





Le **RGPD**, qu'est ce que ça veut dire ?

RGPD

Règlement
Général pour la
Protection des
Données



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



Applicable au **25 mai 2018**



ou **GDPR** pour General Data Protection Régulation



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

RGPD



Il s'agit de **toute donnée** se rapportant
à une **personne physique identifiée**
ou **identifiable**

(nom, prénom, n° de SS, adresse, données de géolocalisation, identifiants en ligne...)



Je suis une base
de données personnelles

Qui est **concerné** ?

RGPD



RGPD s'applique quand :

- ❖ Une **organisation** traite des **données personnelles**
- ❖ Un **résident de l'UE** est directement visé par un traitement de données

- ✓ *Entreprises américaines (Google, Facebook, Amazon...), sites de e-commerce chinois, tout autre service qui cible des résidents de l'UE*
- ✓ *Organismes publics*
- ✓ *Associations*
- ✓ *Sous-traitants y compris s'ils se tiennent en dehors de l'Europe*



Qui est **concerné** ? - Collecte des **données**

RGPD

Cadre personnel
RGPD = *non applicable*

Sauf si le propriétaire du site web
(par ex) en tire des revenus
(ex : publicité, conseil, vente de données,
partenariats...)



Cadre professionnel
= RGPD *applicable*

Protection de la vie privée = **article 9** du code civil

1

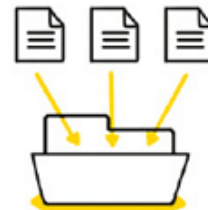


Sont **concernées** :

- ✓ les données **informatisées (1)**
- ✓ les données « **papier** » **(2)**

(ex : CV reçu par courrier et conservé dans un classeur...)

2

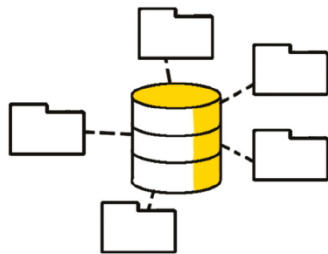


dès l'instant où il y a des **données personnelles collectées**

Impact sur l'entreprise

RGPD

Une multinationale qui traite des **données commerciales** aura des **obligations plus importantes** sur la **gestion, le suivi** et **l'organisation** des données



Une startup de santé qui a peu de clients mais qui traite des **données personnelles sensibles** aura des **obligations plus importantes** pour la **sécurisation** des données



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

RGPD



- ✓ Origines **raciales** ou **ethniques**
- ✓ Opinions **politiques** ou **philosophiques, religieuses**
- ✓ Appartenance **syndicale**
- ✓ Données **biométriques/génétiques/de santé**
- ✓ Orientation **sexuelle**
- ✓ Infractions et **condamnations pénales**

Le DPO (Data Protection Officer)

RGPD

DPO = Data Protection Officer = Délégué à la Protection des Données (DPD)

➤ Rôle :

« Garant de la **conformité** en matière de **protection des données** au sein d'une organisation »



➤ Missions :



- ✓ Informer l'organisation et ses employés
- ✓ Veiller au respect du **RGPD**
- ✓ Conseiller sur la réalisation de l'étude d'impact
- ✓ Etre le **point de contact** de la **CNIL**

- Il est **obligatoire** pour :
- ✓ Les **organismes publics**
 - ✓ Les **organisations** dont les activités nécessitent la **surveillance** à grande échelle **des personnes**
(assurances, banque, tracking publicitaire)
 - ✓ Les **organisations** traitant des **données sensibles**
(hôpital, assurances, sites de rencontre...)

*Pour la plupart des TPE, un DPO n'est **pas** nécessaire*

*Il est possible de faire appel à un **DPO externe**
partagé entre **plusieurs entreprises** :*





L'accountability

RGPD

C'est l'obligation de **rendre compte**

- ❖ L'entreprise n'est **pas soumise** à des **déclarations récurrentes**
- ❖ Elle doit **simplement** tout mettre en œuvre pour se **conformer à la norme**

(rédaction des procédures écrites, registre des traitements, contrôle des contrats de sous-traitance...)





