



# PROTÉGER LES DONNÉES PERSONNELLES

---

## GUIDE ENTREPRISES 2018

TRANSFORMER LE RGPD  
EN OPPORTUNITÉ POUR  
SON ORGANISATION

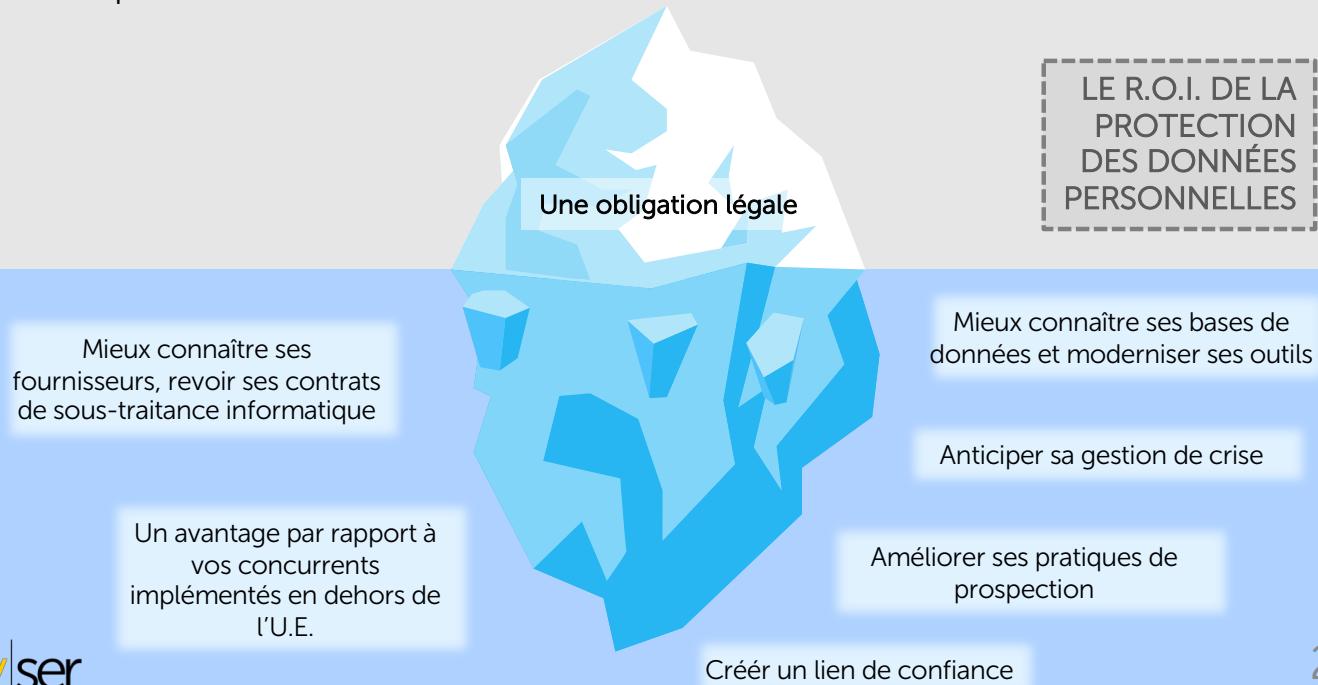
# POURQUOI PROTÉGER LES DONNÉES PERSONNELLES ?

Chaque entreprise est différente, et chaque entreprise collecte différents types de données. Néanmoins, presque toutes les entreprises sont amenées, au cours de leur activité, à collecter des données à caractère personnel. Pourquoi se préoccuper de les protéger ?

**D'abord, parce que c'est une obligation légale**, et que le RGPD a renforcé les contraintes de protection des données. Selon la CNIL, toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement, est une donnée personnelle. Par exemple, un nom, une photo ; ou, moins intuitivement, une adresse IP, la durée de connexion, les habitudes d'achat, ou encore les centres d'intérêts de l'utilisateur. Si vous collectez, traitez ou stockez les données de vos clients, de vos utilisateurs ou de vos collaborateurs, alors vous devez respecter le RGPD et protéger la donnée.

**De plus, parce que c'est un moyen de créer un lien de confiance**. Dans un contexte où les abus, les excès, les négligences et les fraudes sont nombreux, protéger la donnée, recueillir le consentement et informer les personnes sont des clés pour pérenniser son activité sur des bases saines à long terme. Les données sont un sujet de gouvernance générale, un *asset* comme un autre qui, bien géré, peut se révéler être un véritable atout business.

