

# BIENVENUE

# RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES



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



25 MAI 2018

(ou **GDPR** pour:

General Data Protection Regulation)

Le RGPD s'applique quand :

- ❑ Une organisation traite de données personnelles
- ❑ Un résident de l'U.E est directement visé par un traitement de données

# RGPD



# Qu'est-ce qu'une donnée personnelle ?

Un nom/un prénom

Un e-mail

Une donnée pseudonymisée

Un numéro de téléphone

Un numéro de siret

Une adresse IP

Un cookie

Un prénom

Un président Normal

Un numéro de sécurité sociale

Une plaque d'immatriculation

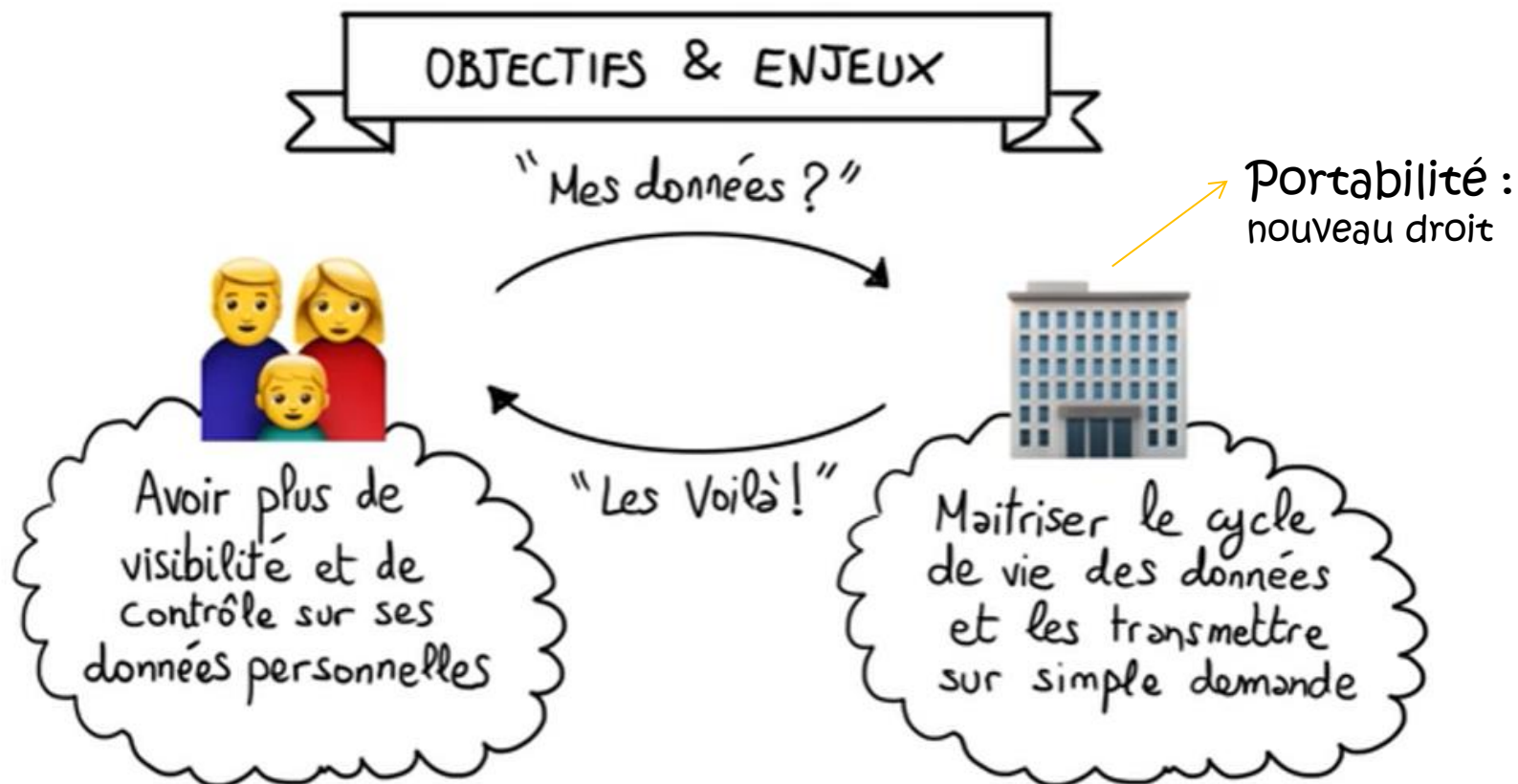
# SANCTIONS

4%

DU CHIFFRE D'AFFAIRES  
ANNUEL MONDIAL

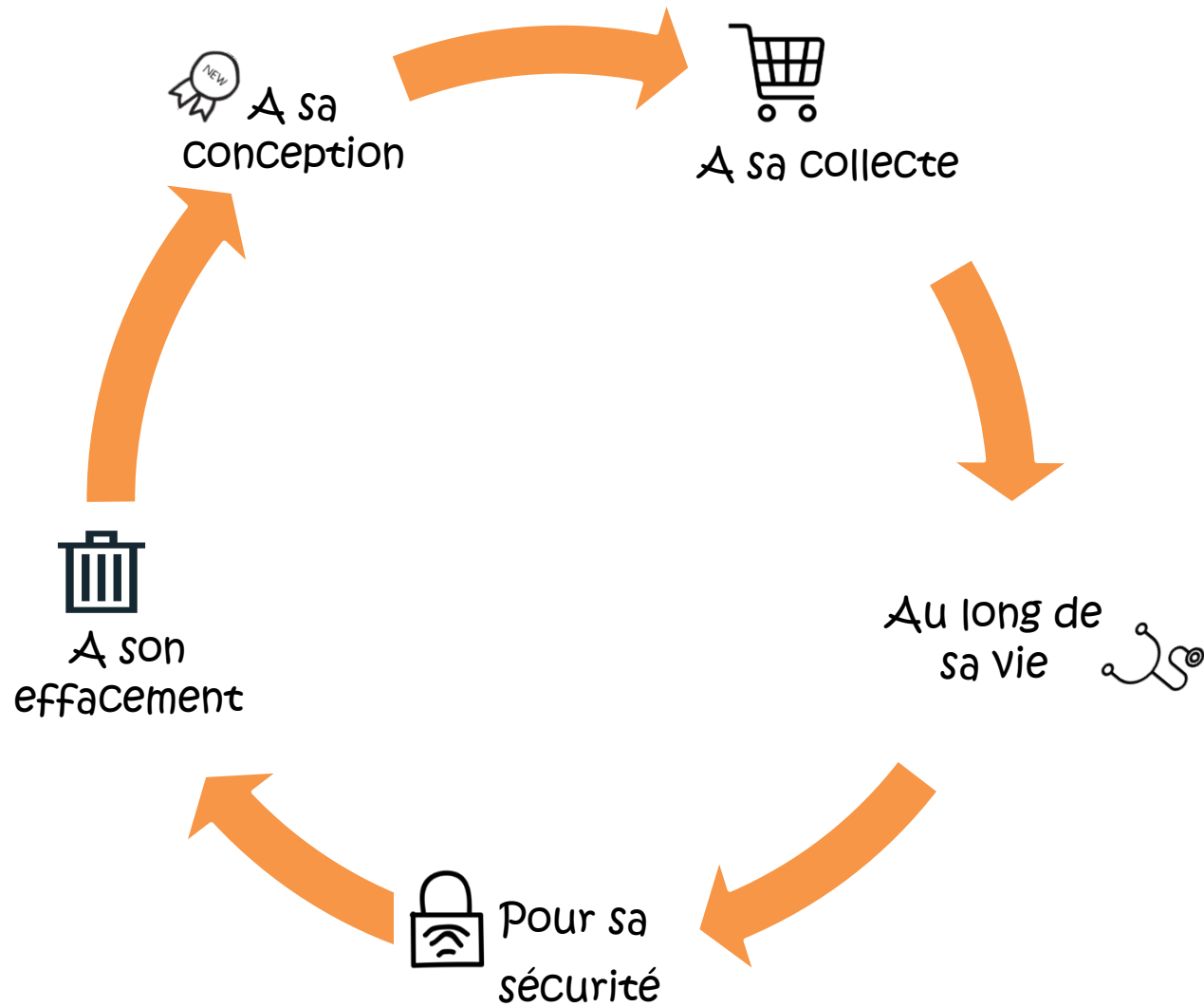
OU

20  
MILLIONS €



« À l'école, tout au long de la vie, les gens doivent prendre conscience que les données sont importantes » (Mounir Mahjoubi)