Sous-traitants

RGPD

- Les **sous-traitants** ont une **responsabilité propre** et sont tenus de **respecter des obligations spécifiques** et notamment une **obligation de conseil** auprès du **responsable de traitement** (*donc leurs clients*) et **d'aider à respecter** le règlement et d'**assurer la sécurité des données** qui leur sont confiées.
- L'entreprise n'est donc **plus la seule responsable**
- Le sous-traitant et l'entreprise peuvent être **sanctionnées**

Responsable
de traitement & Sous-traitant



Tous deux sont concernés
par le RGPD

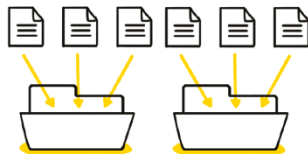
Exemple pratique

RGPD

Ex : une **entreprise** souhaite **refaire son site internet** et **collecter des données**

❖ Obligations :

- ✓ Préciser l'auteur de la **collecte**
- ✓ La **durée** de conservation
- ✓ La **finalité** des **données collectées**
- ✓ Les **informations** sur **leurs droits**
- ✓ **Faire apparaître** ces obligations comme **mentions sur le site**



❖ Les principaux droits données aux personnes concernées :

- ✓ Droit de **consultation/** accès aux données
- ✓ Droit d'**information**
- ✓ Droit de **modification**
- ✓ Droit à **l'oubli**



Respectez les droits
des personnes



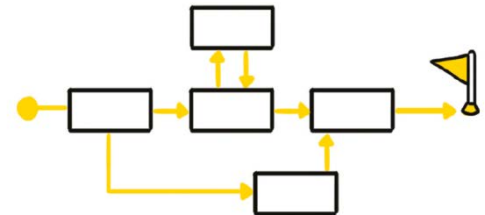
Délai de conservation vs Droit à l'oubli

RGPD

Lorsqu'il existe une **obligation légale** de **conservation des données** (ex : *bulletin de salaire*), les données sont **conservées** dans des **archives consultables** uniquement par les personnes qui en ont une **réelle utilité**.



Tout cela doit **être prévu** et **documenté** au travers du **registre des traitements** et des **procédures internes** à l'entreprise

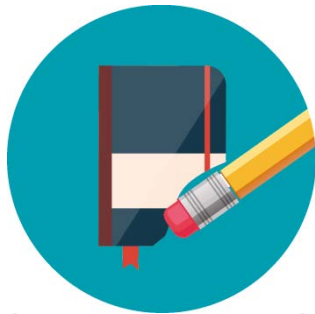




Droit à l'oubli (suite)

RGPD

Les **données collectées** doivent être **supprimées**
une fois que la **finalité a été atteinte**



*Le **délai de conservation** est à **mentionner**
dans le **registre des traitements***



Exemple pratique (suite)

RGPD

Comme l'entreprise traite des **données personnelles**
(comme le fichier des clients, le fichier RH pour ses salariés)
elle devra tenir un **registre de traitement des données**



Constituez un registre
de vos traitements de données

Réponse aux droits des **personnes concernées**

RGPD

En cas de **demande d'informations** sur les **données personnelles** détenues par l'entreprise, le **responsable des traitements** dispose d'un **délai d'un mois** pour y répondre.

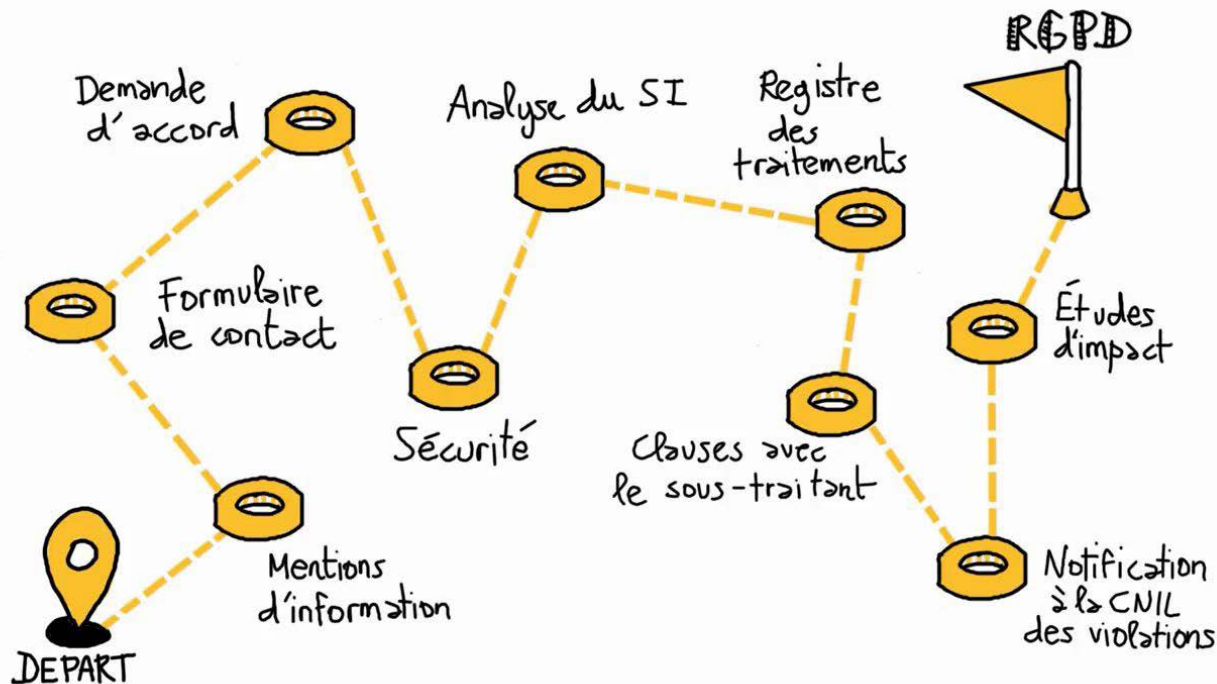
❖ **Dérogation possible** dans **2 cas précis** :

