RGPD

RGPD

- Le RGPD, Règlement Général de Protection des Données, est le texte de référence en matière de protection des données au niveau de l'Union Européenne
- Le règlement a été publié en avril 2016
- Il est entré en application le 25 mai 2018
- Il impacte toutes les entreprises qui traitent des données à caractère personnel sur des résidents de l'Union Européenne

RGPD

- Il s'agit d'un règlement européen
- Le texte entre donc en application directement et en même temps dans tous les Etats membres de l'Union Européenne, sans transposition
- Le RGPD, le règlement 679/2016, remplace la directive 95/46/CE, publiée en 1995
- Cette directive a servi, en France, de fondement à la loi Informatique & Libertés et ses évolutions : 1978, 1991, 2004

RGPD

3 objectifs

Le RGPD poursuit 3 objectifs :

- uniformiser la réglementation sur la protection des données
- responsabiliser davantage les entreprises en développant l'autocontrôle
- renforcer le droit des personnes : droit à l'accès, droit à l'oubli, droit à la portabilité

RGP

Définition et périmètre

- L'environnement technologique et numérique a fortement évolué
- Le RGPD a été conçu pour adapter et moderniser le cadre juridique en matière de protection des données
- Il doit " *redonner aux citoyens le contrôle de leurs données personnelles, tout en simplifiant l'environnement réglementaire des entreprises* "

Périmètre d'application

Les personnes physiques

- Les règles et obligations du RGPD s'appliquent au traitement – automatisé ou non – des données à caractère personnel rattachées à des personnes physiques
- L'objectif est de renforcer l'encadrement des pratiques en matière de collecte et d'utilisation des données à caractère personnel

Périmètre d'application

Les personnes physiques

- 2 illustrations :
  - la collecte de données sur des représentants d'une entreprise, à partir de cartes de visite par exemple, entre dans le champ d'application du RGPD
  - par contre la collecte d'informations sur l'entreprise (dénomination sociale, objet social, numéro de TVA, SIRET, etc.) en est exclue

Périmètre d'application

Le traitement des données

Le traitement des données concerne :

- la collecte
- l'accès
- le stockage
- la manipulation
- la destruction
- la consultation à distance

2 définitions

Données à caractère personnel

Personne physique

Le RGPD donne une définition précise des données à caractère personnel (DCP)

- il s'agit de " *toute information se rapportant à une personne physique identifiée ou identifiable* "
- par personne physique identifiable, il faut comprendre " *une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* "

RGPD

Les entreprises concernées

- Les règles du RGPD s'appliquent à toutes les entreprises privées ou publiques collectant et traitant des données à caractère personnel sur les résidents de l'Union Européenne
- Le règlement s'applique également aux entreprises non implantées en UE, dès lors qu'elles collectent et traitent des données personnelles sur des résidents de l'U
- Exemples : Google, Microsoft, Apple, Facebook …

RGPD

Les entreprises concernées

- Une entreprise qui délègue à un prestataire la collecte et le stockage des données fait néanmoins du traitement de données dans la mesure où elle les utilise
- L'immense majorité des entreprises est donc concernée par les dispositions du RGPD

Les 4 principes clés du RGPD

Les dispositions du RGPD s'articulent autour de 4 principes clés :

- le consentement
- la transparence
- le droit des personnes
- la responsabilité

Les 4 principes clés du RGPD

1

Le consentement

- Ce principe existait déjà, il est renforcé par le RGPD
- Il doit être " explicite et positif "
- Il peut être retiré à tout moment par les personnes qui le demandent
- Les entreprises qui traitent des données doivent être en mesure de prouver le recueil de ce consentement en cas de contrôle

Les 4 principes clés du RGPD

2

La transparence

- Elle complète le consentement
- Les entreprises doivent fournir aux individus des informations claires et sans ambiguïté sur la manière dont leurs données sont traitées, et ce, de façon compréhensible
- La transparence doit s'exprimer sur les formulaires de collecte, dans les documents contractuels, sur la page du site relative à la politique de confidentialité, etc.

