LE RGPD PRÊT ? PARTEZ !

PAR DATAGALAXY

LA PREMIÈRE PLATEFORME AGILE DE CARTOGRAPHIE DES DONNÉES

SOMMAIRE

Introduction 4
De nouveaux droits pour le citoyen 5
Le consentement explicite 7
Privacy by design 9
Les comptes à privilèges 11
Gérer la sous-traitance 13
Sécurisation des données 15
Data Protection Officer 17
Droit à la portabilité des données 19
Le droit à l'information 21
Le registre des traitements 23
Le droit à l'effacement 25
L'analyse d'impact 27
Le droit d'accès 29
Le droit d'opposition 31
Le consentement des enfants 33
Droit de rectification 35
Mise en conformité 37

Introduction

Après quatre années d'échanges et d'allers-retours entre les 28 États Membres de l'Union Européenne, le **Règlement Général sur la Protection des Données** (RGPD) a été adopté !

Il entre en vigueur ce **25 Mai 2018** et sera immédiatement mis en application.

Il vient donc naturellement remplacer la loi adoptée en 1995 sur la protection des données personnelles. De ce fait, le RGPD permettra d'harmoniser le cadre juridique au sein de l'UE. Lors de son adoption, le règlement va stopper les lois nationales en vigueur dans chaque pays membre de l'UE se basant sur la **protection des données**. Voici un texte doté d'une grande envergure qui va donc impacter toute entreprise effectuant de la collecte de données, du marketing... L'emailing va-t-il changer, évoluer dans les stratégies marketing digitales ?

1 De nouveaux droits pour le citoyen

Le règlement général sur la protection des données est aujourd'hui une réalité, il est donc nécessaire de se mettre en conformité. Chaque organisation collectant des données personnelles doit être en conformité avec le RGPD, sous peine de se voir infliger une lourde amende de 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires mondial.

L'objectif affiché du règlement est d'uniformiser la protection des données personnelles au sein de l'Union Européenne. La situation actuelle n'est pas des plus simples avec une accumulation de lois disparates et incompatibles qui ne permettaient pas de protéger correctement les citoyens européens. Enfin, il devenait urgent de redonner confiance aux citoyens dans les différents acteurs qui traitent leurs données personnelles.

- Seuls 15% d'entre eux ont le sentiment de contrôler les données qu'ils fournissent en ligne.
- Pour 57 % des Européens (69% des Français) la divulgation d'informations à caractère personnel pose un réel problème
- 69 % des Européens (72% des Français) sont préoccupés par l'idée que des entreprises puissent utiliser des informations à des fins autres que celle pour laquelle elles ont été collectées.

Le RGPD est bel et bien là, il faut donc, si ce n'est pas le cas, se mettre en conformité pour éviter des amendes mais pas seulement. Ces nouveaux droits pour les citoyens vont permettre de redonner de la confiance dans les services proposés. Enfin, ce nouveau règlement change les règles, il faut maintenant proposer un service ou un produit qui apporte une valeur suffisante par rapport aux données demandées pour utiliser ce service ou acheter ce produit.

? Pour en savoir plus

CNIL : RGPD, par où commencer
Article : Antisèche RGPD 1 : Le RGPD expliqué simplement

LE RGPD EXPLIQUÉ SIMPLEMENT

Le règlement général sur la protection des données fait beaucoup parler de lui alors que son échéance de mise en application se rapproche. En effet, le 28 mai 2018, chaque entreprise collectant des données personnelles devra avoir commencé sa mise en conformité avec ce règlement sous peine de se voir infliger une amende à hauteur de 20 millions d'euros et 4% du chiffre d'affaires mondial .

Enjeu

Le règlement **vise à unifier la protection des données au sein de l'UE**. En effet, une multitude de lois disparate et incompatibles régissent actuellement la protection des données dans les 28 pays de l'UE. En second lieu, RGPD modernise les principes contenus dans la directive de 1995 sur la protection des données.
Enfin, l'objectif est de renforcer la **confiance des citoyens** et entreprises dans le **marché unique du numérique**.

Avec la RGPD l'Europe répond à une vraie préoccupation du citoyen :

15% des Européens ont le sentiment de contrôler les données qu'ils fournissent en ligne

57% des Européens pensent que la divulgation d'informations à caractère personnel pose un problème

69% des Européens sont préoccupés par les usages que les entreprises font de leurs données

Nouveaux droits pour le citoyen

Conçu pour redonner confiance au citoyen, le RGPD lui apporte ces nouveaux droits :

• Droit à la portabilité (exportation pour la personne de ses données personnelles dans un format structuré)

• Droit à la limitation du traitement

• Droit à l'accès et à l'effacement de données (renforcement du droit à l'oubli)

• Droit à la réparation des dommages matériels et moraux

Des responsabilités accrues pour l'entreprise

Face aux données personnelles, RGPD renforce la réglementation existante et introduit de nouveaux concepts.

• La responsabilité de l'entreprise vis-à-vis des données personnelles (charge de garantir et démontrer la conformité, PIA(1), registre des traitements, nomination d'un DPO(2))

• Le privacy by design. Autrement dit, chaque nouveau processus de l'entreprise devra prendre en compte un éventuel impact sur les données personnelles dès la conception.

(1) Privacy Impact Assessment (2) Data Protection Officer

POUR ALLER PLUS LOIN → Le site européen sur la protection des données

2

Le consentement explicite

La demande explicite du consentement est au coeur du nouveau règlement européen pour la protection des données. Le RGPD met la confiance au centre des relations entre les citoyens européens et les organisations, pour plus de sécurité, de contrôle sur les données personnelles.

La nouvelle réglementation, avec le “consentement explicite”, veut apaiser les relations entre les entreprises et leurs clients. Le citoyen européen, avec ces nouveaux droits, va demander plus de valeur ajoutée aux entreprises pour leur permettre d’utiliser ses données personnelles.

Consentement explicite ?

Dans tous les cas, dès que vous demandez des informations personnelles, le consentement explicite de la personne est obligatoire.

Pour en savoir plus

CNIL : Consentement
Article : Antisèche RGPD 2 : Êtes-vous certain d’avoir demandé la permission ?