**Enfin, parce que c'est une remise en question qui peut générer des gains de productivité**. C'est un exercice d'introspection forcément utile, qui permet d'identifier de potentiels blocages, tels qu'un surplus de fichiers inutilement coûteux, ou bien des pratiques de prospection au forceps. C'est également l'occasion de passer à des infrastructures informatiques plus claires et plus souples.



# COMMENT PRÉPARER SON ORGANISATION ?



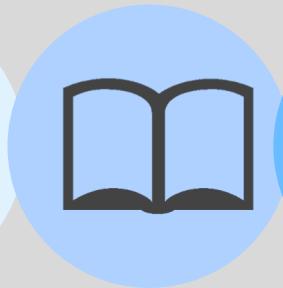
Les éléments importants à prendre en compte lors de la mise en place d'une protection des données personnelles sont, entre autres :

- Désigner et former un « pilote » de la protection des données ;
- Comprendre, au sein de chaque service (RH, commercial/marketing, juridique, informatique), quel type de donnée est collectée et/ou traité ;
- S'assurer que chaque traitement de données repose sur une base légale et un consentement des personnes concernées ;
- N'utiliser que des outils, produits, applications ou services qui, dès leur conception, intègrent de façon effective les principes relatifs à la protection des données ;
- Protéger la donnée *par défaut*, en limitant la collecte, les accès des employés et la durée de stockage à ce qui est strictement nécessaire au service ou à la finalité du traitement ;
- S'assurer de la conformité de ses sous-traitants, au sens de l'article 28 du RGPD ;
- Anticiper les violations de données : évaluer les risques et prévoir des canaux de notifications aux autorités et aux personnes concernées ;
- Documenter et communiquer sur la protection des données : rédiger une politique de confidentialité, revoir les mentions obligatoires relatives à la question. De manière général, il s'agit d'informer les personnes de l'état et du devenir de leurs données, ainsi que des finalités pour lesquelles elles sont traitées et collectées.

Nommer un DPO ou un pilote



Prioriser les actions à mener



Documenter et informer



Anticiper les violations de données



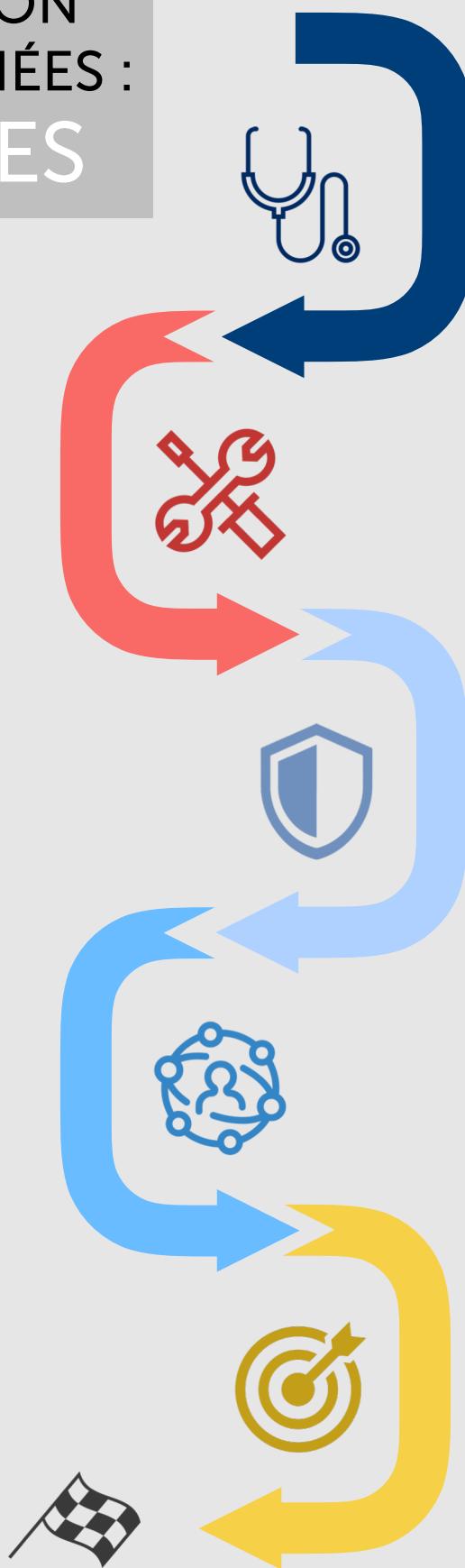
# DIAGNOSTIC YSER PROTECTION DES DONNÉES : 5 ÉTAPES

## Accompagnement dans la protection des données

Sur la base de notre plan d'action, nous vous aidons à mettre en place la protection des données personnelles au sein de votre organisation.

