Le Livre Blanc

de l'agence rgpd

2022

Pourquoi le RGPD a-t-il été adopté ?

La protection de la vie privée est un **droit fondamental** reconnu par la Déclaration Universelle des Droits de l'Homme de 1948.

Ce droit inclut la **protection du domicile**, la **confidentialité des correspondances**, le **secret médical** mais également **la protection des données personnelles**. Toute personne doit pouvoir contrôler ses informations privées et savoir ce qui en est fait.

Le développement du numérique a entraîné **l'émergence de pratiques malveillantes** portant atteinte aux données personnelles des citoyens.

En réaction à ce constat, la Loi informatique et liberté a été promulguée en France en 1978.

Le sujet devenant de plus en plus préoccupant, **le Règlement Général sur la Protection des Données (RGPD)** a été adopté en 2016 au niveau européen.

Il harmonise le droit de l'ensemble des Etats membres pour permettre une **meilleure circulation des données** au sein de l'Union européenne (UE). Cette règlementation est **applicable depuis le 25 mai 2018.**

Êtes-vous concerné(e) ?

Le RGPD est applicable aux organismes **publics et privés** qui collectent et traitent des données personnelles. Il concerne **toutes les structures basées sur le territoire d'un Etat membre de l'UE** ou traitant des données personnelles de personnes physiques situées sur le territoire d'un Etat membre de l'UE.

Dans le but de **garder un contrôle**, le RGPD accorde également des **droits** aux personnes dont les données sont traitées, elles sont donc également concernées par le RGPD.

Qu’est qu’une donnée à caractère personnel ?
Qu’est ce qu’un traitement ?

Un **traitement** correspond à toute **opération** réalisée sur une ou plusieurs **données à caractère personnel**

Une donnée à caractère personnel est une information se rapportant à **une personne physique identifiée ou identifiable, directement ou indirectement**

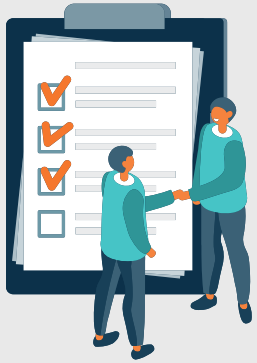
Quels sont les principaux acteurs du RGPD?

Le Responsable de Traitement (RT)

Le RT est l'acteur principal du traitement. Il détermine les finalités et les moyens du traitement.

Le RT doit veiller au respect du RGPD par les sous-traitants qu'il sollicite.

Le contrat de sous-traitance permet d'encadrer les obligations de chacun.



Le Sous-Traitant (ST)

Le ST traite les données à caractère personnel pour le compte du responsable de traitement.

Le RGPD s'appliquant à l'ensemble de la chaîne économique, si le ST fait appel à un prestataire, il doit veiller à ce que son ST respecte les obligations qu'il doit lui-même satisfaire.

Le Délégué à la protection des données (DPO)

Le DPO a pour mission de conseiller les acteurs du traitement, de contrôler le respect de la règlementation, de coopérer avec l'autorité de contrôle et d'être le point de contact des personnes concernées. Le DPO peut être interne à l'entreprise ou externalisé.

La personne concernée (PC)

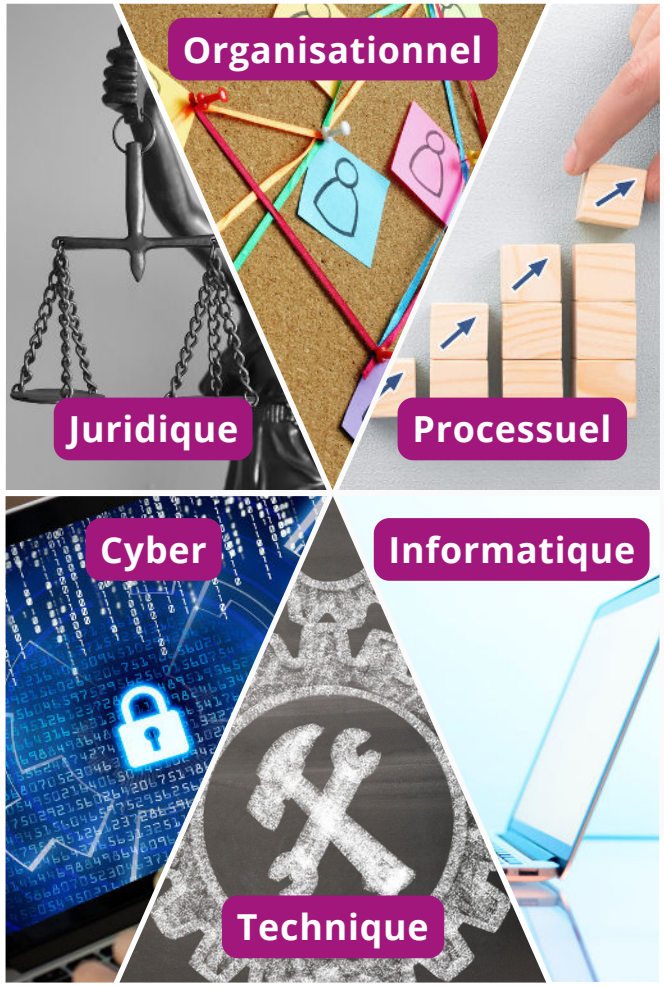
La PC est la personne dont les données personnelles sont traitées.