ÊTES-VOUS CERTAIN D'AVOIR DEMANDÉ LA PERMISSION ?

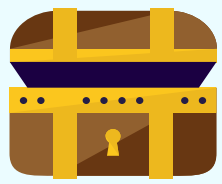
> “ La confiance est au cœur du nouveau règlement européen pour la protection des données ”

Enjeu

Comme dans une relation humaine, obtenir des informations d'une personne exige de sa part à la fois son approbation et, pour ce faire, une connaissance des finalités auxquelles ces données sont destinées. Ces deux notions recouvrent le « consentement explicite » du RGPD/GDPR.

Le consentement peut être retiré à tout moment

La personne doit comprendre à quoi servent ses données



Toute information liée au consentement doit être conservée

En pratique

Comment obtenir le consentement explicite ?

“Dès que vous demandez des informations personnelles, le consentement explicite est obligatoire. Le consentement doit obligatoirement intervenir avant l'activité de traitement.“

Informer et recueillir le consentement

- Site internet (cookie, formulaire)
- Système d'information, digitalisation (traitement des données)
- Print (droit à l'image, contrat de travail)

Stocker les consentements

- Tenir un registre des consentements

POUR ALLER PLUS LOIN

[Lien vers le modèle de mentions par la CNIL]
[Information de l'ICO sur l'obtention du consentement explicite]

3

Privacy by Design

Avec le “Privacy by Design”, les entreprises peuvent penser sécurité des données en amont de leur projet. Cela permet une mise en conformité avec le RGPD dès le départ pour ne pas avoir à faire des modifications par la suite. Cette approche proactive permet de mettre la protection des données

Pour s’inscrire dans la démarche “Privacy by Design”, il faut suivre quelques principes :

- Respecter la vie privée de vos clients, utilisateurs, collaborateurs en privilégiant leurs intérêts particuliers
- Sensibiliser et développer la culture de la protection de la vie privée
- Avoir une approche proactive en intégrant la protection des données dans la conception des solutions et des services
- Assurer la sécurité de bout en bout des données durant le traitement et la conservation
- Rester transparent sur les usages des données.

Avec le Privacy by Design, l’opt-in se généralise : un client ne doit pas recevoir d’offres de partenaires de l’entreprise s’il n’a pas donné son consentement explicite pour cet usage !

Pour en savoir plus

CNIL : Privacy by Design
Article : Antisèche RGPD 3 : Votre vie privée n’est pas négociable !

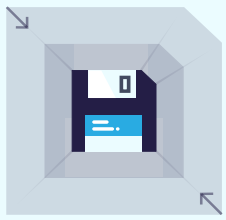
VOTRE VIE PRIVÉE N'EST PAS NÉGOCIABLE

> “ Grâce au “Privacy by Design”, vous respectez dès le départ la vie privée de vos utilisateurs ”

Enjeu

Le Privacy by Design consiste à prendre en compte la protection des données en amont d'un projet. Grâce à ce principe, vous limitez les risques dès la conception de votre application, pour être directement conforme au RGPD *(art.25, alinéa 2)*.

Les données personnelles sont protégées par défaut



Le nombre d'informations collectées est minimisé

Le chiffrement est indispensable

En pratique

Comment protéger au mieux les données personnelles des utilisateurs ?

Avec une démarche Privacy by Design, le respect de la vie privée est au coeur des préoccupations. Il donc normal que cela impacte le développement du projet, notamment lors de la collecte des données.

Se poser les bonnes questions

- Ces données sont-elles nécessaires au fonctionnement de l'application ?
- Pourquoi demander un nom/prénom quand un pseudonyme suffit ?
- L'accés à ces données est-il indispensable pour l'ensemble des utilisateurs de l'application

Penser protection dès la conception

- Généralisation de l'opt-in
- La protection des données crée des opportunités (sans en supprimer)
- Chiffrage des données personnelles

POUR ALLER PLUS LOIN → [Protection de la vie privée dès la conception]

4 Les comptes à privilèges

Les données personnelles sont des données dites sensibles. Ces dernières ne doivent pas être manipulées ou vues par une personne qui n'aurait pas les droits appropriés. L'accès à ces données, comme l'adresse, la localisation, l'opinion politique ou la croyance d'un utilisateur doivent être limitées, contrôlées et tracées.

Pour contrôler l'accès à ces données particulières, il devient nécessaire de faire la chasse aux comptes à privilèges, souvent associés sans raisons légitimes aux postes à responsabilités dans l'entreprise.

Il devient indispensable de surveiller les comptes des collaborateurs "top management" (DG, DAF, DRH) qui ont le plus souvent des droits d'accès très importants sans même le savoir. Ils peuvent donc être le point de départ d'une perte de données sensibles qui peut mettre du temps à être corrigée. Enfin, au sein de la direction des systèmes d'information, les comptes "admin" et/ou "super-utilisateur" ont le plus souvent accès par défaut à toutes les bases de données, sensibles ou non, alors même que leurs fonctions ne les y autorisent pas.

Aucun outil ne pourra remplacer une culture d'entreprise spécifique à la protection des données. Chaque collaborateur doit être responsabilisé sur cette thématique, pour ne plus jamais qu'un post-it/mot de passe se retrouve collé sur un écran.

Pour en savoir plus

Sécurité : Gérer les habilitations
Antisèche RGPD 4 : L'abolition des privilèges, c'est maintenant !

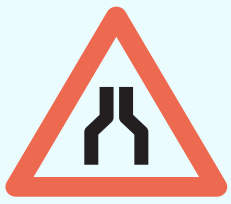
L'ABOLITION DES PRIVILÈGES, C'EST MAINTENANT !

> “ Pour plus de sécurité, pensez à mieux contrôler les comptes utilisateurs à privilèges. ”

Enjeu

Les données personnelles sont des données particulièrement sensibles, que ce soit des opinions politiques ou la religion d'un utilisateur. Ces données ne doivent pas être manipulées ou vues par une personne non habilitée à le faire.