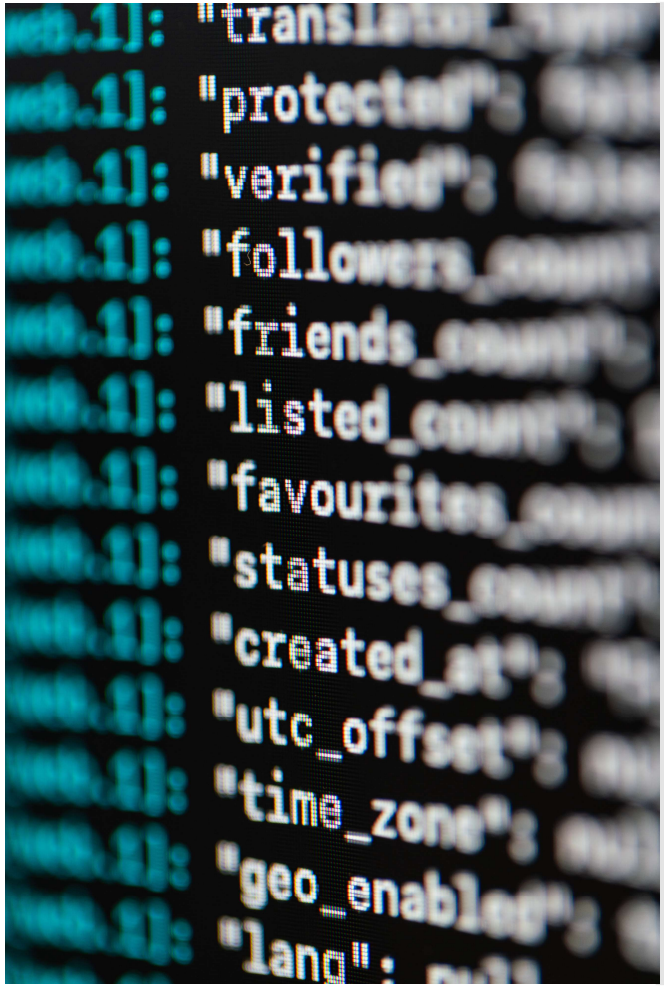
Les 4 principes clés du RGPD

3

Le droit des personnes

1 - Le droit d'accès aux données

- l'entreprise doit faciliter ce droit et mettre en place procédures et outils adaptés
- une solution électronique doit être prévue, si possible avec un accès à distance sécurisé
- en cas de demande d'accès de la part d'un utilisateur, l'entreprise dispose d'un délai d'un mois maximum pour la satisfaire



Les 4 principes clés du RGPD

3

Le droit des personnes

2 - Le droit à l'oubli

- ce droit existait déjà
- il est renforcé
- les entreprises disposent d'un délai d'un mois pour supprimer les données à la suite d'une demande formulée par un client ou un utilisateur
- le délai précédent était de deux mois

- toutes les copies et toutes les reproductions des données doivent aussi être effacées

Les 4 principes clés du RGPD

3

Le droit des personnes

3 - Le droit à la portabilité des données

- il s'agit d'un nouveau droit qui permet à une personne de récupérer les données qu'elle a fournies, sous une forme aisément réutilisable
- par exemple : un fichier texte, un fichier au format Excel …
- on peut aussi transférer les données à un tiers, en cas de changement de fournisseur de services par exemple

Les 4 principes clés du RGPD

4

La responsabilité

Le RGPD vise à responsabiliser davantage les entreprises dans le traitement des données à caractère personnel, à savoir :

- l'obligation faite aux entreprises de documenter toutes les mesures et procédures en matière de sécurité des données à caractère personnel
- l'obligation de démontrer leur conformité avec la réglementation en cas de contrôle
- l'obligation de tenue d'un registre des traitements qui permettra de constituer une base de données des traitements et servira à centraliser et à suivre toutes les démarches de conformité mises en œuvre par l'entreprise