- ✓ Trop de **demandes simultanées**
- ✓ **Demande complexe** à traiter

« L'entreprise doit se justifier pour obtenir cette dérogation »

Démarche de mise en conformité

RGPD



Sanctions

RGPD

En cas de **non-conformité** à la suite d'un **contrôle** par la **CNIL**, l'entreprise encourt :

➤ 4 % du **CA annuel mondial**

ou

➤ 20 millions d'euros **d'amende**

*(le critère retenu sera le **montant le plus important**)*



Le **RGPD** n'est pas une **préconisation** de solutions techniques



C'est un **cadre** qui va définir ce qui est attendu en terme de **protection des données personnelles** pour les **résidents de l'UE**

Conclusion

RGPD

La mise en œuvre de la **RGPD** est un **travail continu** qui
implique tous les acteurs de l'entreprise
(et non pas seulement le service informatique)

❖ Cela induit :

- L'implication de la **gouvernance de l'entreprise**
- La sensibilisation des **utilisateurs**
- Des **mesures organisationnelles**
(ex : procédure en cas de violation des données)
- **Gestion des accès à l'entreprise**
- **Sécurisation des postes de travail**

Passage à l'action !

RGPD

PASSER À L'ACTION

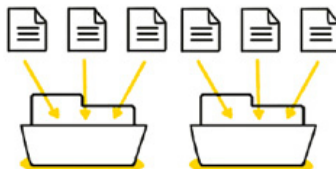
en 4 étapes

1



Constituez un registre
de vos traitements de données

2



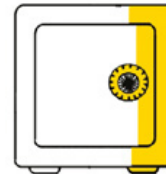
Faites le tri
dans vos données

3



Respectez les droits
des personnes

4



Sécurisez
vos données

Vous n'êtes pas seul !

RGPD



Nos services



“Occupez-vous de votre business, nous nous chargeons du reste !”



DOMICILIATION



WEB



COMMUNICATION



GESTION
ADMINISTRATIVE

EXTERNALISE

✉ hello@externalise.fr

🌐 externalise.fr



PARTENAIRE DE  STECO



- **RGPD :**

- DPO mutualisé
- Accompagnement sur la mise en conformité
- Information des salariés
- Suivi de projets pour veiller au respect du RGPD

Nos services



Pack RGPD Basic

- Diagnostic de l'entreprise (par téléphone)
- Mise à disposition de modèles de documents à compléter

Tarif : 399 € HT



Pack DPO mutualisé

- + Pack RGPD Premium
- + Compte-rendu annuel sur les activités des traitements
- + Analyse d'impact lorsqu'un traitement l'exige
- + Contact avec la CNIL en cas d'incident ou demande d'information

Tarif : à partir de 249,90 €/mois - engagement 12 mois



Pack RGPD Premium

- Diagnostic de l'entreprise
- Aide à la constitution du registre des traitements (inclut 10 traitements)
- Conseils pour l'organisation des données
- Mise en place de procédures pour veiller aux droits des personnes concernées
- Information des salariés (inclut 1 session de 2h) (n'inclut pas l'analyse d'impacts)

Tarif : à partir de 899 € HT (selon diagnostic)



Pack RGPD support en ligne

- Réponses à vos questions
- Intervention éventuelle d'un avocat

Tarif : 80 €/h

EXTERNALISE

✉ hello@externalise.fr

🌐 externalise.fr



PARTENAIRE DE 

Un brun d'humour !

RGPD