Les comptes à privilèges doivent être limités dans la durée



Les accès doivent être restreints aux seuls fichiers strictement nécessaires

Certains champs des données personnels peuvent être obfusqués

En pratique

Comment bien contrôler les droits d'accès de tous les comptes utilisateurs selon leurs besoins ?

La première chose à faire ? Dénombrer le nombre de comptes à privilèges et en diminuer les droits d'accès selon les situations. Enfin, il ne faut pas oublier de supprimer les comptes dormants (des comptes de collaborateurs qui ont quitté la société par exemple).

Recenser les dysfonctionnements existants

- Trouver les comptes ayant des droits d'accès trop importants
- Supprimer les comptes dormants (collaborateurs ayant quitté l'entreprise)
- Définir correctement le niveau de privilèges accordé à tous les comptes utilisateurs

Garder un niveau de sécurité performant

- Protéger les comptes à privilèges (authentification sécurisée)
- Surveiller l'utilisation de ces comptes à privilèges (période d'activité, utilisation anormale)
- Vérifier régulièrement la pertinence des droits d'accès accordés aux comptes

? POUR ALLER PLUS LOIN → Authentification par mot de passe : les mesures de sécurité élémentaires

5 Gérer la sous-traitance

La sous-traitance est souvent un moyen utilisé pour bon nombre d'entreprise afin de renforcer sa production. Ce recours à la sous-traitance permet aux entreprises d'externaliser les RH, la logistique ou toute autre tâche. Cependant, les sous-traitants ont le plus souvent besoin de données gérées par l'entreprise pour répondre aux missions, données qui peuvent être des données personnelles sensibles. Il devient donc primordial pour l'entreprise et le sous-traitant de les protéger.

Une entreprise qui fait appel à des sous-traitants a la responsabilité de s'assurer de leur fiabilité. Elle doit par exemple leur faire signer un contrat spécifique, notamment pour protéger l'utilisation des données fournies à ces sous-traitants. Ce contrat doit définir clairement l'objet, la durée, la finalité du traitement et les obligations des deux parties. Des contrôles de la sous-traitance sont indispensables pour maîtriser la donnée partagée aux tiers.

Il ne faut pas démarrer une prestation de sous-traitance tant que vous n'avez pas signé un contrat avec le prestataire concerné. Ce contrat devra reprendre les exigences déterminées par l'article 28 du Règlement général sur les protection des données (RGPD).

Pour en savoir plus

Article 28 du RGPD : Sous-traitance
Antisèche RGPD 5 : Ne jamais faire confiance à un inconnu

NE JAMAIS FAIRE CONFIANCE À UN INCONNU

> “ Les données partagées à des sous-traitants doivent bénéficier d’une protection suffisante. ”

Enjeu

L’entreprise qui fait appel à des sous-traitants a la responsabilité de s’assurer de leur fiabilité, notamment avec la signature d’un contrat spécifique. Celui-ci a pour but de définir clairement l’objet, la durée, la finalité du traitement et les obligations des deux parties. Ces contrôles de la sous-traitance ont pour objectif de maîtriser la donnée partagée à des tiers.

Signer un contrat spécifique avec son sous-traitant

Travailler avec des sous-traitants aux garanties suffisantes

S’assurer des capacités de protection des données de ses prestataires

En pratique

Comment être conforme au RGPD en travaillant avec des sous-traitants ?

Pour être conforme au RGPD, il est nécessaire de suivre quelques précautions élémentaires. Ne travailler qu’avec des sous-traitants qui possèdent des garanties minimales (Une politique interne de sécurité des systèmes d’information). Penser à prendre connaissance des moyens utilisés par le prestataire pour assurer une protection des données effective

Précautions élémentaires

- Choisir des sous-traitants aux garanties minimales de sécurité
- Travailler avec des sous-traitants protégeant leurs données (chiffrement, traçabilité)
- Signer un contrat spécifique avec ses sous-traitants

À ne pas faire

- Travailler avec un prestataire sans avoir signer un contrat spécifique (Article 28 du RGPD)
- Avoir recours à un service de cloud sans garanties sur la localisation géographique des données stockées (en dehors de l’UE ?)

POUR ALLER PLUS LOIN → La sous-traitance dans le RGPD

6 Sécurisation des données

Le Règlement Général sur la Protection des Données exige des entreprises et organisations une sécurisation minimale pour les données personnelles et sensibles utilisées par le responsables des traitements.

Le RGPD impose de sécuriser techniquement les données, notamment possible grâce à deux grandes techniques de sécurisation : l'anonymisation et la pseudonymisation des données.

La pseudonymisation est une technique de sécurisation réversible, qui consiste à réduire le lien de corrélation entre les données d'identification et les autres données d'une personne. Ces données ne sont alors pas tout à fait anonymes, mais pas directement identifiables non plus. Le tout est protégé par une clé d'identification, pièce maîtresse pour rétablir le lien entre les données.

Pour en savoir plus

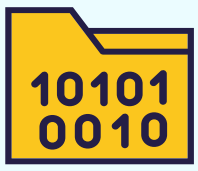
CNIL : Garantir la sécurisation des données
Antisèche RGPD 6 : Et s'il ne fallait pas choisir entre anonymisation et pseudonymisation ?

ANONYMISATION OU PSEUDONYMISATION, À CHACUN SA FORMULE !

“ Encryptez vos fichiers pour des données mieux protégées. ”

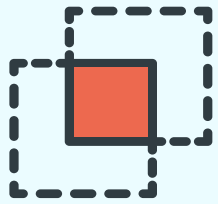
Enjeu

La sécurisation des données implique l’utilisation de techniques permettant de protéger l’identité des individus. Deux grandes techniques de sécurisation sont disponibles pour répondre à ce besoin: l’anonymisation et la pseudonymisation des données.



A chaque donnée/utilisation sa technique et son cryptage

Anonymisation ou pseudonymisation ?



Combiner les techniques et méthodes pour plus de protection

En pratique

Quelles techniques de sécurisation pour ses données ?

La meilleur façon de renforcer la protection de données personnelles et/ou sensibles est de combiner ces techniques de sécurisation des données (anonymisation et pseudonymisation) en fonction de la nature des données, des risques et des besoins d’utilisation finale.

