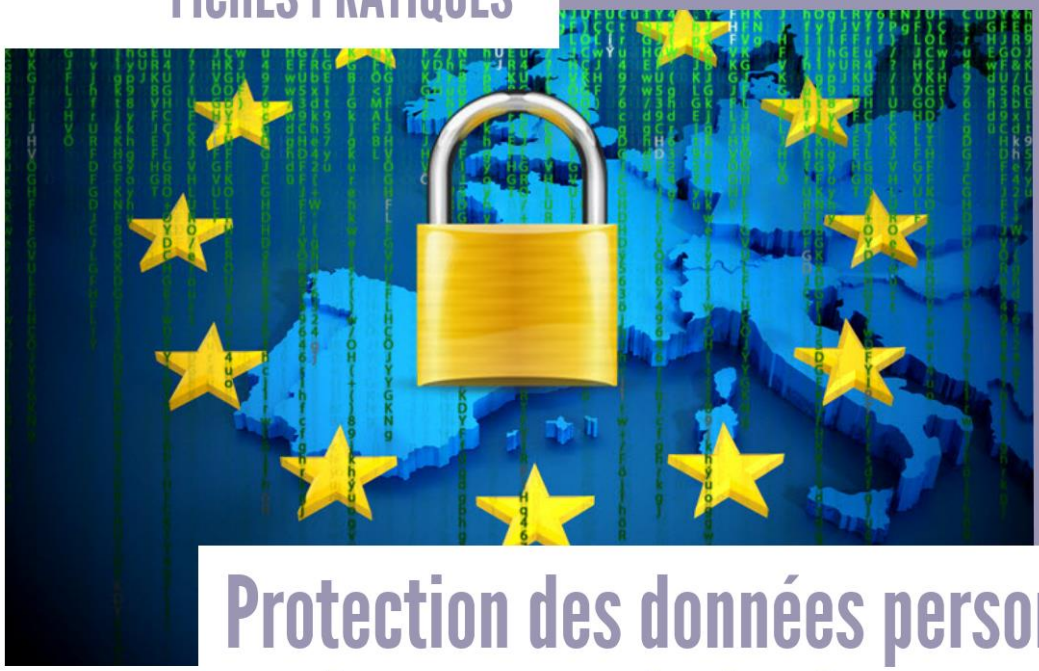
FICHES PRATIQUES



Protection des données personnelles : quels sont vos droits ?

Entré en vigueur le 25 mai 2018 dans toute l'Union européenne, le Règlement général sur la protection des données (RGPD) instaure un nouveau cadre juridique pour la protection des données personnelles. Qu'est-ce que cela change pour vous ?

En France, la protection des données personnelles est encadrée par la loi du 6 janvier 1978 dite « Informatique et libertés ».

La loi du 20 juin 2018 relative à la protection des données personnelles a modifié la loi « Informatique et Libertés » pour l'adapter aux dispositions du Règlement général sur la protection des données (RGPD), applicable partout en Europe depuis le 25 mai 2018.

Ce nouveau cadre juridique renforce les droits de chaque citoyen européen sur la protection de ses données personnelles et responsabilise les acteurs traitant ces données.

A noter
En plus du RGPD, l'Union européenne a adopté la directive (UE) du 27 avril 2016 dite "Directive Police Justice" relative aux traitements de données personnelles en matière pénale. Ces deux textes constituent "le paquet européen" sur la protection des données.

Quel est le champ d'application du RGPD ?

Le RGPD s'applique aux entreprises, aux organismes publics et aux associations quelles que soient leur taille ou leur activité, dès lors qu'ils traitent de données personnelles de personnes physiques se trouvant sur le territoire de l'Union européenne. **Le critère d'applicabilité n'est donc pas celui du lieu d'établissement du responsable du traitement. Le RGPD s'applique également aux entreprises ayant leur siège en dehors de l'UE qui traitent les données de citoyens européens.**

À quoi correspondent les données à caractère personnel ?

Ce sont toutes les informations se rapportant à une personne physique **identifiée ou identifiable**.

