LE RGPD

Le RGPD est un règlement européen qui vise à protéger les données personnelles des citoyens de l'Union européenne1234. Le RGPD renforce les droits des personnes concernant l'utilisation de leurs données, responsabilise les acteurs qui traitent ces données et crédibilise la régulation grâce à une coopération entre les autorités de protection des données54. Le RGPD est entré en vigueur le 25 mai 2018 et constitue une avancée majeure et unique au niveau mondial34.
Qui est concerné par le RGPD ?
Tout organisme quels que soient sa taille, son pays d'implantation et son activité, peut être concerné.

En effet, le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :

qu'elle est établie sur le territoire de l'Union européenne,
ou que son activité cible directement des résidents européens.
Par exemple, une société établie en France, qui exporte l'ensemble de ses produits au Maroc pour ses clients moyen-orientaux doit respecter le RGPD.

De même, une société établie en Chine, proposant un site de e-commerce en français livrant des produits en France doit respecter le RGPD.

Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organismes.

Ainsi, si vous traitez ou collectez des données pour le compte d'une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées.

LES DERNIERES CONDANATIONS CNIL

- 1 - NE COLLECTEZ QUE LES DONNÉES VRAIMENT NÉCESSAIRES POUR ATTEINDRE VOTRE OBJECTIF

  Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.

  Le principe de finalité limite la manière dont vous pourrez utiliser ou réutiliser ces données dans le futur et évite la collecte de données « au cas où ».

  Le principe de minimisation limite la collecte aux seules données strictement nécessaires à la réalisation de votre objectif.

  Comment définir une finalité ?

2 - SOYEZ TRANSPARENT

Les individus doivent conserver la maîtrise des données qui les concernent. Cela suppose qu'ils soient clairement informés de l'utilisation qui sera faite de leurs données dès leur collecte. Les données ne peuvent en aucun cas être collectées à leur insu. Les personnes doivent également être informées de leurs droits et des modalités d'exercice de ces droits.

Comment informer les personnes et assurer la transparence ?

3 - ORGANISEZ ET FACILITEZ L'EXERCICE DES DROITS DES PERSONNES

Vous devez organiser des modalités permettant aux personnes d'exercer leurs droits et répondre dans les meilleurs délais à ces demandes de consultation ou d'accès, de rectification ou de suppression des données, voire d'opposition, sauf si le traitement répond à une obligation légale (par exemple, un administré ne peut s'opposer à figurer dans un fichier d'état civil). Ces droits doivent pouvoir s'exercer par voie électronique à partir d'une adresse dédiée.

Comment respecter les droits des personnes ?

4 - FIXEZ DES DURÉES DE CONSERVATION

Vous ne pouvez pas conserver les données indéfiniment.

Elles ne sont conservées en « base active », c'est-à-dire la gestion courante, que le temps strictement nécessaire à la réalisation de l'objectif poursuivi. Elles doivent être par la suite détruites, anonymisées ou archivées dans le respect des obligations légales applicables en matière de conservation des archives publiques.

Comment concilier les durées de conservation et les archives ?

5 - SÉCURISEZ LES DONNÉES ET IDENTIFIEZ LES RISQUES

Vous devez prendre toutes les mesures utiles pour garantir la sécurité des données : sécurité

physique ou sécurité informatique, sécurisation des locaux, armoires et postes de travail, gestion stricte des habilitations et droits d'accès informatiques. Cela consiste aussi à s'assurer que seuls les tiers autorisés par des textes ont accès aux données. Ces mesures sont adaptées en fonction de la sensibilité des données ou des risques qui peuvent peser sur les personnes en cas d'incident de sécurité.

Comment assurer la sécurité des données ?

6 - INSCRIVEZ LA MISE EN CONFORMITÉ DANS UNE DÉMARCHE CONTINUE

La conformité n'est pas gravée dans le marbre et figée.
Elle dépend du bon respect au quotidien par les agents, à tous les niveaux, des principes et mesures mis en oeuvre.
Vérifiez régulièrement que les traitements n'ont pas évolué, que les procédures et les mesures de sécurité mises en place sont bien respectées et adaptez-les si besoin.

Date	Type d'organisme	Manquements principaux / Thème	Décision adoptée
29/12/2023	SOCIETE DE SITES EN LIGNE DE JEUX-CONCOURS ET TESTS PRODUITS	Obligation de traiter les données de façon licite (prospection commerciale) Registre des activités de traitement	Amende de 75 000 euros et injonction
29/12/2023	SOCIETE PROPOSANT DES SERVICES DE TELECOMUNICATION	Information des personnes et transparence Consentement des personnes (cookies)	Amende de 10 millions d'euros
29/12/2023	SOCIETE PERMETTANT D'EFFECTUER DES PAIEMENTS EN LIGNE	Durée de conservation Information des personnes et transparence Défaut de sécurité des données Consentement des personnes (cookies	Amende de 105 000 euros
29/12/2023	SOCIETE DE CONSEIL EN SYSTEMES ET LOGICIELS INFORMATIQUES	Interdiction pour le sous-traitant de recruter un autre sous-traitant sans l'autorisation du responsable de	Amende de 100 000 euros

		traitement Défaut de sécurité des données	

DEFINITION DES PERSONNES PHISIQUES POURLE CNIL

Une personne physique peut être identifiée :

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

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

- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association).

- Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

  Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :

  si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
  si les informations sont manifestement rendues publiques par la personne concernée ;
  si elles sont nécessaires à la sauvegarde de la vie humaine ;
  si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL ;
  si elles concernent les membres ou adhérents d'une association ou d'une organisation .

  Les données sensibles forment une catégorie particulière des données personnelles.

  Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

  Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :

  si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;

  si les informations sont manifestement rendues publiques par la personne concernée ;

si elles sont nécessaires à la sauvegarde de la vie humaine ;

si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL ;

si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :

si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
si les informations sont manifestement rendues publiques par la personne concernée.

CONCLUSION

Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :

si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
si les informations sont manifestement rendues publiques par la personne concernée