Les sanctions en cas de non-respect du RGPD

Description

Depuis l'entrée en vigueur du règlement pour la protection générale des données personnelles (RGPD) en 2018, de nombreux organismes ont dû mettre en place un certain nombre de mesures afin d'être en conformité à la nouvelle réglementation relative au traitement des données personnelles. Lorsque les organismes ne respectent pas ces mesures ils s'exposent à des sanctions plus ou moins lourdes en fonction de la gravité de la violation.

Obtenir un devis gratuit RGPD

Comment un organisme est-il sanctionné en cas de non-respect du RGPD ?

Un organisme peut être sanctionné au titre du non-respect du RGPD dans le cadre d'une plainte ou d'un contrôle effectué par la CNIL.

Le dépôt d'une plainte ou d'un signalement auprès de la CNIL

Toute personne est en mesure de déposer une **plainte** ou un **signalement** auprès de la CNIL dans les cas suivants :

- Lorsqu'elle n'arrive pas à exercer ses droits relatifs à la loi « Informatique et Libertés »
- Lorsqu'elle souhaite signaler une atteinte aux règles de protection des données personnelles par un organisme public ou privé

Pour adresser une **réclamation**, elle peut se rendre sur le site internet de la CNIL par le téléservice de plainte en ligne pour certains cas. Elle peut également contracter l'autorité de contrôle par courrier postal en écrivant à :

« CNIL – SERVICES DES PLAINTES – 3 PLACE DE FONTENOY – TSA 80715 – 75334 PARIS CEDEX 07 ».

La personne doit joindre à sa réclamation **tous les documents** pouvant attester des faits décrits.

Bon à savoir : S'agissant des réclamations, les délais de traitement sont souvent très importants du fait du grand nombre de **saisines** reçues par la CNIL et dépend également de la **complexité du dossier.**

Le contrôle effectué par la CNIL

La CNIL peut également être amenée à **sanctionner les responsables de traitement** suite à un contrôle effectué à posteriori. Ce dernier vise à vérifier la mise en œuvre concrète de la loi et peut s'opérer auprès de tout organisme traitant des données à **caractère personnel** dès lors :

- Que l'organisme visé par le contrôle est établi en France
- Que le traitement concerne des résidents français

Ce contrôle peut être effectué par la CNIL en coopération avec d'autres autorités de protection des données si l'organisme dispose de **plusieurs établissements** dans l'UE ou traite les données personnelles de personnes dans l'UE.

Le RGPD permet également à la CNIL d'effectuer des vérifications auprès de **prestataires sous-traitants** chargés de la mise en œuvre d'un traitement pour le compte d'un organisme.

Ainsi ces contrôles peuvent avoir lieu du fait :

- Du programme annuel des contrôles
- De l'initiative de la CNIL
- D'un contrôle des dispositifs de vidéoprotection
- De la procédure de contrôle clôturée, des mises en demeure et des sanctions

Quelles sont les sanctions en cas de non-respect du RGPD ?

Les organismes contrevenant aux règles imposées par le RGPD relatives au traitement de données personnelles s'exposent à des **sanctions de diverses nature** :

- Administrative
- Pénales

- Versement de dommages et intérêts
- Déficit d'image

Les sanctions administratives

La CNIL peut prononcer plusieurs types de sanctions administratives à l'encontre de l'organisme contrevenant, dont la mise en œuvre peut être graduelle :

- Mesures correctrices
- Sanctions administratives
- Sanctions pénales
- Versement de dommages-intérêts et publicité de la violation

Les mesures correctrices

L'article 58 du RGPD offre aux autorités de contrôle le pouvoir d'adopter des **mesures correctrices**. Celles-ci peuvent être prononcées en complément des **sanctions administratives**. Cependant, du fait de leur caractère dissuasif, elles ont tendance à être prises avant les amendes liées au RGPD.