Exemples :

- nom, prénom ;
- adresse personnelle ;
- adresse de courriel telle que prénom.nom@entreprise.com ;
- numéro de carte d'identité ;
- adresse de protocole internet (IP) ;
- cookie[1] ;
- données détenues par un hôpital ou un médecin, qui permettraient d'identifier de manière unique une personne.

Que recouvre le traitement des données ?

Par traitement des données, on entend toute opération effectuée sur des données à caractère personnel, de manière automatisée ou manuelle, comme, par exemple, la collecte, l'enregistrement, la conservation, la modification, la consultation, la diffusion ou l'effacement des données à caractère personnel.

Exemples :

- gestion du personnel et administration des salaires ;
- consultation d'une base de données de contacts contenant des données à caractère personnel ;
- envoi de courriels promotionnels ;
- publication/affichage d'une photo d'une personne sur un site internet ;
- conservation d'adresses IP ;
- enregistrement de vidéosurveillance.

Quels sont vos droits sur vos données personnelles ?

Vous avez le droit :

- de demander des informations sur le traitement de vos données à caractère personnel ;
- d'obtenir l'accès aux données à caractère personnel détenues à votre sujet ;
- de demander que les données à caractère personnel incorrectes, inexactes ou incomplètes soient corrigées ;
- de demander que les données à caractère personnel soient effacées lorsqu'elles ne sont plus nécessaires ou si leur traitement est illicite ;
- de vous opposer au traitement de vos données à caractère personnel à des fins de prospection ou pour des raisons liées à votre situation particulière ;
- de demander la limitation du traitement de vos données à caractère personnel dans des cas précis ;
- de récupérer vos données personnelles, dans un format utilisé et lisible par machine, pour un usage personnel ou pour les transférer à un autre organisme ;
- de demander que les décisions fondées sur un traitement automatisé qui vous concernent ou vous affectent de manière significative et fondées sur vos données à caractère personnel soient prises par des personnes physiques et non uniquement par des ordinateurs. Dans ce cas, vous avez également le droit d'exprimer votre avis et de contester lesdites décisions ;
- en cas de dommage matériel ou moral lié à la violation du RGPD, vous disposez d'un droit de recours. Vous pouvez déposer une réclamation auprès de la Commission nationale Informatique et libertés (CNIL) ou introduire une action collective en faisant notamment appel aux associations nationales agréées de défense des consommateurs.

Quelles sont les obligations des entreprises ?

Les entreprises ont l'obligation :

- de respecter le principe de protection des données personnelles et de la vie privée imposées par le règlement, dès la conception de tout projet ;
- de recenser les traitements qu'elles mettent en œuvre dans un registre des traitements ;
- d'être en capacité de prouver que les traitements de données à caractère personnel mis en œuvre respectent les règles applicables, notamment via l'adhésion à des codes de conduite et l'obtention d'une certification ;
- de notifier toute violation de données à caractère personnel par le responsable de traitement et le sous-traitant aux autorités et aux personnes concernées ;
- de réaliser une étude d'impact sur la vie privée pour les traitements à risque ;
- de désigner un délégué à la protection des données pour les organismes publics et les entreprises dont l'activité principale les amène à réaliser un suivi régulier et systématique des personnes à grande échelle ou encore des organismes qui traitent des données dites « sensibles » ou relatives à des condamnations pénales et infractions ;
- de s'assurer que les personnes sont informées, de manière claire et concise, de la durée de conservation des données, de l'existence de profilage, de leurs droits et des voies de recours disponibles ;

[1] Les cookies sont des traceurs de navigation pouvant permettre d'analyser la navigation, les déplacements et les habitudes de consultation ou de consommation

- de permettre aux personnes dont les données sont traitées d'exercer leurs droits (à l'oubli, à la portabilité des données, de limitation… etc.).

Pratiques abusives liées à la mise en conformité des entreprises au RGPD : comment s'en prémunir ?