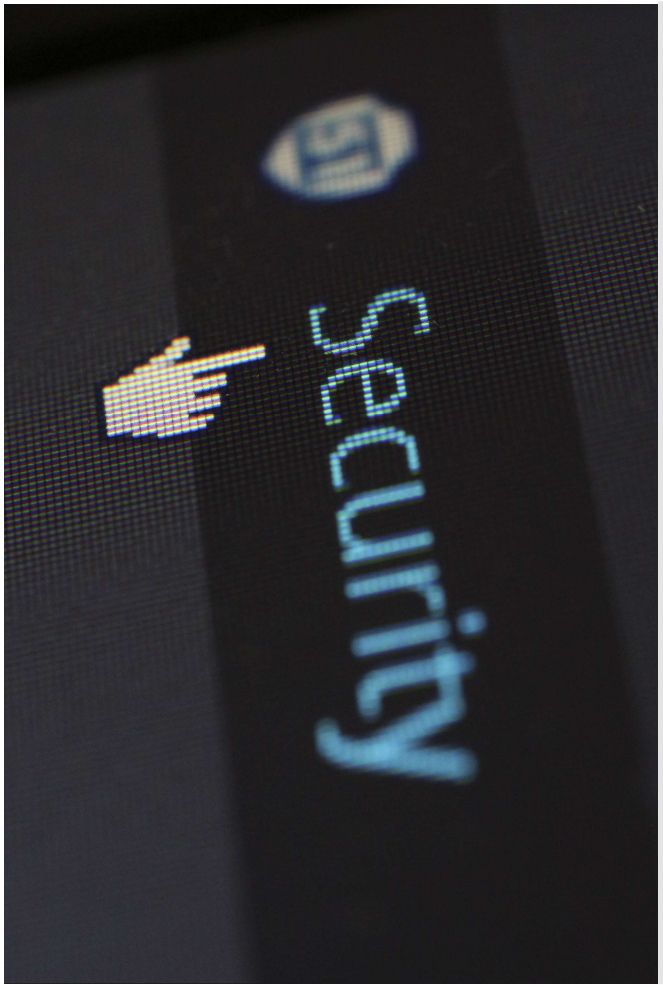
Les 4 principes clés du RGPD

4

La responsabilité

1 - Le renforcement des mesures de sécurité

- les entreprises sont responsables de la sécurité des données qu'elles traitent et doivent mettre en place les mesures adéquates pour la garantir, notamment :
  - la pseudonymisation des données
  - les tests d'intrusions



Les 4 principes clés du RGPD

4

La responsabilité

2 - Pseudonymisation

- c'est un processus réversible qui consiste à remplacer un attribut par un autre
- exemple : changer un nom par un autre nom, ou un par alias
- c'est une technique privilégiée dans les projets où l'identité d'un individu n'est pas essentielle notamment dans les expérimentations de type Big Data où le volume est privilégié à l'identité

Les 4 principes clés du RGPD

4

La responsabilité

3 - Anonymisation

- c'est un processus irréversible qui consiste à supprimer ou modifier toutes les informations directement ou indirectement identifiantes pour rendre impossible toute réidentification des personnes
- c'est le niveau maximal de protection
- l'utilisation d'une fonction de hachage permet de ne pas stocker les mots de passe en clair dans la base mais uniquement de stocker une empreinte de ces derniers *(www.cnil.fr)*
- exemple
  - votre mot de passe est : 123soleil
  - on va le « hasher » (hacher en français) avec un algorithme
  - le mot de passe stocké dans la base de données est :

    1f30014ac280f540d342a9d6d3e06aa9547d7bbfda4413cc677ff1b3dd186972

Les 4 principes clés du RGPD

4

La responsabilité

4 - L'encadrement du profilage

- le profilage est un traitement automatisé de données personnelles visant à évaluer certains traits d'une personne physique :
  - comportement professionnel, productivité, absences, retards …
  - état de santé
  - religion
  - orientation sexuelle
  - affiliation politique …