Attention

- L’anonymisation des données est irréversible.
- La pseudonymisation des données dépends de la protection des clés d’identifications.
- Fini le droit d’oublier le droit à l’oubli.

Les techniques de sécurisation

- L’anonymisation est la technique qui consiste à empêcher l’identification d’une donnée de manière irréversible.
- La pseudonymisation consiste à réduire le lien de corrélation entre les données d’identification et les autres données d’une personne.

POUR ALLER PLUS LOIN → Securite : chiffrer, garantir l’intégrité, ou signer.

7

Data Protection Officer

Le RGPD est bel et bien là. Il faut donc rapidement nommer un DPO si votre organisation est dans l'obligation de le faire. Mais dans quels cas la nomination d'un Data Protection Officer est obligatoire ?

Ce délégué à la protection des données (DPD en français) doit obligatoirement être recruté par certaines structures, notamment pour la sécurisation des données et la protection de ces dernières.

A savoir : le non respect de cette obligation peut entraîner l'application d'une sanction administrative pouvant aller jusqu'à 10 millions d'euros ou dans le cas d'une entreprise, jusqu'à 2% du CA annuel mondial, le montant le plus élevé étant retenu. Une sanction très lourde qui oblige à respecter cette dernière et nommer rapidement un DPO si notre organisation est dans l'obligation de le faire.

Obligation de nommer un DPO ?

La réponse est oui dans ces 3 cas :

- Êtes-vous une autorité publique ou un organisme public qui traite des données personnelles ?
- Vos activités de base consistent-elles en des traitements qui exigent, du fait de leur nature, de leur portée et/ou de leur finalité, un suivi régulier et systématique à grande échelle des personnes concernées ?
- Vos activités de base consistent-elles en un traitement à grande échelle de catégories particulières de données ou de données relatives à des condamnations pénales ou à des infractions ?

Pour en savoir plus

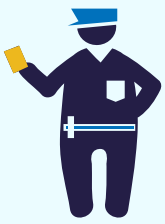
CNIL : Désigner un délégué à la protection des données (DPO)
Antisèche RGPD 7 : Un pour tous, tous pour un !

UN POUR TOUS, TOUS POUR UN !

“ La nomination d’un DPO est obligatoire pour certaines organisations, encore faut-il savoir pour lesquelles et se mettre en conformité réglementaire. ”

Enjeu

Ne pas nommer un DPO quand on y est obligé par le RGPD peut entraîner une amende de 10 millions d’euros ou jusqu’à 2% du chiffre d’affaires annuel mondial total de l’exercice précédent !



Éviter l’importante amende de 10 millions d’euros ou 2% du CA

Se mettre en conformité réglementaire

Évoluer vers une culture d’entreprise tournée vers la protection des données personnelles

En pratique

Comment savoir si son entreprise est dans l’obligation de nommer un DPO avec l’arrivée du RGPD ?

L’article 37 du RGPD désigne trois cas particuliers où la désignation d’un DPO par un responsable de traitement ou par un sous-traitant est obligatoire.

3 cas où l’organisation doit nommer un DPO

- Pour les autorités ou organismes publiques
- Pour une entreprise qui doit manipuler des données personnelles avec un suivi régulier
- Pour une entreprise qui manipule des données sensibles (religion, orientation sexuelle, etc.)

Comment choisir son DPO ?

- Le candidat a-t-il une formation spécifique pour devenir DPO ?
- Le candidat a-t-il un label certificateur ? (labels CNIL en audit et gouvernance)
- Le candidat doit posséder d’importantes compétences techniques pour gérer les traitements

? POUR ALLER PLUS LOIN → Devenir délégué à la protection des données

8 Droit à la portabilité des données

Avec le “droit à la portabilité”, le RGPD permet aux citoyens de l’Union Européenne de reprendre le contrôle de leurs données personnelles. Ce nouveau droit leur permet d’obtenir et de réutiliser leurs données personnelles à leur convenance, pour d’autres services.

L’objectif est donc de permettre aux citoyens de changer de services plus facilement sans craindre une perte de leurs données ou qu’elles deviennent inaccessibles. Les responsables du traitement doivent donc communiquer sur ce nouveau droit, pour permettre aux personnes concernées de jouir de ce dernier.

Enfin, ces responsables sont encouragés à délivrer une information spécifique sur le droit à la portabilité en amont d’une clôture de compte, permettant à la personne concernée de récupérer ses données personnelles et les réutiliser si besoin.

Ce nouveau droit permet à une personne :

De récupérer les données traitées par un organisme et la concernant, pour son usage personnel et/ou pour les stocker sur un appareil de son choix ou un cloud privé. La gestion des données personnelles en est facilité.
De transférer ses données personnelles d’un organisme à un autre. Ces données peuvent ensuite être utilisées par le nouvel organisme, qui les reçoit de la personne elle-même ou par l’organisme qui les détient si cela est “techniquement possible”.

? Pour en savoir plus

CNIL : Le droit à la portabilité en questions
Antisèche RGPD 8 : Ce qui est à moi n’est pas à toi

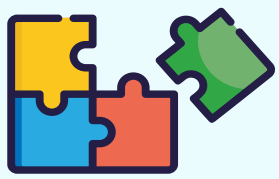
CE QUI EST À MOI N'EST PAS À TOI

“ Le “droit à la portabilité” offre la possibilité aux personnes d’obtenir et de réutiliser leurs données personnelles à leur convenance, pour d’autres services. ”

Enjeu

Ce nouveau droit doit permettre aux citoyens de reprendre le contrôle de leurs données personnelles, en ayant la possibilité de changer de services plus facilement sans avoir la crainte de voir leurs données personnelles perdues ou inaccessibles.

Le responsable des traitements doit communiquer sur ce nouveau droit



Le responsable des traitements doit faciliter le droit à la portabilité

Les citoyens pourront reprendre le contrôle de leurs données personnelles

En pratique

Le droit à la portabilité offre aux personnes la possibilité de récupérer une partie de leurs données dans un format ouvert et lisible par machine.