Elle dispose de droits :

- Sur ses données (droit d'accès, de rectification, d'oubli, de portabilité)
- Sur ses traitements (droit de limitation, d'opposition).

Comment puis-je assurer au mieux la mise en conformité de mon entité ?

Une mise en conformité porte sur plusieurs domaines bien distincts :



Le processus de mise en conformité se fait en plusieurs étapes :

Cependant, être en conformité à un instant “T” ne suffit pas. La conformité est une notion qui s’évalue dans la durée. Il est donc indispensable de développer des méthodes permettant une protection des données à caractère personnel de manière constante. La mise en conformité est une démarche active et en continu.

Principe de Licéité et Loyauté

Pour être licite, le traitement doit être fondé sur une des 6 bases légales. La loyauté implique le respect des engagements pris envers les personnes concernées à propos du traitement (Art 5 RGPD).

Principe de transparence

Les personnes concernées doivent être informées des conditions du traitement. Cette information doit être concise, transparente, compréhensible et accessible (Art 5-12-13-14 RGPD).

Principe de Finalité

Le traitement doit être effectué dans un objectif déterminé. Celui-ci doit être explicite, légitime et limité (Art 5 du RGPD)

Quelles sont les grands principes du RGPD ?

Le RGPD pose des grands principes qui guident le RT tout au long du traitement

Durée de conservation limitée

Les données ne doivent pas être conservées pour une durée excédant celle nécessaire à la réalisation de l'objectif justifiant le traitement. (Art 5 RGPD)

Principe de minimisation et d'exactitude

Doivent être traitées uniquement les données pertinentes au regard des finalités pour lesquelles elles sont traitées (ART 5 RGPD). Toutes les données inexactes doivent être effacées ou rectifiées (Art 5 RGPD)

Principe de Sécurité

Le RT et le ST doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques et aux besoins. (Art 5 RGPD)

Quels sont les risques en cas de non respect des dispositions ?

Impact sur les personnes concernées :

Tout incident de sécurité ayant un impact sur les données personnelles traitées représente un risque pour les droits et libertés des personnes concernées. Selon la gravité du risque, le responsable de traitement peut avoir l'obligation de le notifier à la CNIL dans les 72h.

Sanctions :

Le RGPD a renforcé les sanctions prévues. En cas de non-respect du RGPD, des amendes administratives peuvent être prononcées, pouvant atteindre les 20 Millions d'€ ou 4% du CA annuel. Des sanctions pénales peuvent également être prononcées, pouvant atteindre 5 ans d'emprisonnement et/ ou 300 000€ d'amende.

Exemple de manquements constatés par la CNIL :

Un géant de la navigation a écopé d'une amende de 50 Millions d'euros pour manque de transparence.

Une importante compagnie Aérienne a du débourser plus de 200 Millions d'euros suite aux négligences de l'entreprise ce qui a entrainé le vol de données personnelles de passagers.

Une entreprise allemande a été condamnée à payer 9,55 Millions d'euros pour ne pas avoir su protéger les données de ses clients dans le cadre de son service client téléphonique.