# Le cycle de vie de la donnée personnelle





# A la collecte des Données Personnelles



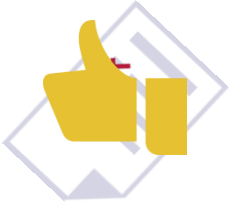
Mentions d'information

- ▶ Auteur de la collecte
- ▶ Durée de conservation
- ▶ Finalité des données collectées
- ▶ Informations sur leurs droits





# A la collecte des Données Personnelles



Si le consentement est requis ...

Exemples de consentement par finalité :

- Si vous voulez recevoir nos offres commerciales, merci de cocher cette case.
- Si vous voulez recevoir des offres de nos partenaires, merci de cocher cette case.



## La Minimisation

- Collecte du nom+prénom+ Adresse mail et postale pour envoi Newsletter ?  
L'e-mail uniquement !
- Agent immobilier ?  
Vous avez combien d'enfants ? Ils ont quel âge ?  
Vous avez combien de chambres ?
- Collecte de la date de Naissance sur un site de vente de piscine ?
- Collecte de la sécurité sociale recrutement ?

# Quelles pratiques pour les e-mails ?

BtB		BtC
E-mail générique	E-mail nominatif PRO	E-mail nominatif
Hors champ RGPD	<ul style="list-style-type: none"><li>• Le Consentement n'est pas obligatoire</li><li>• Au moment de la collecte = <a href="#">information</a></li></ul> + objet de la sollicitation en rapport avec la profession	Le Consentement préalable est obligatoire

# Sécurité et sûreté des données

Etude  
d'impact

Mesures  
techniques

Faibles de  
sécurité

Données  
sensibles

Mesures  
organisationnelles



# A l'effacement des Données Personnelles

Les données personnelles sont conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées

## Exemples pratiques :

**Abonnement EDF ?**

Le temps de la souscription + délai de prescription

**Newsletter ?**

Jusqu'au moment de la désinscription

**Coordonnées bancaires sur internet ?**

Conservées le temps de l'opération de paiement

**Agent immobilier : le prospect a acheté son bien ?**

Stop, on le retire du fichier de prospection

## Référentiel de durées CNIL :

3 ans pour la gestion d'un fichier client à compter de la fin de la relation commerciale

3 ans pour un fichier prospect à compter de leur collecte ou du dernier contact émanant du prospect

1 an pour de la vidéosurveillance

5 ans pour la gestion de la paie

2 ans pour des CV

# Les autres principes clés du RGPD

# Le Délégué à la Protection des données personnelles

- Chef d'orchestre de la mise en conformité
- Il conseille le Responsable de traitement
- Gère les registres
- Il est l'interlocuteur de la CNIL
- Il est l'interlocuteur des personnes qui ont subi une violation de leurs données personnelles ou qui veulent exercer leurs droits
- Il informe / forme les collaborateurs
- Il mène les études d'impact
- Il identifie les non-conformités