Les 4 principes clés du RGPD

4

La responsabilité

5 - Le principe de "Privacy By Design"

- il désigne la démarche visant à prendre toutes les mesures pour protéger les droits des personnes lors de la commercialisation d'un produit ou d'un service :
  - dès la conception du produit ou service
  - tout au long du cycle de vie des données, de leur collecte à leur suppression, par ce produit ou service
  - exemple : création d'une nouvelle montre connectée, d'un nouveau traceur d'activités …

Les 4 principes clés du RGPD

4

La responsabilité

6 - L'encadrement des sous-traitants

- les entreprises doivent choisir des sous-traitants présentant des garanties suffisantes
- en cas de faille de sécurité au niveau du sous-traitant, ce sera l'entreprise qui sera tenue pour responsable
- les entreprises doivent revoir les contrats signés avec les sous-traitants en intégrant des clauses concernant les données à caractère personnel
- le RGPD instaure donc un régime de coresponsabilité des sous-traitants

Les 4 principes clés du RGPD

4

La responsabilité

7 - Notifications en cas de failles de sécurité

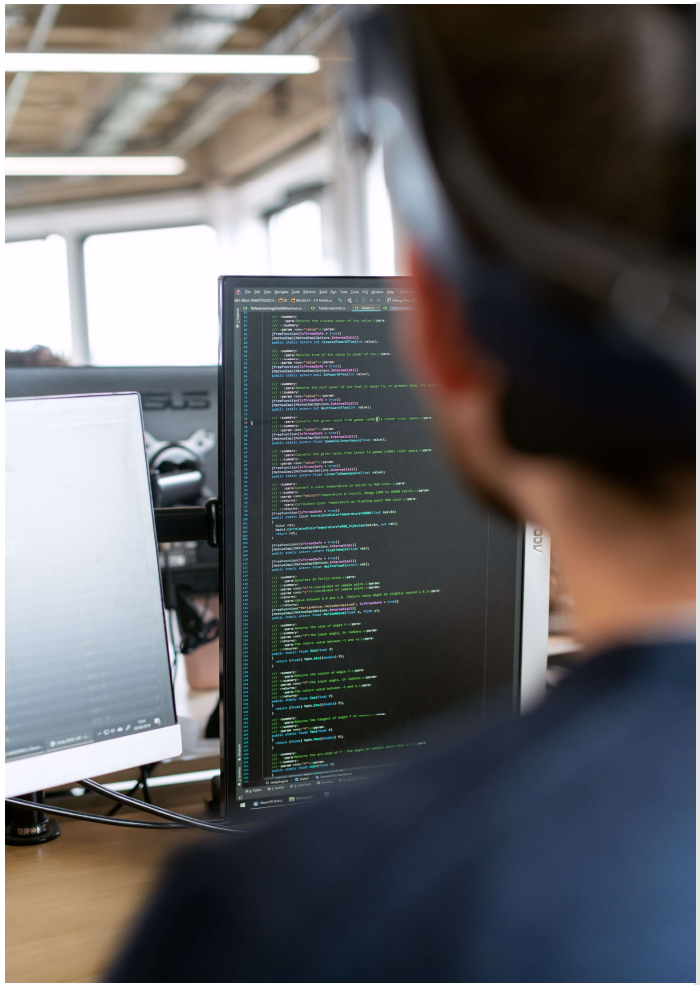
- les entreprises ont pour obligation de mettre en place des actions en cas de violation de sécurité entraînant la destruction, la perte, l'altération ou la divulgation non autorisée de DCP
- en cas de faille de sécurité, l'entreprise doit la notifier à l'autorité de régulation compétente (en France, la CNIL) dans un délai de 72h
- les personnes physiques concernées doivent être informées "dans les meilleurs délais" si la faille ou la violation de données comporte un risque élevé pour les droits et libertés