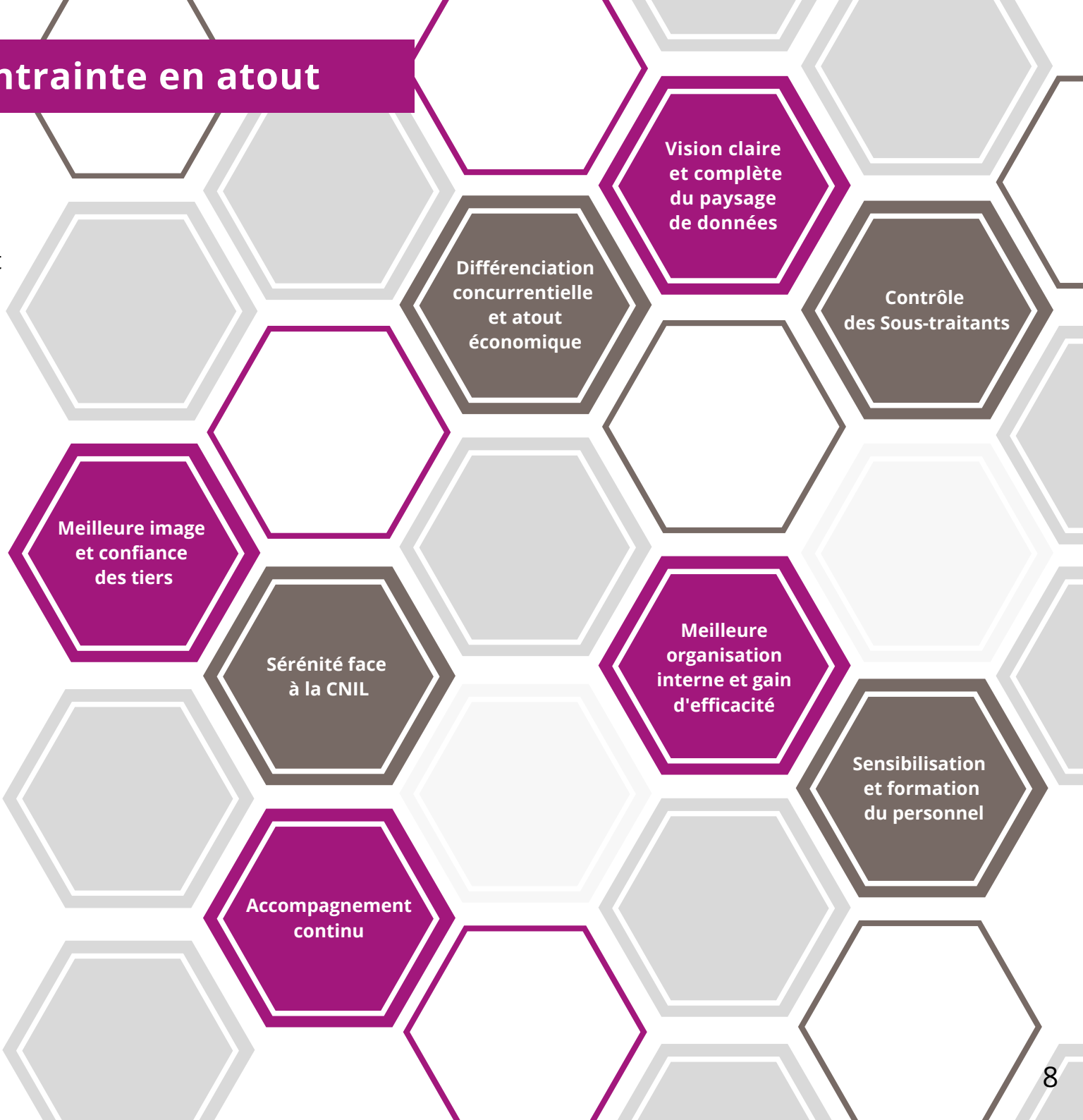
Transformez une contrainte en atout

Ce règlement est souvent perçu comme une contrainte pour les entités concernées. Pourtant, il peut constituer une **réelle valeur ajoutée.**

Être conforme au RGPD est un **gage de qualité**, et permet ainsi de **renforcer son image** et la **confiance** de vos clients et partenaires.

Il offre aussi aux entités concernées l'opportunité de réorganiser leurs activités pour avoir un réel encadrement des responsabilités, une meilleure gestion des données traitées, et ainsi gagner en efficacité.

Il est donc dans votre intérêt de vous assurer de votre conformité RGPD



Quizz de positionnement

Où en êtes-vous dans votre conformité RGPD ?

1 - Savez-vous ce qu'est un traitement de données à caractère personnel ?	a) ☐ Oui b) ☐ Non
2 - Savez-vous ce qu'est un registre des traitements ?	a) ☐ Oui b) ☐ Non
3 - Connaissez-vous les 8 informations de base à noter dans un registre de traitement ?	a) ☐ Oui b) ☐ Non
4 - Faites-vous attention pour chaque traitement de collecter les données strictement nécessaires, déterminez-vous toujours les modalités de leur conservation et destruction ?	a) ☐ Oui b) ☐ Non
5 - Déterminez-vous clairement, notamment par contrat, les responsabilités de chaque acteur (responsable de traitement, sous-traitant, ou coresponsable de traitement) et vérifiez-vous bien que leurs obligations sont remplies ?	a) ☐ Oui b) ☐ Non
6 - L'entrée de vos locaux est-elle verrouillée (code, badge) et encadrez-vous la venue des visiteurs?	a) ☐ Oui b) ☐ Non

