Sensibilisation au RGPD

dpo@groupeastek.fr

C2 - DIFFUSION CONTRÔLÉE - 09/02/2021 - SMI-000574-DOC

SENSIBILISATION RGPD

Le Règlement Général de Protection des Données (RGPD) est un texte réglementaire européen qui impose l'encadrement du traitement des données personnelles de manière identique sur tout le territoire de l'Union Européenne. Entré en vigueur le 25 mai 2018, il s'inscrit dans la continuité de la loi Informatique et Libertés de 1978 établissant les règles sur la collecte et l'utilisation des données sur le territoire français.

Imposé par l'article 39 du RGPD, l'entreprise doit s'assurer que ses salariés sont sensibilisés :

- aux droits et obligations des personnes ;
- au comportement à adopter, au rôle et aux responsabilités de chacun.

QU'EST CE QUE LE RGPD

Dans un contexte où les données sont de plus en plus nombreuses du fait de la digitalisation, il n'est pas toujours aisé de savoir ce que deviennent nos données collectées sur les outils numériques. En effet, l'utilisation qui est faite des données personnelles est déterminante pour le respect de notre vie privée. Aussi, les enjeux de la sécurisation des données sont devenus de plus en plus importants et ont donc conduit à la recherche d'un meilleur encadrement afin que les personnes puissent garder la maîtrise des informations les concernant.

C'est pourquoi, le Règlement Général à la Protection des Données vise à mettre **en place un cadre juridique** adapté aux nouvelles technologies qui renforce notamment le contrôle des citoyens de l'utilisation qui est faite de leurs données.

Toute structure qui effectue de la collecte et/ou du **traitement de données personnelles** est concernée par le RGPD quelque soit son secteur d'activité ou sa taille dès lors qu'elle est établie en UE et/ou que son activité concerne des résidents européens.

Par ailleurs, ce règlement harmonise également les règles de protection à l'ensemble du territoire de l'Union Européenne. Au-delà, des règles particulières sont prévues en cas de transfert de données hors de l'Union Européenne.

OBJECTIFS DU RGPD

Renforcement des droits des personnes

Les personnes concernées par les données sont au cœur du RGPD. Le règlement renforce la maîtrise de leurs informations par une plus forte exigence de leur consentement, un droit à l'information plus étendu et plus précis et par l'introduction de nouvelles prérogatives.

Responsabilisation des acteurs traitant des données

Auparavant, la protection des données reposait sur une logique de déclaration à la CNIL. Désormais, le RGPD impose la responsabilisation des acteurs intervenant dans le traitement des données personnelles. Ces acteurs doivent être en mesure de démontrer qu'ils sont en conformité avec les règles imposées.

Uniformisation de la réglementation

Le RGPD étant un texte européen, la règlementation a donc vocation à s'appliquer sur l'ensemble de l'Union Européenne de manière uniforme. Par ailleurs, le RGPD prévoit aussi la protection des données dès qu'un transfert est opéré hors de l'Union Européenne en exigeant une protection au moins équivalente.

DÉFINITIONS

Donnée personnelle

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ». Toute donnée qui vise une identification **directe ou indirecte** est une donnée personnelle.

Identification directe	Identification indirecte
Un nom, un prénom etc.	Un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, ainsi que tout élément spécifique propre à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi **la voix** ou **l'image.**

L'identification d'une personne physique peut être réalisée :

- **à partir d'une seule donnée** (exemple : numéro de sécurité sociale, ADN)
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

DÉFINITIONS

Donnée sensible

Parmi les données personnelles, certaines bénéficient d'une protection plus particulière : il s'agit des données sensibles. Toute collecte ou consultation de ces données est par principe interdit car elles relèvent de l'intimité de la vie privée.

Constitue des **données sensibles** les données relatives aux éléments suivants :

- Santé / vie sexuelle
- Données génétiques ou biométriques
- Appartenance syndicale
- Convictions religieuses ou philosophiques
- Origine raciale ou ethnique
- Opinions politiques

DÉFINITIONS

Traitement

Le traitement est « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel ».

Informatisés mais pas uniquement :

Un traitement de données à caractère personnel peut être informatisé ou non. Un fichier papier organisé selon un plan de classement, des formulaires papiers nominatifs ou des dossiers de candidatures classés par ordre alphabétique ou chronologique sont aussi des traitements de données personnelles.

