RGPD

TOUT SAVOIR POUR VOS CAMPAGNES

AU SOMMAIRE
DE CE DOCUMENT

INTRODUCTION

Alors que cette nouvelle législation européenne paraît être un frein à vos stratégies marketing, elle a pourtant comme objectif d'offrir plus de contrôle et de transparence aux consommateurs.

Il est essentiel de l'aborder comme un moyen de créer une relation de confiance avec vos clients.

RGPD
Règlement Général sur la Protection des Données

GDPR
General Data Protection Regulation

OBJECTIF

Harmoniser la régulation des données personnelles sur l'ensemble du territoire européen.

POURQUOI CETTE LOI ?

- Législation vieillissante
- Augmentation du volume de collecte et de traitement des données personnelles
- Manque de contrôles et de sanctions concrètes

COMMENT ?

Trois années de négociations entre les trois grandes institutions européennes : Parlement européen, Conseil de l'UE et Commission européenne.

POUR QUAND ?

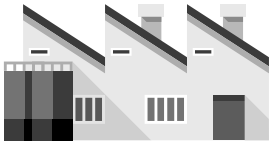
Le 25 mai 2018.
À cette date, vous devez être en mesure de prouver que vous avez entamé les démarches de mises en conformité.

POUR QUI ?

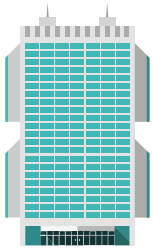
Tous les organismes qui opèrent des traitements de données personnelles au sein de l'Union européenne dans le cadre de leur activité professionnelle.

AMENDES

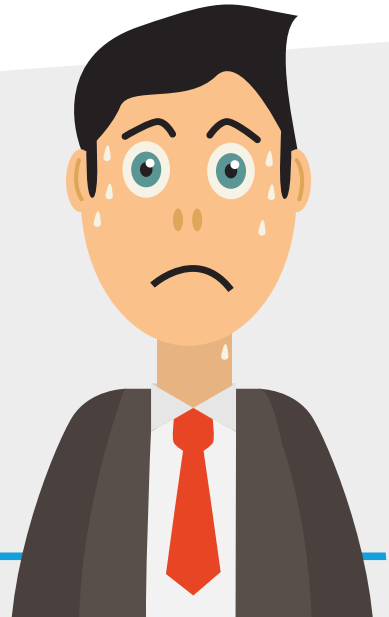
Concernant les infractions les plus graves, les sanctions sont extrêmement dissuasives :



20 millions d'euros
pour les PME et les organismes publics



4% du CA du groupe
pour les grandes entreprises



PAS DE PANIQUE !

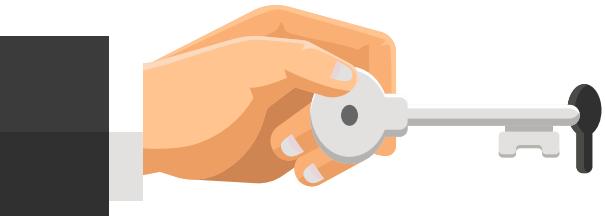
Avant d'atteindre ces montants considérables, la loi prévoit des rappels à l'ordre et des amendes plus modestes. Ceux-ci sont établis au regard des transgressions effectuées et de l'échelle de collaboration avec la CNIL.

DROITS DES PERSONNES CONCERNÉES

Cette nouvelle loi a pour objectif premier d'augmenter les droits des personnes concernées ayant partagé leurs données personnelles.

Vous trouverez donc ci-dessous la liste et les modalités d'application des différents droits.

1 DROIT D'ACCÈS



La personne concernée a le droit d'avoir accès aux données que vous avez collectées.

Elle peut vous demander notamment : les finalités, les catégories de données possédées, les personnes ou entités ayant accès à ses informations…

Plus d'informations

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article15

DROIT DE RECTIFICATION 2

Vos contacts peuvent modifier les données collectées inexactes et peuvent faire la demande de compléter les données incomplètes.

Plus d'informations

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article16

3 DROIT À LA PORTABILITÉ

Vos contacts peuvent exporter (ou vous en faire la demande) l'ensemble des données que vous avez récoltées les concernant.