## En faire une opportunité

La transparence aux utilisateurs sur l'usage des données est une obligation de la RGPD. Mais c'est avant tout une opportunité pour votre entreprise, en ce qu'elle permet à vos interlocuteurs de comprendre comment vous utilisez les données personnelles.



## Diagnostic & Plan d'action

Évaluation de la gestion des données personnelles. Nous venons à votre rencontre afin d'obtenir une vision claire et précise des risques existants ou potentiels.

## Gestion des risques

Nous identifions les traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées et vous aidons à vous prévenir de ces dangers.

## Opérations et suivi dans le temps

Remise du rapport de diagnostic, de recommandation et de consolidation

# QUELQUES QUESTIONS QUE VOUS DEVEZ VOUS POSER

- Devez-vous nommer un DPO ? Si oui, l'avez-vous formé ? À défaut, avez-vous nommé un Pilote de la conformité RGPD ?
- Quelles-sont vos pratiques de démarchage ? Comment obtenez-vous le consentement des personnes et des entreprises que vous contactez ? Que faites-vous de leurs données ? Savez-vous quand obtenir ce consentement, par l'opt-in ou l'opt-out ?
- Qui a accès aux données du personnel de l'entreprise et des candidats au recrutement ? Disposez-vous d'un système de vidéo-surveillance ou d'une badgeuse ? Avez-vous pensé à informer vos salariés du traitement de leurs données et avez-vous obtenu leur consentement à ces traitements ?
- Comment stockez-vous les données personnelles ? Qui peut y avoir accès ? Combien de temps les conservez-vous ? Les transmettez-vous à des tiers ? Pour chacun de ces points, le RGPD définit des règles strictes.
- Transmettez-vous les données personnelles à des sous-traitants ? Respectent-ils les principes de protection de ces données ?
- Déposez-vous des cookies sur vos sites web et applications ? Quand obtenez-vous le consentement des utilisateurs à la lecture ou au dépôt de ces cookies ? Vous êtes vous assuré que ces cookies n'utilisent pas les données qu'ils collectent à d'autres fins que celles consenties par vos usagers ? Avez vous rédigé une Politique des Cookies ?
- Avez-vous rédigé une Politique de confidentialité des données personnelles ? Comment informez-vous les personnes des données que vous collectez et des traitements que vous appliquez ? Comment les personnes concernées peuvent-elles exercer leurs droit d'accès, de rectification, de suppression, de portabilité ou d'opposition ?
- Ne collectez-vous que des données strictement nécessaires au fonctionnement de vos services ? Protégez-vous les données par défaut, dès la conception (« privacy by default and by design ») ?
- Disposez-vous d'une documentation interne relative à la protection des données ? Avez-vous sensibilisé vos collaborateurs à la protection des données personnelles ?
- Comment gardez-vous la sécurité des données que vous collectez, traitez et stockez ? Avez-vous prévu un canal de notification aux autorités en cas de violation des données personnelles ?

Notre mission : vous aider à créer un lien de confiance fort avec vos collaborateurs, clients et utilisateurs

Notre équipe d'intervenants est forte de ses connaissances des différents textes juridiques relatifs à la protection données personnelles, et notamment du Règlement Général sur la Protection des Données (RGPD).



Nicolas Esnis  
Business Developer



Pierre-Florian  
Dumez  
Juriste IT



Timothy Lengliné  
Developer



Etienne Jaunet  
Expert Sécurité

C'est pour avoir vu de près toutes les contraintes et rigidités pesant sur le traitement de données personnelles en entreprise que nous avons choisi de participer avec enthousiasme à l'aventure du « self-data ». Convaincus par ses bénéfices, par ce qu'il peut apporter aux entreprises autant qu'aux individus, nous avons créé yser en 2018 pour vous aider à en tirer le meilleur parti.

Ils nous ont fait confiance :



Nous sommes à votre disposition pour réaliser un diagnostic de l'état de la protection des données personnelles dans votre entreprise, sensibiliser vos employés sur ces sujets, ou organiser des formations au RGPD.

[contact@be-yser.com](mailto:contact@be-yser.com)

06 14 08 25 47

[www.be-yser.com](http://www.be-yser.com)