Ce droit renforce la maîtrise des personnes sur leurs données personnelles. Il crée également de nouvelles opportunités de développement et d’innovation en facilitant le partage de données personnelles, de manière sécurisée et sous le contrôle de la personne concernée.

Le droit à la portabilité permet de

- Récupérer les données la concernant traitées par un organisme, pour son usage personnel.
- Transférer ses données personnelles d’un organisme à un autre.

Conditions du droit à la portabilité

- Limité aux données personnelles fournies par l’individu en question
- Seulement si les données sont traitées de manière automatisée
- Ne doit pas porter atteintes aux droits et libertés de tiers

POUR ALLER PLUS LOIN → Droit à la portabilité des données, article 20 du RGPD

9

Le droit à l'information

Comment mieux contrôler la diffusion de ses données personnelles ? Le RGPD permet aux citoyens de l'Union Européenne d'avoir un droit de regard sur la gestion de ses données personnelles, le "droit d'information". Ce nouveau règlement impose moins de procédures administratives pour l'utilisation des données, avec comme contrepartie plus de responsabilités définies par le RGPD.

Avec comme responsabilité, par exemple, en cas de violation de données, de devoir informer toutes personnes dont les données traitées sont concernées. C'est l'article 34 du RGPD qui le spécifie, celui-ci prévaut uniquement dans le cas de violation "susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique".

Vous êtes une organisation qui traite des données personnelles, et sans autorisation, de façon accidentelle ou illicite, ces données ont été : détruites, perdues, altérées, divulguées ou accédées par des individus ? Vous remplissez les conditions de violation importante de données à caractère personnel.

Pour en savoir plus

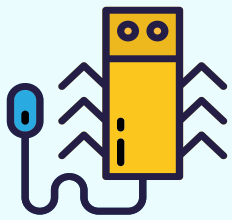
CNIL : Le droit à l'information
Antisèche RGPD 9 : Le droit à l'information, c'est votre droit de savoir !

LE DROIT À L'INFORMATION: C'EST VOTRE DROIT DE SAVOIR !

“ Vous avez le droit de savoir ! ”

Enjeu

Plus de responsabilité, c'est notamment - en cas de violation de données - le devoir pour une organisation d'en informer toutes personnes dont les données (traitées) sont concernées.



Un piratage grave de données à caractère personnel doit être communiqué.

Exigence de réactivité et d'informations.

Impératif de gouvernance et de sécurisation des données personnelles.

En pratique

Le piratage, c'est quand? et comment l'éviter?

Vous êtes une organisation qui traite des données personnelles et, sans autorisation, de façon accidentelle ou illicite, ces données ont été piratées dans le cadre de votre activité ? Alors vous remplissez les conditions de violation importante de données à caractère personnel.

Piratage = Données...

- Détruites
- Perdues
- Altérées
- Divulguées
- Accédées

Que faire?

- Plus de maîtrise: **data governance / data knowledge**
- Plus de responsabilités: **sécuriser / protéger**
- Plus de transparence: **communiquer / informer**

POUR ALLER PLUS LOIN → Notifier une violation des données personnelles

10

Le registre des traitements

Le registre des activités de traitements n'est pas nouveau, il existait déjà avant l'arrivée du RGPD. Mais celui-ci servait notamment pour conserver les traitements exonérés de déclaration auprès de la CNIL, tenu par le correspondant informatique et libertés.

Aujourd'hui, avec le RGPD, les responsables du traitement mais aussi les sous-traitants seront dans l'obligation de tenir un registre des traitements. Ces derniers (les sous-traitants) n'étaient notamment pas soumis à cette obligation avant le nouveau règlement.

Le but de cette obligation ? Permettre à la CNIL des contrôles facilités et accompagner les responsables et sous-traitants dans l'application du RGPD, notamment avec une vision plus éclairée des traitements effectués dans leur société. Avec un registre bien bien tenu, il sera plus simple d'avoir un état des lieux fiable des traitements, permettant une meilleure gestion pour cibler d'éventuels écarts à la loi : catégories des données, destination des données, finalités, caractères…

Concrètement, quelles entreprises sont concernées par cette obligation ? Il s'agit de toute entreprise ou administration qui emploie plus de 250 personnes. Cependant, celles employant moins de 250 personnes n'en sont pas totalement exonérées.

Pour en savoir plus

CNIL : Le registre des activités de traitement
Antisèche RGPD 10 : On ne mélange pas les torchons et les serviettes

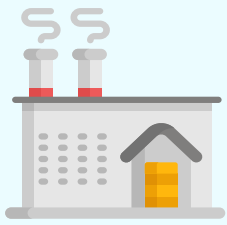
ON NE MÉLANGE PAS LES TORCHONS ET LES SERVIETTES

“ Le registre des activités de traitements n’est pas une nouveauté du RGPD. Il existait déjà au temps de la loi informatique et liberté, pour conserver les traitements exonérés de déclaration auprès de la CNIL. ”

Enjeu

Permettre à la CNIL des contrôles facilités, accompagner les responsables et sous-traitants dans l’application du RGPD avec une vision plus éclairée des traitements.

Obligation de tenir un registre des traitements pour les sous-traitants



Registre pour les entreprises de plus de 250 employés

Ce registre doit faciliter le contrôle de la CNIL

En pratique

Quelles entreprises sont-concernées par cette obligation de tenir un registre des traitements ?

Il s’agit de toute entreprise ou administration qui emploie plus de 250 personnes. Cependant, celles employant moins de 250 personnes n’en sont pas totalement exonérées.

Obligation de tenir un registre des traitements

- Pour les entreprises de plus de 250 employés
- Pour les sous-traitants de ces entreprises concernées
- Pour les plus petites entreprises qui traitent des données personnelles sensibles

Le contenu du registre des traitements

- Le nom du responsable du traitement ou de son représentant
- Les finalités du traitement
- Les différentes catégories de données traitées
- Les délais prévus de destruction des données

POUR ALLER PLUS LOIN → [l’article 30 du RGPD relatif au "Registre des activités de traitement]

11

Le droit à l'effacement

Avec le "droit à l'oubli" ou "droit à l'effacement", le RGPD redonne encore un peu plus de contrôle aux citoyens européens pour mieux maîtriser leurs données personnelles. Ce droit permet aux personnes concernés de demander l'effacement de données qui porteraient atteinte à leur vie privée.