Idée : Espace dédié sur votre site internet qui permettrait à vos clients de le faire en autonomie afin de vous éviter une perte de temps.

Plus d'informations

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article20

4 DROIT À L'OUBLI / DROIT D'EFFACEMENT

Vos contacts peuvent demander à tout moment et dans un délai court, l'effacement de toutes leurs données personnelles.

Dans certaines circonstances, vous êtes autorisés à refuser l'effacement des données personnelles. Toutefois, si la personne concernée en fait la demande, vous serez tenus de limiter les finalités du traitement.

Plus d'informations

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article17
https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article18

5 DROIT D'OPPOSITION

Les personnes concernées ont le droit de s'opposer au traitement de leurs données. Le responsable peut cependant refuser ce traitement s'il démontre des motifs légitimes et impérieux justifiant le traitement.

Plus d'informations

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article21

6 RETRAIT DU CONSENTEMENT

Vos contacts ont le droit de retirer à tout moment leur consentement. Vous devez leur mettre à disposition un moyen simple d'en faire la demande.

OBLIGATION DE NOTIFICATION 7

Vos contacts doivent être informés dans ces trois cas : rectification, effacement ou limitation.

Vous pouvez cependant échapper à cette obligation si vous prouvez que celle-ci est impossible ou demande un effort disproportionné.

Plus d'informations

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article19

8 QUELQUES PRÉCISIONS

1. Identité de la personne concernée

Vous avez le droit d'exiger des personnes concernées qu'elles fournissent une preuve d'identité.

2. Délai pour respecter les droits des personnes concernées

Vous devez fournir les éléments demandés dans un délai d'un mois.
Si vous avez un trop grand nombre de demandes et/ou que les demandes sont trop complexes, vous pouvez prolonger ce délai de 2 mois supplémentaires.

3. Frais relatifs aux demandes des personnes concernées

Dans le cas d'individus qui tentent d'exercer ces droits abusivement, vous êtes autorisés à facturer des frais raisonnables pour des "demandes répétitives", «demandes manifestement non fondées ou excessives» ou pour «copies supplémentaires».

Plus d'informations

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article12
https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article13
https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article14

POUR APPROFONDIR
LE SUJET

CARTOGRAPHIE DES DONNÉES

C'est un des éléments de la documentation demandée par la norme qui consiste à répondre à des questions simples qui encadrent le traitement des données personnelles au sein de votre organisme.

Vous trouverez ci-dessous les différents points concernés :

1 QUI... ?

1. Qui est le responsable du traitement des données personnelles dans votre société ?

Désignez un référent en charge d'encadrer le traitement des données, ou un « Data Protection Officer » (DPO) en fonction de votre situation :

	RÉFÉRENT	DPO
Traitement de données standards*	✔	✔
Traitement de données sensibles*	✖	✔
TPE / PME**	✔	✔
Autorités / Organismes publics**	✖	✔
Obligation de déclaration à la CNIL***	✖	✔

* https://www.cnil.fr/fr/definition/donnee-sensible
** https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees
*** https://www.cnil.fr/fr/designez-en-ligne-votre-delegue-la-protection-des-donnees-aupres-de-la-cnil

2. Quelles seront les personnes amenées à traiter des données personnelles au sein de votre organisation ?

Cela peut être des personnes désignées en fonction de leur activité, de leur position hiérarchique ou encore de leurs compétences.

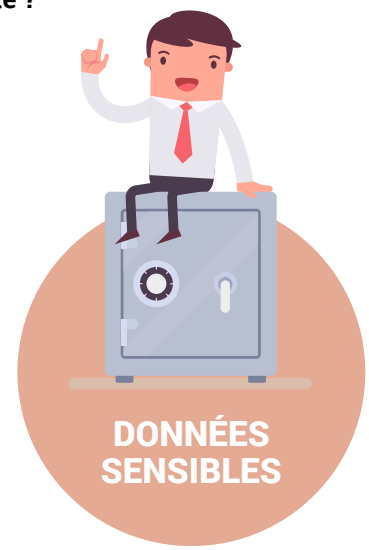
3. Qui sont les sous-traitants ayant accès aux données personnelles de vos clients ?