Les 4 principes clés du RGPD

4

La responsabilité

- l'obligation de désignation d'un Data Protection Officer, en français : " Délégué à la Protection des Données "
- doté d'un rôle très important, le DPO sera chargé de :
  - piloter la gouvernance des données
  - contrôler la conformité de l'entreprise avec le RGPD
  - conseiller le responsable des traitements



Les 4 principes clés du RGPD

4

La responsabilité

- cette obligation de désignation d'un DPO ne s'applique qu'aux entreprises réalisant des traitements sur des données sensibles et/ou à grande échelle
- l'obligation de déclaration préalable à la CNIL est supprimée
- cette mesure traduit le principe qui gouverne le RGPD, responsabiliser les entreprises en développant l'autocontrôle

Les sanctions

Qui ?

Source : www.cnil.fr

Qui prononce les sanctions à la CNIL ?

- les sanctions sont prononcées par la formation restreinte
- la formation restreinte de la CNIL est composée de 5 membres et d'un Président distinct du Président de la CNIL
- ces 5 membres sont élus parmi le collège des 18 membres qui composent la CNIL

Les sanctions

Les étapes d'une procédure

Source : www.cnil.fr

Quelles sont les étapes de la procédure de sanction à la CNIL ?

- lorsqu'il est constaté au cours d'un contrôle ou à la suite d'une plainte, qu'un organisme ne respecte pas le RGPD, le président de la CNIL désigne un Commissaire parmi les membres de la Commission : c'est le rapporteur
- le rapporteur est chargé de rédiger un rapport décrivant les manquements au RGPD et proposant une sanction (par exemple une amende ou un rappel à l'ordre)
- le rapport est envoyé à l'organisme concerné qui a un mois pour répondre
- le président de la CNIL saisit en parallèle la formation restreinte chargée de prononcer les sanctions
- la procédure est écrite

Les sanctions

Les étapes d'une procédure

Source : www.cnil.fr

- cependant, une séance au cours de laquelle le rapporteur présente son rapport se tient systématiquement
- le responsable du fichier peut y présenter des observations orales, à l'appui de sa réponse écrite, et répondre aux questions des Commissaires de la formation restreinte
- les Commissaires de la formation restreinte délibèrent à huis-clos
- ils rédigent la décision de sanction qui est adressée au responsable du fichier
- la décision peut être publique ou non

Les sanctions

La procédure simplifiée

Source : www.cnil.fr

Il existe aussi une procédure simplifiée pour les dossiers peu complexes ou de faible gravité

La procédure est alors :

- instruite par un rapporteur désigné parmi les agents de la CNIL (et non parmi le collège de la Commission)
- les sanctions ne peuvent pas être rendues publiques et sont limitées (rappel à l'ordre, amende d'un montant maximum de 20 000 euros, injonction avec astreinte plafonnée à 100 euros par jour de retard)
- le président de la formation restreinte (ou un membre qu'il désigne) statue seul
- aucune séance publique n'est organisée, sauf si l'organisme demande à être entendu

RGPD

La valeur des sanctions

Source : www.cnil.fr

Lorsque des manquements au RGPD ou à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut prononcer, après une procédure contradictoire, l'une ou plusieurs des mesures suivantes :

- un rappel à l'ordre
- une injonction de se mettre en conformité
- cette injonction peut être assortie d'une astreinte dont le montant ne peut excéder 100 000 euros par jour de retard
- une limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation
- le retrait d'une certification