Pour jouir de ce droit, les citoyens peuvent en faire la demande directement auprès de l'organisation et de son responsable des traitements, qui devra donc supprimer les données incriminées dans les meilleurs délais. A savoir que les données que l'individu souhaite supprimer doivent entrer dans les motifs décrits par le RGPD.

Attention aux entreprises qui prendraient trop de temps pour répondre aux demandes de suppressions ou qui refuseraient une demande d'effacement. La violation du RGPD peut exposer les entreprises à des actions collectives de la part des citoyens européens.

Le "droit à l'oubli" ou droit à l'effacement est un droit renforcé par le nouveau règlement général pour la protection des données (RGPD). L'article 17 permet à la personne concernée de demander au responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant.

? Pour en savoir plus

Outil CNIL : contrôler votre droit à l'oubli
Antisèche RGPD 11 : Quand tourner la page devient possible

QUAND TOURNER LA PAGE DEVIENT POSSIBLE

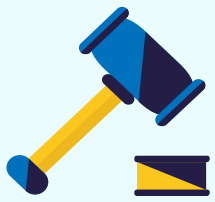
> “Le RGPD renforce le droit à l’effacement ou “droit à l’oubli” pour redonner aux citoyens européens le contrôle de leurs données personnelles.”

Enjeu

Ce droit leur permet de demander l’effacement de données qui porteraient atteinte à leur vie privée.

Les citoyens européens peuvent demander la suppression leurs données personnelles

Le RGPD prévoit des motifs où la demande de suppression est obligatoire



En cas de refus, l’organisation s’expose à des amendes et/ou plaintes

En pratique

L’article 17 permet à la personne concernée de demander au responsable du traitement l’effacement, dans les meilleurs délais, de données personnelles la concernant.

Le responsable du traitement a donc l’obligation d’effacer ces données le plus rapidement possible, dans ces différents cas :

Cas où le “droit à l’oubli” s’applique

- Les données utilisées ne sont plus nécessaires leur finalité première
- L’individu retire son consentement pour l’utilisation de ses données
- Les données personnelles utilisées le sont de manière illicite

Cas où le droit à l’effacement ne peut être appliqué

- Pour le droit à la liberté d’expression et d’information
- Afin de respecter une obligation légale de l’UE ou d’un État membre
- Pour l’intérêt public (santé, recherches scientifiques et historiques)
- Pour la constatation, l’exercice ou la défense de droits en justice

POUR ALLER PLUS LOIN → l’article 17 du RGPD relatif au "Droit à l'effacement («droit à l'oubli»)

12 L’analyse d’impact

L’article 35 du RGPD impose au responsable des traitements de conduire une analyse d’impact sur la protection des données (DPIA – Data Protection Impact Assessment) dès lors qu’un traitement de données personnelles est susceptible de devenir un risque élevé pour les droits et libertés des individus concernés.

L’objectif annoncé de ce DPIA est de prévenir une perte de données ou des risques d’utilisation frauduleuse. Cette analyse d’impact est un outil important pour les entreprises, leur permettant de contrôler les traitements de données, avec la volonté de les rendre respectueux de la vie privée en amont (Security by Default).

Le DPIA est donc un moyen de protéger les citoyens européens contre les risques sur leur vie privée et leurs données personnelles.

A titre d’exemple : Une organisation met en place une offre à destination des enfants avec l’analyse des données résultants de celle-ci. Le traitement remplit donc le critère de surveillance systématique et celui des données concernant des individus vulnérables (ici des enfants), la mise en place d’un DPIA est donc obligatoire et nécessaire.

Pour en savoir plus

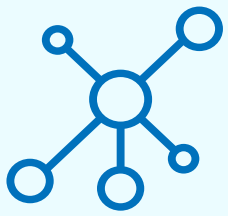
CNIL : L’analyse d’impact relative à la protection des données (DPIA)
Antisèche RGPD 12 : Prudence est mère de sûreté

PRUDENCE EST MÈRE DE SÛRETÉ

> “ Le RGPD impose de conduire un DPIA dès qu’un traitement de données personnelles est susceptible d’entraîner un risque élevé pour les droits et libertés des individus concernés. ”

Enjeu

Ce droit leur permet de demander l’effacement de données qui porteraient atteinte à leur vie privée.



L’analyse d’impact permet de prévenir la fuite de données ou les risques élevés

Le DPIA permet le contrôle des traite-ments avec le “Security by Default”

Prouver la conformité des traitements de données avec le RGPD

En pratique

Avec l’article 35, le RGPD demande au responsable des traitements de conduire une analyse d’impact sur la protection des données (DPIA - Data Protection Impact Assessment).

L’analyse d’impact n’est pas obligatoire dans ces cas

- Le traitement ne présente pas de risque important pour les droits et libertés
- Le traitement envisagé est similaire à un autre pour lequel un DPIA a déjà été mené
- Lorsque le traitement résulte d’une obligation légale du service public
- Quand le traitement rentre dans la liste des exceptions déterminées par la CNIL

L’analyse d’impact est obligatoire si un traitement remplit 2 critères

- Collecte de données sensibles
- Scoring / évaluation / profilage
- Surveillance systématique
- Collecte de données personnelles à grande échelle
- Décision automatique avec effet légal ou similaire
- Croisement de données
- Usages innovants (technologie novatrice)
- Personnes vulnérables (enfants, patients, personnages âgés, etc.)

POUR ALLER PLUS LOIN → Article 35 : Analyse d'impact relative à la protection des données

13

Le droit d'accès

Véritable opportunité pour les organisations, le RGPD est un règlement qui va réorganiser la manière dont fonctionne l'utilisation des données personnelles, redonnant confiance aux citoyens européens dans les organisations les utilisant. Le RGPD entraîne la mise en place de nouvelles stratégies spécifiques pour la gestion, la protection et l'utilisation des données personnelles des utilisateurs / clients.