Voir la rubrique “sous-traitants”

2 QUOI... ?

Quelles catégories de données sont récoltées par votre société ?

Catégorisez vos typologies de données.



Qu’est-ce qu’une donnée sensible ?

Information concernant l’origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l’appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu’avec le consentement explicite des personnes.

Source : https://www.cnil.fr/fr/definition/donnee-sensible

POURQUOI... ? 3

Dans quel but récoltez-vous les données de vos clients ?

Déterminez les objectifs de votre collecte de données.

Exemple : gestion de la clientèle, enquête de satisfaction, opération de fidélisation

Attention, en fonction des finalités le temps de conservation varie.

Exemple : Lors d’un paiement en CB, la conservation des données bancaires ne peut durer que le temps du paiement.

3 OÙ... ?

Où sont hébergées vos données ? Où transitent vos données ?

Indiquez le lieu d'hébergement et listez les pays où transitent les données personnelles.

JUSQU'À QUAND... ? 4

Combien de temps devez-vous conserver les données récoltées ?

La durée de conservation varie en fonction de la nature des données et des finalités poursuivies lors de la collecte.

ARCHIVES COURANTES
Base active

ARCHIVES INTERMÉDIAIRES
(accès restreint, étape intermédiaire avant suppression)

ARCHIVES DÉFINITIVES
(données avec un intérêt historique, statistique justifiant la non-destruction)

Concrètement une donnée doit être conservée uniquement le temps de l'accomplissement de l'objectif initial.

Exemple : Données personnelles à finalité commerciale = maximum 3 ans.

Plus d'informations

https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

5 COMMENT... ?

Comment sont traitées les données une fois que vous les avez récoltées ?

Mettez en place des processus de sécurités afin de minimiser les risques, de limiter les accès pour éviter tout impact sur la vie privée des personnes concernées.

Exemple : sécurisation des postes de travail = verrouillage automatique des sessions / installation d'un pare-feu / Multiplier les sauvegardes

LA CNIL VOUS AIDE 6

COLLECTE
DES DONNÉES PERSONNELLES

Ce qui est amené à disparaître pour protéger les personnes concernées :

Case précochée

Récolte sauvage

Opt-in passif

L'élargissement des données personnelles

Des données qui étaient jusqu'à présent non considérées comme des données personnelles le sont aujourd'hui, comme les cookies ou les données de localisation.

1 FINALITÉ DE LA COLLECTE DES DONNÉES

1. Indiquez clairement vos objectifs de collecte

Comme nous l'avons vu dans la rubrique "Pourquoi" de la cartographie des données, il est important de déterminer les finalités, mais il est également primordial de les indiquer clairement aux personnes concernées.

Chaque case à cocher de vos formulaires devra donc préciser la finalité et le support utilisés pour cette communication.

2. La finalité doit être respectée

Si votre traitement des données personnelles ne correspond pas à l'usage que vous aviez indiqué au moment de la collecte, les personnes concernées seront en droit de demander l'oubli ou l'opposition de leurs données.

2 CADRE DE LA COLLECTE DU CONSENTEMENT DES PERSONNES

1. Les pratiques à mettre en place

Obligation d'obtenir une réponse claire, précise, et univoque des personnes quant à la collecte de leur consentement.

2. Limitez les données collectées

Il ne faut récolter que les données en lien direct avec la finalité.
Afin d'éviter toute erreur qui pourrait entraîner des demandes de droit à l'oubli, mieux vaut demander uniquement l'information principale.