Les sanctions sont donc graduelles en fonction de la **gravité de la violation** du RGPD constatée. Ainsi, la CNIL est en mesure de délivrer :

- un avertissement ou une mise en demeure de l'entreprise fautive avec rappel du devoir de mise en conformité des traitements de données sensibles au RGPD
- une injonction de cesser la violation
- une limitation ou suspension temporaire des traitements de données
- des sanctions administratives en cas de non-respect des règles du RGPD après injonction vaine de l'autorité de contrôle

Bon à savoir : Les sanctions prévues par le RGPD ne sont donc en réalité que les **ultimes sanctions** auxquelles les organismes s'exposent s'ils ne suivent pas les injonctions de la CNIL.

Les sanctions administratives

La CNIL peut sanctionner le non-respect du RGPD par des **sanctions administratives**. Ces dernières doivent être **proportionnées et dissuasives**. Elles tiennent compte des critères suivants :

- La gravité et la durée de la violation

- Le degré de coopération
- Les mesures prises pour atténuer le dommage subi par la personne concernée

Ainsi, l'autorité de contrôle peut également fixer des amendes à régler. Leur montant dépend de la violation constatée :

- 10 millions d'euros ou 2% du chiffre d'affaires : c'est le cas lorsque les entreprises violent les conditions imposées concernant le recueil du consentement des enfants ou si elles ne respectent pas le principe du privacy by design ou du privacy by default.
- 20 millions d'euros ou 4% du chiffre d'affaires : c'est le cas lors d'une violation des principes de traitement des données ou le non-respect des conditions de licéité du traitement.

Bon à savoir : Afin d'éviter de telles conséquences, des formations RGPD sont proposées aux entreprises. Cela leur permet ainsi de **comprendre les enjeux** du RGPD et de **se mettre en conformité**.

Les sanctions pénales

Les Etats membres peuvent mettre en place des **sanctions supplémentaires** en cas de violation du RGPD, grâce à l'article 84 du RGPD.

En France, l'article 226-21 du code pénal prévoit une sanction en cas de **détournement de la finalité** lors du traitement des **données personnelles** pouvant aller jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende.

Le versement de dommages et d'intérêts et le déficit d'image

Enfin, outre les sanctions précédemment listées, la violation du RGPD peut également entrainer d'autres conséquences telles que :

- La publicité de la violation commise par l'organisme : la CNIL peut en effet obliger l'organisme ou l'entreprise contrevenante à publier la sanction dont elle a fait l'objet.
- La condamnation au versement de dommages et intérêts : les personnes victimes de la violation du RGPD peuvent subir un dommage matériel ou moral. Dans ce cas, l'organisme contrevenant pourra se voir condamner au versement de dommage-intérêts en réparation du préjudice subi.

Attention : Le versement de **dommages et intérêts** ne se substitue pas aux

sanctions administratives et pénales mais vient s'y ajouter.

FAQ

Quelles sont les sanctions prévues en cas de violation du RGPD ?

Le RGPD prévoit des sanctions administratives et pénales en cas de violation du règlement. Il permet également aux Etats membres de prévoir des sanctions pénales. La France prévoit notamment des sanctions à l'article 226-21 du code pénal.

Qui peut sanctionner les organismes en cas de violation du RGPD ?

Le RGPD confère aux autorités telles que la CNIL un pouvoir de sanction. Celle-ci doit ainsi veiller au respect des principes du RGPD. Dans le cas contraire, elle peut prononcer des mesures correctrices telles qu'un avertissement. Si la violation persiste, des sanctions pécuniaires seront alors prononcées.

Comment éviter les sanctions liées au RGPD ?

Afin d'éviter toutes sanctions, les responsables de traitement sont dans l'obligation de se mettre en conformité avec le RGPD. Pour cela, ils doivent veiller à respecter plusieurs obligations et principes, tels que la licéité du traitement ou la minimisation des données. Ils doivent également respecter les droits conférés aux personnes dont les données sont traitées.