L'article 15 du RGPD (droit d'accès) permet à toute personne résidant dans l'Union Européenne et dont une organisation détient ses données personnelles de demander un accès à ces dernières. Cet article donne la possibilité aux individus de mieux contrôler leurs données personnelles, notamment en ayant une information claire sur quelles données sont utilisées par les organisations et pour quelles finalités.

L'article 15 du RGPD "Droit d'accès de la personne concernée" permet à la personne concernée de demander au responsable du traitement la confirmation que les données à caractère personnel la concernant sont ou ne sont pas traitées.

Pour en savoir plus

CNIL : Le droit d'accès
Antisèche RGPD 13 : Donner, c'est donner, modifier, c'est autorisé

DONNER, C'EST DONNER ; MODIFIER, C'EST AUTORISÉ

> “ L’article 15 (droit d’accès) permet à toute personne résidant dans l’Union Européenne et dont une organisation détient ses données personnelles de demander un accès à ces dernières. ”

Enjeu

Le RGPD est une opportunité pour les organisations avec la mise en place de stratégies spécifiques pour la gestion, la protection et l’utilisation des données personnelles de leurs clients / utilisateurs.

Permettre aux individus de reprendre le contrôle sur leurs données personnelles

Amendes de 20 millions d’euros ou 4% du chiffre d’affaires annuel

Améliorer la confiance et la relation client

En pratique

Dès que le RGPD entrera en application, le délai pour répondre à une demande d’accès aux données personnelles sera réduite à un mois.

En plus des données, l’accès aux informations suivantes doit être assuré :

- les finalités du traitement de ces données
- de quelles catégories sont les données personnelles utilisées
- les destinataires ou catégories de destinataires auxquels les données personnelles ont été ou seront communiquées, notamment pour les destinataires situés dans des pays tiers ou organisations internationales
- dans la mesure du possible, le temps de conservation des données envisagé ou, si possible, les critères utilisés pour déterminer cette durée
- la possibilité de demander au responsable du traitement de rectifier ou de supprimer des données personnelles, ou une limitation de l’utilisation de celles-ci

POUR ALLER PLUS LOIN → Article 15 : Droit d'accès de la personne concernée

14

Le droit d'opposition

L'article 21 du RGPD permet aux citoyens européens de mieux contrôler leurs données personnelles, avec par exemple un droit à l'opposition. Cela signifie que chaque individu peut s'opposer pour des motifs légitimes, à figurer dans un fichier. En ce qui concerne la prospection, commerciale par exemple, ce droit peut être utilisé sans obligation de justification d'un motif légitime.

Ce droit à l'opposition peut donc s'appliquer dans plusieurs situations, comme contrôler plus concrètement ses donnée personnelles :

- Stopper la diffusion de données personnelles par un site internet
- Changer d'avis et demander la suppression de ses données de la base client de son coiffeur
- S'opposer à l'envoi de publicités d'une société
- Supprimer son profil dans l'organigramme de son ancien employeur

Toujours conserver une copie des démarches engagées.
Dès que vous démarrez des démarches pour jouir de votre droit à l'opposition, pensez à toujours envoyer votre courrier avec un accusé de réception. Cela permettra de prouver si nécessaire la date exacte de la démarche.

Pour en savoir plus

CNIL : Le droit d'opposition
Antisèche RGPD 14 : Quand c'est non, c'est toujours non.

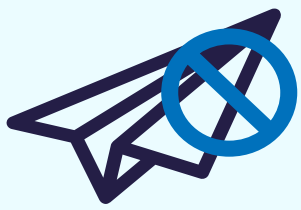
QUAND C'EST NON, C'EST TOUJOURS NON.

“ Avec l'article 21 et ce droit à l'opposition, chaque individu peut s'opposer à la conservation, la diffusion ou la transmission de ses données personnelles. ”

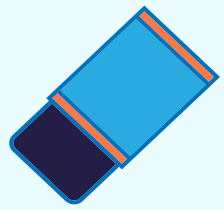
Enjeu

Ce droit à l'opposition peut s'appliquer dans plusieurs situations, notamment pour contrôler plus concrètement ses données personnelles.

Mettre fin à la diffusion de données personnelles par un site internet



Stopper l'envoi de publicités d'une société



Changer d'avis et effacer ses données de la base client de son fleuriste

En pratique

Le droit d'opposition est exclusivement personnel, avec l'impossibilité de l'étendre au informations relatives à des tiers, sauf les cas de représentation de mineurs ou de majeurs protégés.
Ce droit s'exerce dans 2 situations.

Première situation : 1

- Au moment de la collecte d'informations (en remplissant un formulaire par exemple), l'organisation vous informe de la possibilité de refuser de recevoir de la publicité de leur part, en cochant une case.

- En la cochant, vous indiquez à l'organisme que vous vous opposez au traitement de vos informations.

Deuxième situation : 2

- Vos données personnelles sont utilisées dans un fichier non obligatoire et ce n'est plus votre souhait.

- Vous suivez donc plusieurs étapes pour demander à l'organisme l'arrêt des traitements de vos données personnelles.

? POUR ALLER PLUS LOIN → Article 21 : Le droit d'oppositions

15 Le consentement des enfants

Le Règlement Général Européen sur la Protection des Données (RGPD) apporte des règles spécifiques, avec pour objectif de renforcer la protection des individus et dans le cas de l'article 8, des enfants. Ce dernier impose une limite d'âge avant lequel les jeunes citoyens européens ne peuvent donner légalement leur consentement. Enfin, le responsable du traitement et l'organisme sont dans l'obligation d'utiliser un vocabulaire accessible pour les plus jeunes lors de la demande de leur consentement.

Le nouveau règlement RGPD permet de mieux protéger les enfants vis à vis des services de la société de l'information.

Dès lors qu'un service est proposé directement à un enfant, les responsables du traitement doivent s'assurer qu'un langage clair et simple est utilisé pour les avis de confidentialité, notamment pour les enfants puissent facilement les comprendre.