Certaines sociétés profitent de l'entrée en vigueur du RGPD pour démarcher les professionnels (entreprises, administrations, associations), parfois de manière agressive, afin de vendre un service d'assistance à la mise en conformité au RGPD. Au regard de pratiques commerciales trompeuses constatées, la DGCCRF et la CNIL ont formulé plusieurs recommandations ayant pour but de :

- **vérifier l'identité des entreprises démarcheuses qui ne sont en aucun cas, contrairement à ce que certaines prétendent, mandatées par les pouvoirs publics pour proposer à titre onéreux des prestations de mise en conformité au RGPD ;**
- **vérifier la nature des services proposés : la mise en conformité au RGPD nécessite plus qu'un simple échange ou l'envoi d'une documentation. Elle suppose un vrai accompagnement, par un professionnel qualifié en protection des données personnelles, pour identifier les actions à mettre en place et assurer leur suivi dans le temps.**

Dans certains cas, il peut aussi s'agir de manœuvres pour collecter des informations sur une société en vue d'une escroquerie ou d'une attaque informatique.

Qui est chargé de contrôler la bonne application du règlement ?

Ce sont les autorités indépendantes de chaque Etat (en France, la CNIL) qui contrôlent l'application de la législation relative à la protection des données. Elles sont dotées de pouvoirs d'enquête et peuvent imposer des mesures correctrices, en cas d'infraction. Elles fournissent des conseils d'experts sur les questions liées à la protection des données et traitent les réclamations introduites relatives à des violations du Règlement général sur la protection des données et des législations nationales en la matière.

La CNIL, votre interlocuteur privilégié

Le RGPD consacre le mécanisme de "guichet unique". En cas de transfert de données personnelles hors de l'Union européenne, **la Commission nationale Informatique et libertés** est l'interlocuteur unique pour tous les établissements du responsable de traitement de données, y compris ceux situés en dehors de l'Union européenne. La CNIL rend des décisions valables dans toute l'UE : ce mécanisme facilite les recours des consommateurs, la CNIL demeurant l'unique interlocuteur des personnes résidant sur le territoire français.

Textes de référence

Règlement général sur la protection des données (RGPD)

Loi du 6 janvier 1978 dite « Informatique et libertés »

La loi du 20 juin 2018 relative à la protection des données personnelles

Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (version consolidée au 08 août 2018)