RGPD

La valeur des sanctions

Source : www.cnil.fr

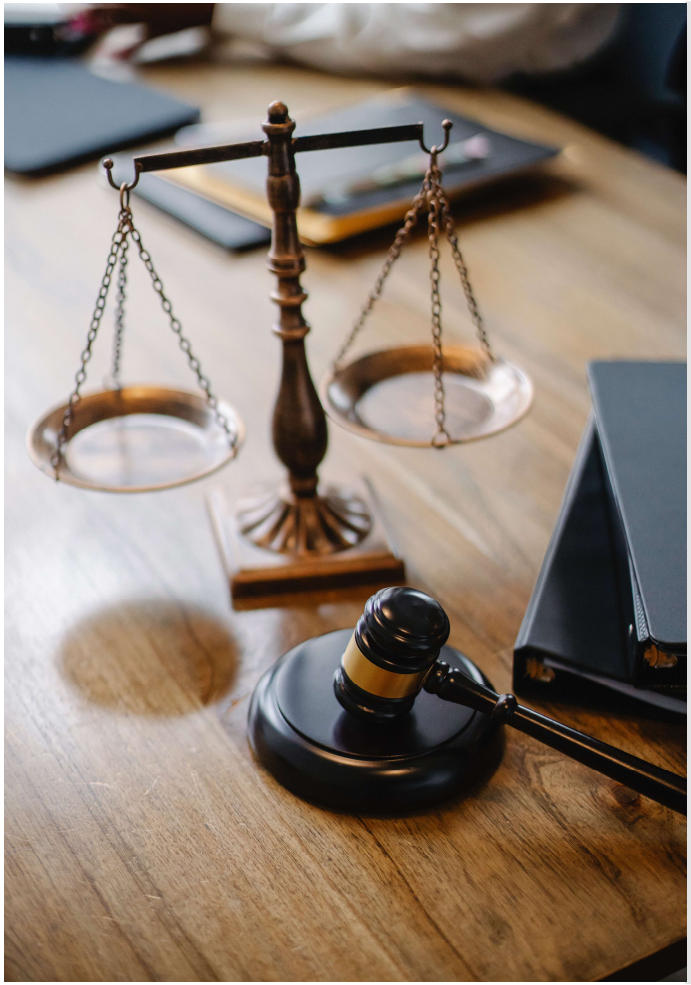
- la suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale
- une suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes (BCR)
- une amende administrative ne pouvant excéder 10 millions d'euros ou 2% du chiffre d'affaire annuel mondial de la société
- pour les manquements les plus graves, ce montant peut s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial

RGPD

La valeur des sanctions

Source : www.cnil.fr

- la formation restreinte peut décider de rendre publique la décision qu'elle adopte
- elle peut également ordonner l'insertion, aux frais des organismes sanctionnés, de la décision dans des publications, journaux et supports qu'elle désigne



RGPD

Les arnaques

Source : www.cnil.fr

Comment reconnaître les arnaques au RGPD ?

Les tentatives d'arnaque peuvent prendre des formes diverses :

- faux courriers, fax ou e-mails utilisant des termes ou symboles laissant penser que le message est adressé par la CNIL ou une autre institution française ou européenne (logo de la CNIL ou d'une autre institution, drapeau tricolore, « Marianne », emblème européen, etc.)
- appels de personnes se faisant passer pour des agents de la CNIL ou pour des sociétés agissant au nom de la CNIL (avec, dans certains cas, l'affichage frauduleux du numéro de téléphone de la CNIL 01 53 73 22 22)

RGPD

Les arnaques

Source : www.cnil.fr

Plusieurs modes opératoires ont été identifiés :

- des sociétés démarchent des professionnels, parfois de manière agressive, afin de vendre de faux services d'assistance à la mise en conformité du RGPD
- des personnes se faisant passer pour des agents de la CNIL (contrôleurs, etc.), ou pour des sociétés mandatées par la CNIL, proposent à des professionnels des services payants d'assistance à la mise en conformité au RGPD, en les menaçant d'une lourde sanction financière ou d'une action contentieuse
- des personnes se faisant passer pour des agents de la CNIL, ou pour des sociétés mandatées par la CNIL, proposent à des particuliers victimes d'une première arnaque d'être remboursés des sommes précédemment versées