Voici des exemples et contre-exemples de collecte de données :

- ✓ J'accepte de recevoir la newsletter mensuelle par EMAIL
- ✓ J'accepte de recevoir des SMS ciblés en fonction de mes données de navigation
- ✓ J'accepte de recevoir des offres ponctuelles par SMS (soldes, promotions…)
- ✓ J'accepte de recevoir le magazine trimestriel Champs à remplir : adresse postale, nom, prénom.
- ✓ J'accepte les CGV (pop up qui reprend les cas ci-dessus)

- ✗ J'accepte de recevoir chaque semaine la newsletter ainsi que des offres ciblées

  > Interdiction d'utiliser une case pour recueillir les consentements pour plusieurs finalités; et le canal n'est pas précisé

- ✗ Si vous ne souhaitez pas recevoir d'offres commerciales, cochez la case

  > Interdiction d'utiliser une case décochée comme acte de consentement

- ✗ J'accepte de recevoir le magazine trimestriel / champ à remplir : email, mobile, adresse postale, nom, prénom

  > Interdiction de récolter des informations sans lien avec la finalité

- ✗ J'accepte les CGV et donne mon accord pour le traitement de mes données personnelles

  > Interdiction de mélanger les CGV et un traitement des données non détaillées

3. Créez de nouvelles mentions légales

Dans vos campagnes, redirigez vos clients ou prospects vers des mentions légales spéciales "Traitement des données" où vous démontrez que la confidentialité des données est au coeur de vos préoccupations.

1. Présentez la personne en charge du traitement des données dans votre structure et indiquez comment la contacter

2. Informez vos clients de leur droit de retirer leur consentement en proposant une marche à suivre simple et rapide.

4. N'oubliez pas la désinscription

Au delà de tous les changements apportés par la norme, n'oubliez pas de continuer à appliquer les bonnes pratiques. Vous êtes toujours tenus d'offrir à vos destinataires la possibilité de se désabonner de vos campagnes.

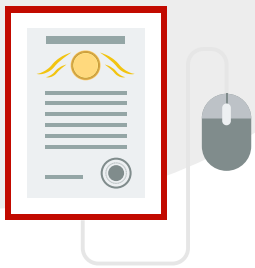
Ainsi, pensez à utiliser les listes d'exclusion et à intégrer les moyens de désinscription présents sur notre outil.

Plus d'informations

https://www.cnil.fr/fr/comprendre-vos-obligations/les-principes-cles

SOUS-TRAITANCE

Lorsque vos données sont amenées à transiter hors de votre organisme, vous en restez responsable. Il est donc primordial pour vous d'appliquer un processus complet afin de garantir à vos clients, des sous-traitants "conformes".



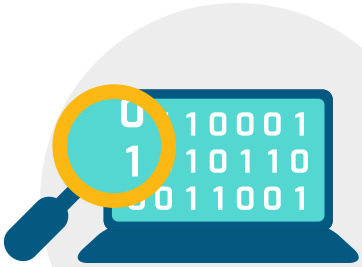
Ne faire appel qu'à des sous-traitants présentant des garanties

Vous devez exiger des prestataires concernés un document détaillant leur politique de traitement des données personnelles, appelé "Registre des traitements". Cela vous permettra de vérifier les connaissances et l'implication du prestataire sur ce sujet.

Mettre en place des mesures de sécurité

En collaboration avec vos sous-traitants il vous faudra appliquer certaines mesures :

- Chiffrement des données selon leur sensibilité
- Chiffrement des transmissions de données (HTTPS, VPN…)
- Garanties en matière de protection du réseau, traçabilité, authentification



Modifier vos contrats

Il est préférable de formaliser les engagements du prestataire dans les contrats afin de pouvoir prouver que vous avez recours à des prestataires conforment.

- Définir clairement l'objet, la finalité du traitement et les obligations
- Inscrivez des contraintes minimales en matière d'authentification
- Définissez les conditions de restitution/ destruction des données en fin de contrat
- Déterminez les règles de gestion et de notification en cas d'incident avec les données personnelles

Nous sommes en conformité avec les exigences de la RGPD.

Notre “Registre des traitements” est accessible à tout moment sur notre site.