Pour en savoir plus

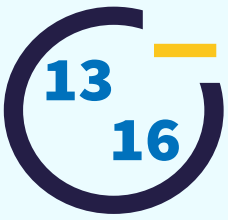
CNIL : COMMENT ADAPTER L'INFORMATION AUX ENFANTS ?
Antisèche RGPD 15 : Il faut que jeunesse se fasse protéger

IL FAUT QUE JEUNESSE SE FASSE PROTÉGER

> “ Le Règlement Général Européen sur la Protection des Données (RGPD) apporte des règles spécifiques, avec pour objectif de renforcer la protection des individus et dans le cas de l’article 8, des enfants. ”

Enjeu

Il est aussi demandé au responsable du traitement et à l’organisme d’utiliser un vocabulaire accessible pour les enfants et leur demander leur consentement au préalable.



Une limite entre 13 et 16 ans pour le consentement individuel

L’organisme doit utiliser un vocabulaire accessible pour l’audience cible

Consentement du responsable parental pour un enfant en dessous de l’âge requis

En pratique

Dans le cas d’un enfant en dessous de l’âge limite de consentement, le responsable des traitements devra demander l’autorisation de consentement de la personne détenant la responsabilité parentale.

Le RGPD demande au responsable des traitements :

- De s’assurer qu’un langage clair et simple est utilisé pour les avis de confidentialité, notamment pour les enfants puissent facilement les comprendre.

- De faire des “efforts raisonnables” pour vérifier que la personne fournissant le consentement est bien la figure parentale.

POUR ALLER PLUS LOIN → Article 8 : Conditions applicables au consentement des enfants

16

Droit de rectification

Le droit de rectification est assuré par le RGPD et permet aux citoyens européens de garder la main sur leurs données personnelles. Avec ce droit, les citoyens européens peuvent supprimer leurs données personnelles, les exporter vers un nouveau service, y avoir accès et de jouir de leur droit de rectification de toute donnée personnelle qui serait inexacte (article 16 du RGPD).

La personne concernée a le droit de demander la rectification de ses données personnelles au responsable du traitement qui les utilise. Une fois demandée, la rectification doit être réalisée dans les plus brefs délais. Selon la finalité du ou des traitements utilisant ses données personnelles, l'individu concerné a le droit d'obtenir une modification de ces dernières pour les compléter, en fournissant une déclaration supplémentaire.

Pour ne pas être en infraction vis à vis du RGPD, il est nécessaire de mettre en place un processus interne qui permettra de garantir l'identification et le traitement des demandes dans un délai raisonnable (1 mois maximum).

Pour en savoir plus

CNIL : Le droit de rectification
Antisèche RGPD 16 : Mieux vaut rectifier que tout supprimer

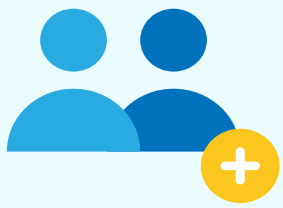
MIEUX VAUT RECTIFIER QUE TOUT SUPPRIMER

“ Une fois la demande de rectification formulée, le responsable du traitement doit y répondre dans les meilleurs délais. ”

Enjeu

Avec l’article 16 du RGPD, la personne concernée a le droit de demander la rectification de ses données personnelles au responsable du traitement qui les utilise.

Répondre à une demande en 1 mois maximum



Faciliter la mise en contact avec le respon-sable des traitements

Consentement du responsable parental pour un enfant en dessous de l’âge requis

En pratique

La personne concernée a le droit d’obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui seraient inexactes.

Quelles sont les différentes étapes pour demander une rectification de ses données personnelles ?

- Identifier le responsable du traitement
- Ecrire au responsable du fichier (La CNIL propose des modèles types de courriers)
- Justifier votre identité auprès de l’organisme
- Toujours conserver une copis des démarches (courrier avec accusé de réception par exemple)

POUR ALLER PLUS LOIN → [Article 16 : Le Droit de rectification]

17 Mise en conformité

Avec l'arrivée du RGPD, la possibilité de voir son organisation contrôlée par la CNIL est belle et bien présente. A savoir que c'est bien l'entreprise qui doit prouver qu'elle est bien en conformité avec les différentes réglementations en vigueur. Pour plus de facilité, il est donc recommandé de constituer et regrouper les documents nécessaires à cette tâche.

Avec le RGPD, c'est bien au responsable des traitements de contrôler et de réexaminer les actions et documents réalisés à chaque étape d'un traitement, notamment pour s'assurer de la protection des données en continu.
ses données personnelles, l'individu concerné a le droit d'obtenir une modification de ces dernières pour les compléter, en fournissant une déclaration supplémentaire.

Apporter la preuve de sa mise en conformité avec le RGPD est obligatoire, surtout lors d'un contrôle de la CNIL. Ne pas pouvoir prouver que l'organisation respecte les obligations prévues par le règlement européen peut l'exposer à de fortes amendes.

Pour en savoir plus

CNIL : RGPD : se préparer en 6 étapes
Antisèche RGPD 17 : La preuve incombe à celui qui se met en conformité !

LA PREUVE INCOMBE À CELUI QUI SE MET EN CONFORMITÉ

> “ Dès lors qu’un contrôle est effectué dans une organisation, c’est à celle-ci deprouverqu’elle est bien en conformité avec les différentes réglementations en vigueur. ”

Enjeu

Afin de prouver facilement la conformité avec le RGPD, il est donc recommandé de constituer un dossier documentaire, regroupant les mesures organisationnelles et techniques mises en place.

Obligation de prouver sa conformité

CNIL.

Faciliter les contrôles de la CNIL

Regrouper les mesures organisationnelles

En pratique

Afin de répondre à une demande de contrôle, de la part de la CNIL par exemple, l’organisation doit donc prouver sa conformité.

Le dossier devra notamment comporter les éléments qui suivent :

- Tenir un registre des traitements (pour les responsables de traitements)
- Mener des analyses d’impact sur la protection des données (DPIA)
- Stocker les mentions d’information
- Mettre en place des modèles de recueil du consentement des personnes
- Les procédures utilisées pour permettre l’exercice des droits des personnes
- Les contrats signés avec les sous-traitants

POUR ALLER PLUS LOIN → Documenter la conformité