7 - Avez-vous une politique d'accès aux données ?	a) ☐ Oui b) ☐ Non
8 - Avez-vous une charte informatique ?	a) ☐ Oui b) ☐ Non
9 - Êtes-vous capable de mettre en place le chiffrement, la pseudonymisation, l'anonymisation de données lorsque cela est nécessaire ?	a) ☐ Oui b) ☐ Non
10 - Sécurisez-vous l'informatique (antivirus, firewall, VPN...) ?	a) ☐ Oui b) ☐ Non
11 - Savez-vous à quoi correspond une violation de données ?	a) ☐ Oui b) ☐ Non
12 - Informez-vous suffisamment les personnes concernées chaque fois que vous traitez leurs données (nature des données traitées, le traitement effectué, l'identité du responsable de traitement, les modalités d'exercice de leurs droits...) ?	a) ☐ Oui b) ☐ Non
13 - Êtes-vous capable de permettre aux personnes concernées d'exercer leurs droits dans les délais requis ?	a) ☐ Oui b) ☐ Non

14 - Sur votre site internet, permettez-vous aux visiteurs de consentir ou non aux cookies, et de retirer leur consentement aussi facilement ?	a) ☐ Oui b) ☐ Non
15 - Transférez-vous des données hors UE ?	a) ☐ Oui b) ☐ Non
16 - Si oui, êtes-vous capable d'assurer la sécurité de ce transfert ?	a) ☐ Oui b) ☐ Non
17 - Avez-vous mis en place des mesures techniques et organisationnelles me permettant de maintenir la conformité de mon entité dans le temps et démontrer mon « accountability »	a) ☐ Oui b) ☐ Non
18 - Savez-vous ce qu'est un DPO (Délégué à la Protection des Données) ?	a) ☐ Oui b) ☐ Non
19 - Avez-vous pu déterminer su un DPO était obligatoire dans votre cas ?	a) ☐ Oui b) ☐ Non
20 - Si oui, avez-vous procédé à sa désignation ?	a) ☐ Oui b) ☐ Non

21 - Avez-vous mis en place un calendrier de sensibilisation / formation de votre personnel en matière de RGPD pour inculquer / maintenir les bonnes pratiques ?	a) ☐ Oui b) ☐ Non
22 - Un des membres de votre personnel vous informe que son poste a été piraté, et que certaines adresses email de vos clients ont été publiées sur internet. Que faites-vous ?	a) ☐ Je débranche immédiatement le poste et j'appelle le DSI pour l'informer de la situation, je documente la violation dans mon registre, et en fonction de mon évaluation du risque, je notifie à la CNIL ; b) ☐ Je jette le poste par la fenêtre, et l'employé avec (ni vu ni connu) c) ☐ Je débranche immédiatement le poste et j'appelle le DSI pour l'informer de la situation, je notifie à la CNIL, et je notifie à toutes les personnes concernées l'existence de cette violation et ses potentielles conséquences.

Solutions

Moins de 5 réponses a)	Entre 5 et 15 réponses a)	Entre 16 et 22 réponses a)
RGP… Quoi ? Le RGPD a encore beaucoup de secrets pour vous. Lui accorder de l'attention peut pourtant vous apporter bien plus que vous ne le pensez ! En effet, au-delà de la contrainte légale qu'il peut représenter, il vous apportera une optimisation de votre organisation et de l'utilisation de vos données. Sans parler de la sécurisation indispensable de votre système d'information. N'attendez plus et accordez à votre entité la valeur qu'elle mérite en contactant l'Agence RGPD, afin de bénéficier d'un accompagnement efficace et d'un outil intuitif pour assurer sereinement votre conformité RGPD.	Oui c'est bon je suis conforme… enfin je crois… on passe à autre chose ? Et bien pas tout à fait. Vous avez amorcé quelques actions, et c'est déjà une très bonne initiative, bravo ! Mais pourquoi s'arrêter en si bon chemin ? Contactez l'Agence RGPD pour maîtriser pleinement votre conformité RGPD et faire de cette vague notion quelque chose de concret et de réellement bénéfique pour votre entité, et ce dans la durée. Il vous reste encore du travail mais vous avez déjà manifesté votre volonté de mettre les bonnes actions en place, et nous pouvons vous aider à optimiser cette initiative pour renforcer votre conformité RGPD.	Je suis un pro du RGPD, j'ai tout mis en place, c'est bon je suis tranquille. Félicitations, vous avez pris beaucoup d'initiatives pour tenter d'appliquer correctement le RGPD. Mais comment être sur que vos actions sont suffisantes, ou correctement mises en places, ou encore bien appliquées par vos équipes ? L'Agence RGPD vous permet d'avoir une vision objective de votre organisation, et conforme aux exigences de la CNIL. De même, une conformité à un instant T ne suffit pas. Il est important de savoir la maintenir, et l'Agence RGPD est à vos côtés pour assurer ce maintien de votre conformité RGPD.

agence rgpd

contact@agencergpd.eu

https://www.agencergpd.eu/