Des fichiers mais pas seulement :

Un traitement n'est donc pas uniquement un fichier, une base de données ou un tableau Excel. Il peut s'agir aussi d'une installation de vidéosurveillance, d'un système de paiement par carte bancaire ou de reconnaissance biométrique, d'une application pour smartphone, etc.. Des traitements apparaissent et évoluent selon les innovations technologiques.

En revanche, un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « communication@groupeastek.fr») n'est pas un traitement de données personnelles.

Liste non limitative de traitements : *la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.*

DÉFINITIONS

Responsable traitement et sous traitant

LE RESPONSABLE DE TRAITEMENT (RT)

Il est la personne morale (entreprise, commune, etc.) ou physique qui **détermine les finalités et les moyens d'un traitement**, c'est-à-dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

Par exemple, Astek est le responsable de traitement des données personnelles collectées auprès de ses salariés.

LE SOUS-TRAITANT (ST)

Il est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel **pour le compte du responsable du traitement**.

Par exemple, lors d'une intervention chez un client (SNCF, Orange, Amadeus…), Astek est le sous-traitant de son client concernant les données personnelles traitées dans le cadre des prestations effectuées.

→ Le responsable de traitement et le sous traitant sont tous les deux des acteurs intervenant dans le traitement des données.

CADRE JURIDIQUE

Les droits des personnes dont les données sont collectées

Afin d'encadrer l'utilisation qui est faite des données, différents droits sont accordés aux personnes concernées par les traitements. Le RGPD n'a pas seulement facilité le recours aux droits préexistants mais a aussi introduit deux nouveaux droits.

LES DROITS RENFORCÉS :

Droit d'accès	Droit d'obtenir des copies de ses données, exercé auprès du responsable de traitement.
Droit de rectification	Droit de corriger et compléter les données personnelles collectées.
Droit d'opposition	Droit de s'opposer au traitement pour un motif légitime. Néanmoins, l'organisme peut refuser de faire droit à la demande dans plusieurs situations notamment dans le cadre d'une obligation légale ou de la bonne exécution d'un contrat. *Ex : contrat de travail.*
Droit à l'effacement ou l'oubli	Droit de demander la suppression de ses données (traitement illicite, données non nécessaires au regard des objectifs fixés, etc...).

CADRE JURIDIQUE

Les droits des personnes dont les données sont collectées

LES DEUX NOUVEAUX DROITS :

Le droit à la limitation du traitement

En cas de contestation de l'exactitude des données ou d'opposition, l'organisme dispose d'un certain délai pour examiner la demande. Pendant ce délai, ce droit à la limitation permet de demander à l'organisme de geler l'utilisation des données c'est-à-dire les conserver mais ne pas les utiliser.

Le droit à la portabilité

Ce droit **permet à une personne** :

- **de récupérer les données la concernant** traitées par un organisme, **pour son usage personnel**, et de les stocker sur un appareil ou un cloud privé par exemple. Ce droit permet de gérer plus facilement et par soi-même ses données personnelles.
- **de transférer ses données personnelles d'un organisme à un autre**. Les données personnelles peuvent ainsi être transmises à un nouvel organisme :
  - soit par la personne elle-même,
  - soit directement par l'organisme qui détient les données, si ce transfert direct est « techniquement possible ».

CADRE JURIDIQUE

Cas particulier du transfert de données personnelles hors UE

Le RGPD vise à créer une bulle de protection autour des données personnelles. Ainsi, lorsqu'un transfert de données personnelles hors UE est envisagé plusieurs points de vigilance doivent être respectés.

1. PAYS ADÉQUATS

Si le pays destinataire est « adéquat » c'est-à-dire **qu'il offre une protection de niveau identique que celle de l'UE** alors aucun encadrement spécifique n'est exigé.