# — L'obligation de rendre compte

Accountability



Registre des traitements

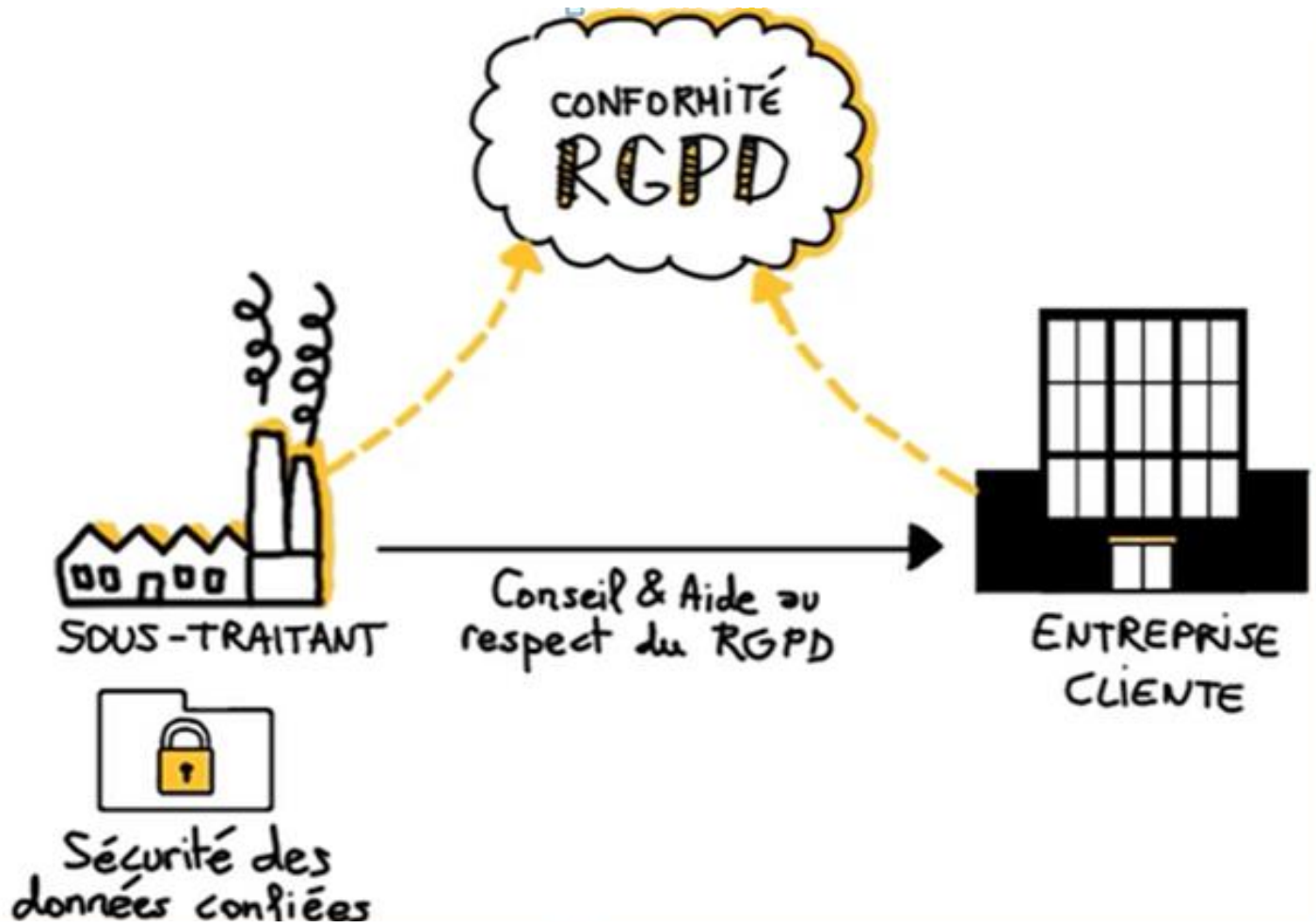


Registre des ST



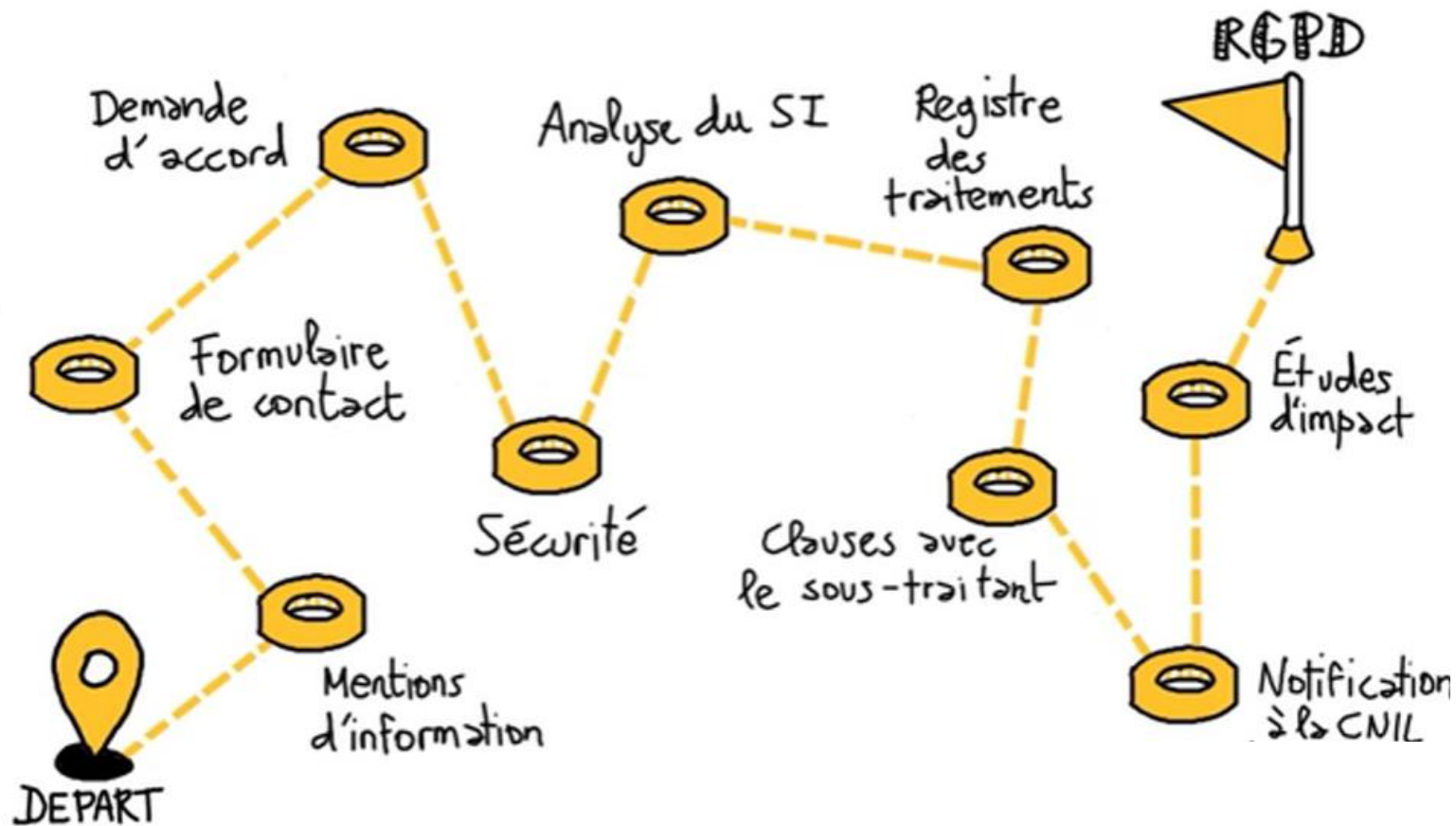
Registre des violations

# Les Sous-Traitants





# Dans quel ordre procéder ?



# En savoir plus ?

## Deux Formations clés organisées par la CCI :

1. **Se mettre en conformité avec la nouvelle réglementation européenne : RGPD**  
<http://nantesstnazaire.Cci.fr/formation-continue/web-et-culture-numerique/se-mettre-en-conformite-avec-la-nouvelle-reglementation>
2. **Devenir Délégué à la protection des données personnelles : découvrez les fondamentaux !**  
<http://nantesstnazaire.Cci.fr/formation-continue/web-et-culture-numerique/devenir-deleguee-la-protection-des-donnees-dpddpo>

## Des Liens utiles :

Formulaire DPO :

<https://www.cnil.fr/fr/designation-dpo>

RGPD, se préparer en 6 étapes :

<https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes>

Testez-vous sur le RGPD

<https://rgpd.medef.com/>

Renforcer la sécurité de son système d'information en 42 mesures :

<https://www.ssi.gouv.fr/uploads/2017/01/gui-de-hygiene-informatique-anssi.pdf>

Guide RGPD pour les PME et les ETI le 17 avril