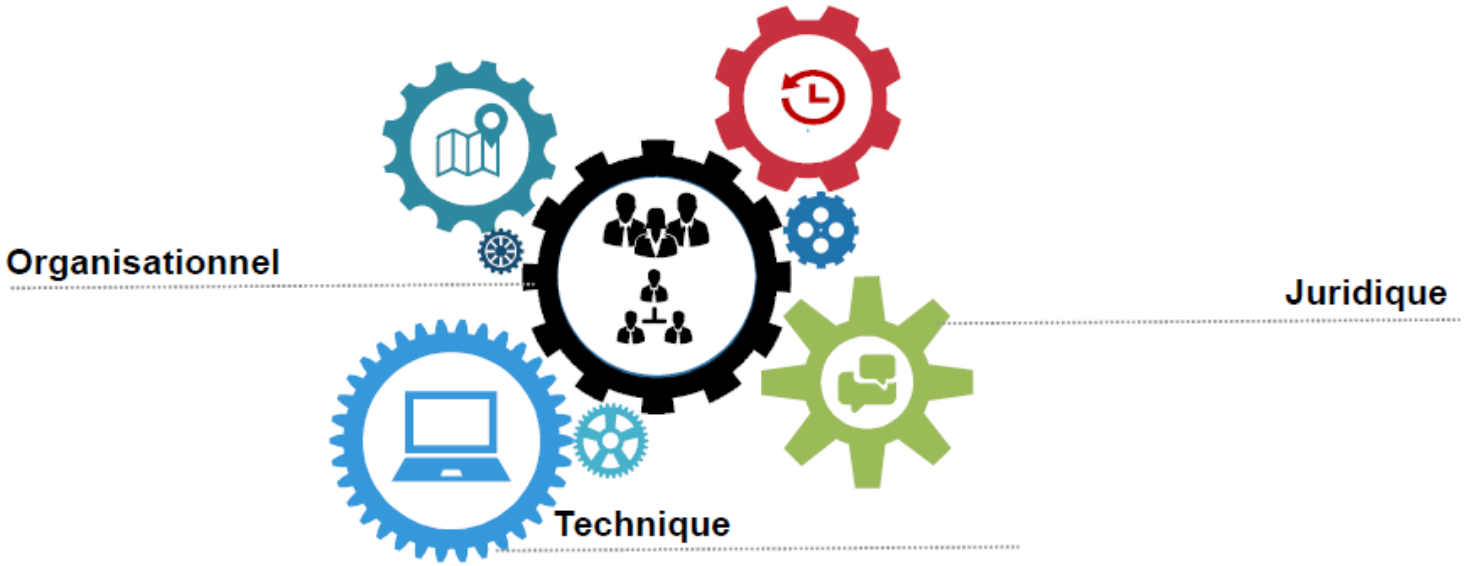
Accountability: Désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

- ✓ Prouver ce que l'on met en place.
- ✓ Documenter toutes les mesures et procédures devant assurer à tout moment la protection des données.

CONCLUSION

Conclusion

C’est un Projet qui doit s’appréhender dans ces 3 dimensions



Conclusion

Avantages collatéraux du RGPD:

Atout concurrentiel:

Améliore son image auprès de ses Collaborateurs, de ses Clients en garantissant le respect de leur vie privée (face à une population de plus en plus inquiète sur les données personnelles).

Gouvernance interne:

- ✓ Optimiser l'identification, l'utilisation et l'exploitation des différents traitements de données mis en œuvre
- ✓ Mettre fin à la multiplication de solutions ou des applications qui ne sont pas répertoriés en interne ou « sous le radar » (Shadow IT,…)
- ✓ Mieux cibler sa Cybersécurité sur les données essentielles:
  - ➢ les données personnelles
  - ➢ les données stratégiques

Mon argent ?
J'en prends soin.
Ma vie privée,
aussi.

CNIL.

Vous accompagner dans la mise en œuvre du RGPD

Groupe SCOPELEC
La performance collective

Merci pour votre attention.

Groupe SCOPELEC

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

David BOUCHER
Responsable **S**écurité du **S**ystème d'**I**nformation / DPO
dboucher@groupe-scopelec.fr / 06.83.81.99.67
CESIN

Groupe SCOPELEC
La performance collective