Liens utiles

CNIL

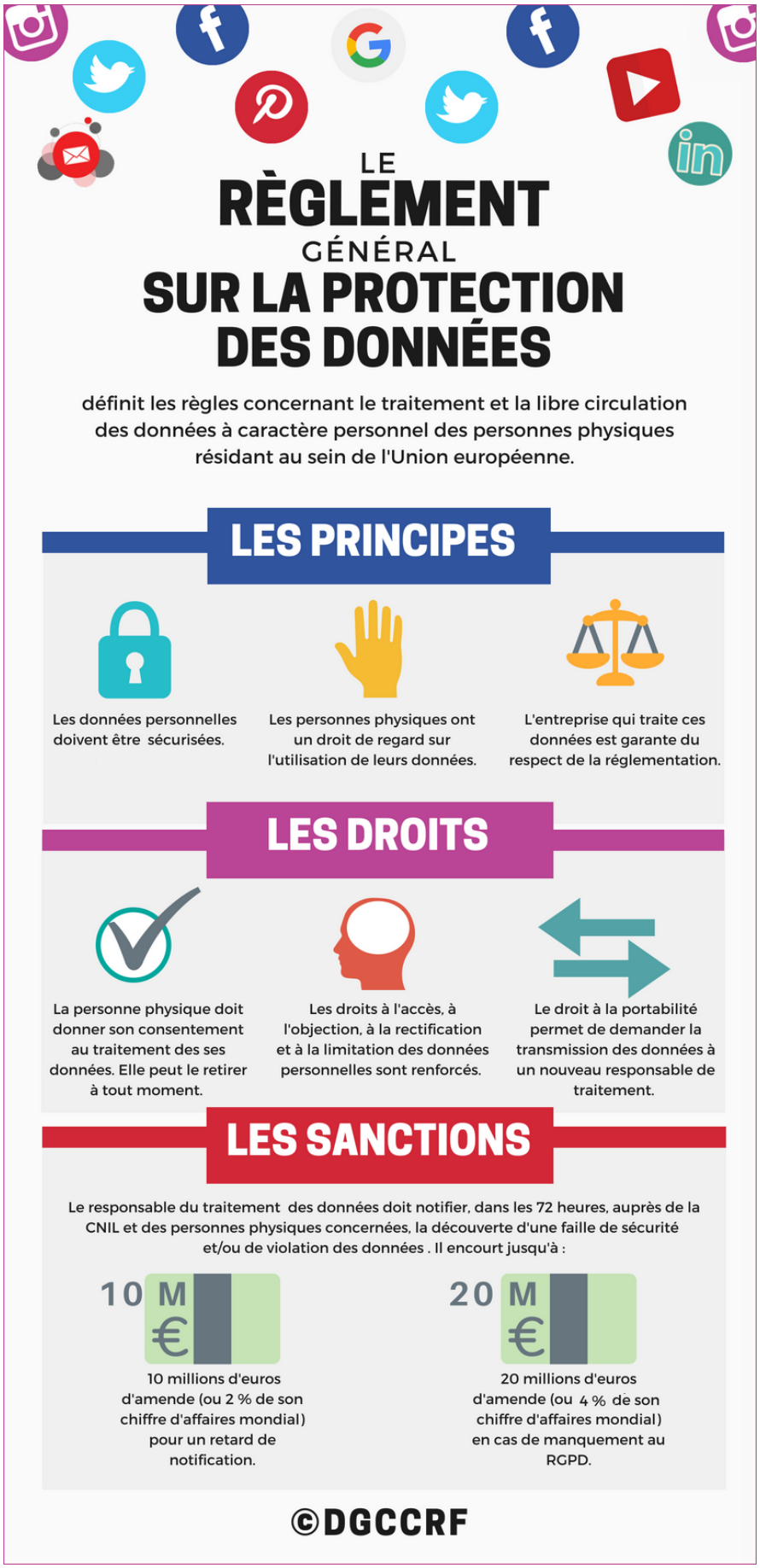
Réforme des règles de l'UE en matière de protection des données 2018 – Site Europa

Les éléments ci-dessus sont donnés à titre d'information. Ils ne sont pas forcément exhaustifs et ne sauraient se substituer aux textes officiels.

Vous avez rencontré un problème en tant que consommateur ?

Signalez-le sur www.signal.conso.gouv.fr, le site de la DGCCRF

Crédit photo : ©Fotolia/Pixabay


LE
RÈGLEMENT
GÉNÉRAL
SUR LA PROTECTION
DES DONNÉES
définit les règles concernant le traitement et la libre circulation des données à caractère personnel des personnes physiques résidant au sein de l'Union européenne.
LES PRINCIPES
Les données personnelles doivent être sécurisées.
Les personnes physiques ont un droit de regard sur l'utilisation de leurs données.
L'entreprise qui traite ces données est garante du respect de la réglementation.
LES DROITS
La personne physique doit donner son consentement au traitement des ses données. Elle peut le retirer à tout moment.
Les droits à l'accès, à l'objection, à la rectification et à la limitation des données personnelles sont renforcés.
Le droit à la portabilité permet de demander la transmission des données à un nouveau responsable de traitement.
LES SANCTIONS
Le responsable du traitement des données doit notifier, dans les 72 heures, auprès de la CNIL et des personnes physiques concernées, la découverte d'une faille de sécurité et/ou de violation des données . Il encourt jusqu'à :
10 M €
10 millions d'euros d'amende (ou 2 % de son chiffre d'affaires mondial) pour un retard de notification.
20 M €
20 millions d'euros d'amende (ou 4 % de son chiffre d'affaires mondial) en cas de manquement au RGPD.
©DGCCRF