Plus d’informations

https://www.cnil.fr/fr/securite-gerer-la-sous-traitance

EXEMPLE DE CLAUSES À METTRE EN PLACE AVEC VOS SOUS-TRAITANTS

https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses

SÉCURISATION

Informer les collaborateurs des obligations et attentes de la RGPD

Protéger les locaux

- Alarmes
- Détecteurs de fumée
- Distinguez des zones à risque de vos locaux (mettre en place un listing des personnes autorisées en fonction des zones)
- Listez les entrées/sorties des salles hautement sécurisées

Sécuriser les postes de travail

- Verrouillage de session avec mot de passe robuste
- Pare-feu
- Antivirus (mis à jour régulièrement)

Protéger les réseaux informatiques

- Gérer les réseaux WIFI avec un chiffrement (WPA2 ou WPA2-PSK)
- Séparer les réseaux ouverts aux invités du réseau interne
- Limiter les flux réseau en filtrant flux entrants/sortants

Sécuriser les serveurs

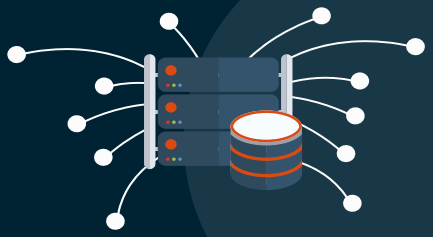
- Mettre en place le protocole TLS ou un autre protocole permettant de chiffrer l'authentification

Processus de sauvegarde et continuité d'activité

- Sauvegardes fréquentes et si possible sur un site extérieur
- Protéger les sauvegardes (chiffrement)
- Instaurer un plan de reprise et de continuité d'activité informatique
- Prévoir une redondance des matériels, notamment de stockage

Encadrer la maintenance et la destruction des données

- Enregistrer les interventions dans une main courante (si la maintenance est effectuée par un organisme externe, se référer à notre rubrique sous-traitants)
- Instaurer un processus de suppression sécurisé des données (par exemple, suppression des données contenues sur un ordinateur avant de l'envoyer en réparation)



Sécuriser les échanges externes

- Chiffrer les données
- Utiliser un protocole garantissant la sécurité (HTTPS, SFTP…)
- Exemple : si vous envoyez des données par email, chiffrez-les, et envoyez le mot de passe via un autre canal (SMS…).

Plus d'informations

https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

CERTIFICATION

Les certifications seront délivrées par des organismes agréés par la CNIL ou accrédités par le COFRAC (organisme national d'accréditation).

Soyez vigilant sur les "propositions" d'accréditations.

Comme pour toutes les nouveautés, elles sont accompagnées d'un "effet de mode", qui peut potentiellement amener des entreprises peu scrupuleuses à proposer des certifications sans valeurs.

Faites appel à des organismes sérieux et reconnus !

Plus d'informations

https://www.cnil.fr/fr/transition-vers-le-rgpd-des-labels-la-certification

CONCLUSION

Une réforme à deux vitesses

Cette nouvelle réglementation a été pensée initialement pour protéger les utilisateurs des géants comme FaceBook ou Google. Le niveau d'exigence sera évidemment adapté à chaque typologie d'entreprise.

Il vous faudra être pragmatique sur la mise en place des différents processus, et procéder par étape en fonction des points sur lesquels vous êtes déjà plus ou moins avancé.

Un processus sur le long terme

La date butoir du 25 mai 2018 n'a pas pour finalité de vous voir 100% conforme.

Votre objectif doit être de pouvoir prouver que vous avez connaissance des méthodes à mettre en place, que vous avez pris la norme au sérieux, et que vous avez démarré votre mise en conformité.

FEUILLE DE ROUTE

Afin de vous aider à vous évaluer, nous vous proposons une feuille de route qui vous permettra de juger votre mise en conformité.

ETAPE 1

DÉSIGNER UN PILOTE

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne.

ETAPE 2

CARTOGRAPHIER

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles.

ETAPE 3

PRIORISER

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir.

ETAPE 4

GÉRER LES RISQUES

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).

ETAPE 5

ORGANISER

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment.

ETAPE 6

DOCUMENTER

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire.

Pour finir, bien que complète, cette documentation sur le nouveau règlement européen du traitement des données personnelles ne fait pas office de référentiel officiel.

Il peut donc être utile de solliciter un conseil extérieur pour valider vos bonnes pratiques, par exemple un bureau d'avocats spécialisés.