2. GARANTIES APPROPRIÉES

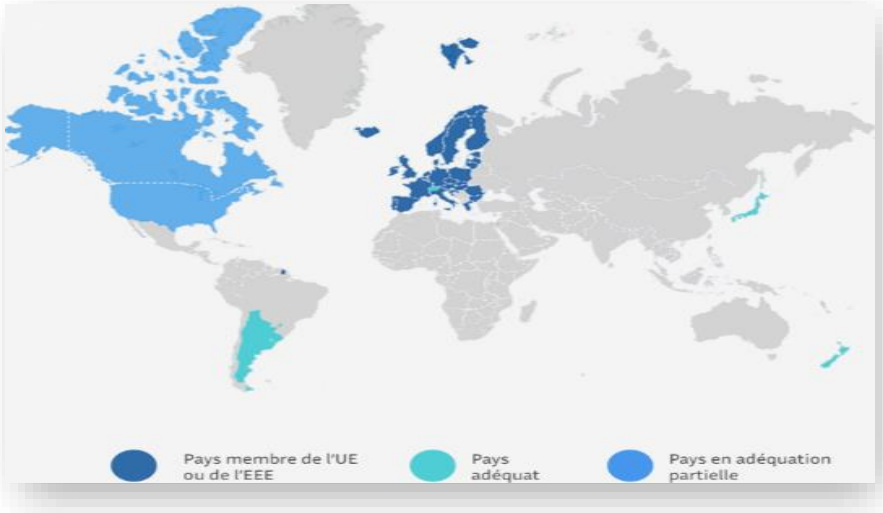
À défaut, le transfert de données n'est possible que si des garanties ont été mises en place comme des règles d'entreprises contraignantes au sein d'un même groupe (BCR) ou des clauses contractuelles types élaborées par la Commission Européenne.

3. AUTORISATION

En l'absence de ces garanties, le transfert peut être effectué après autorisation préalable de l'Autorité compétente.

4. DÉROGATION

Enfin, par exception, le transfert peut être réalisé en l'absence de telles garanties dans des cas précis et limitativement énumérés par le RGPD (art 47).



Ces règles ont vocation à s'appliquer même au sein d'un même groupe. Par exemple, lorsqu'un transfert de données personnelles est envisagé entre Astek et Astek Mauritius, il est nécessaire de s'assurer que ce transfert présente des garanties appropriées.

CADRE JURIDIQUE

Le Délégué à la Protection des Données

Le Délégué à la Protection des Données est un acteur mis en place par le RGPD afin de favoriser la mise en conformité à ce règlement. Il s'agit du point de contact essentiel en matière de données personnelles et des droits s'y attachant.

Le DPO a plusieurs missions :

- Informer et conseiller le responsable de traitement et le sous traitant de leurs obligations
- Contrôler le respect du RGPD au sein de l'organisme et gérer toute violation
- Coopérer avec la CNIL

Afin de faire remonter un incident ou d'exercer vos droits sur vos données personnelles vous pouvez contacter :

- Chez Astek : dpo@groupeastek.fr
- Chez votre client : demandez à votre interlocuteur client le ou les contacts existants

CADRE JURIDIQUE

Violation de données

CONTESTATION

Il y a violation de donnée dès lors qu'il y a « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données » Art. 4 RGPD

RÉACTION

Le sous-traitant doit notifier au responsable de traitement toute violation des données dans les meilleurs délais. Le responsable de traitement doit notifier la violation de données à la CNIL si possible dans les 72h après en avoir connaissance.
Le responsable de traitement doit également, le cas échéant, informer les personnes concernées de la violation des données.
Tout collaborateur d'Astek doit signaler un incident portant sur des données personnelles directement par mail en utilisant l'adresse suivante : dpo@groupeastek.fr et, le cas échéant informer ses interlocuteurs chez le client.

CADRE JURIDIQUE

Sanctions

Pour garantir le respect des obligations liées à la protection des données personnelles, le RGPD renforce les sanctions en cas de non-conformité.

Ainsi, la CNIL peut prononcer des **sanctions graduées** selon le type de violation :

- Avertissement contre le responsable de traitement ou le sous traitant
- Mise en demeure de respecter le RGPD
- Rectification ou effacement de données personnelles
- Amende administrative (soit 2% du CA annuel mondial ou 10 millions d'euros, soit 4% du CA annuel mondial ou 20 millions d'euros) :

Exemple : la CNIL a prononcé une sanction de 400 000 euros contre une agence immobilière pour avoir insuffisamment protégé les données des utilisateurs de son site web et mis en œuvre des modalités de conservation des données inappropriées.

Des **sanctions pénales** peuvent également être prononcées.

Exemple : détournement de la finalité des données personnelles : 300 000 euros d'amende et 5 ans d'emprisonnement.

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

La Commission Nationale de l'Informatiques et Liberté est chargée de garantir le respect du RGPD en accompagnant les professionnels à la conformité et par le pouvoir d'information, de conseil et de sanction dont elle dispose.

ASTEK
GROUP

Merci pour votre attention