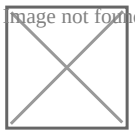
Image not found or type unknown



FICHE PRATIQUE "Données personnelles RGPD" : Êtes-vous vraiment en conformité ?

Fiche pratique publié le **12/05/2022**, vu **1668 fois**, Auteur : Mounia BELKACEM

RGPD : Quels sont les réflexes à avoir pour s'assurer d'être en conformité ? Êtes-vous vraiment en conformité ? Vérifiez si vous avez eu les bons réflexes lors de la mise en place de votre politique RGPD !

Afin d'appréhender ce qu'est le Règlement Général sur la Protection des Données personnelles (RGPD), il convient de comprendre ce qu'est une donnée à caractère personnel.

Une donnée à caractère personnel est un élément d'information qui sert de base à l'identification d'un individu, personne physique vivante, identifiée ou identifiable.

L'omniprésence de l'internet, sa nécessité et son immédiateté sont à l'origine d'une volonté d'encadrer l'utilisation des données à caractère personnel appartenant à chaque individu.

A ce jour, l'internet fait partie du quotidien des milliards d'individus sur Terre et son développement infini a conduit à la nécessité de poser les jalons d'un premier cadre juridique, en France.

Ce cadre juridique a débuté avec la loi informatique et liberté du 6 janvier 1978 créant également la Commission Nationale de l'Informatique et des Libertés, visant à faire respecter la loi susmentionnée.

La protection des données personnelles n'est donc pas une nouveauté.

Plusieurs textes notamment européens sont intervenus et ce sont largement inspirés de la loi française du 6 janvier 1978 mais le texte phare est le Règlement Général sur la Protection des Données 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et entré en vigueur le 23 mai 2018.

Ce règlement encadre et contrôle les traitements des données à caractère personnel des citoyens faisant partie des états-membres de l'Union Européenne.

Cette protection a été jugée nécessaire à l'encontre des entreprises qui, à l'aide de l'internet, n'hésitent pas vendre, acheter, et donc donner une dimension pécuniaire aux données personnelles des individus.

La valorisation monétaire de ces données à caractère personnel a provoqué des dérives qu'il a fallu contrer par une protection renforcée et ciblée.

Par conséquent, aujourd'hui, et à l'aune d'une intelligence artificielle grandissante, il était plus que

nécessaire de consolider les règles et développer des mesures visant à protéger le traitement des données personnelles des personnes physiques à l'encontre des entreprises et entités personnes morales.

Le respect de ce texte est devenu un sujet essentiel pour les personnes morales dans le cadre de leur activité.

Il importe donc de s'interroger sur les réflexes à adopter pour être en conformité du RGPD et comment s'y conformer.

Les réflexes à adopter en tant que personne morale traitant les données personnelles des citoyens européens

Par réflexe, il faut entendre les réflexions principales à avoir pour s'assurer de respecter les règles du RGPD, avant de s'interroger sur le « comment » s'assurer de ce respect.

Premier réflexe : Avoir à l'esprit que la personne morale ne peut collecter et traiter que les données strictement nécessaires à son activité.

Il faut donc un but déterminé et limité au strict nécessaire pour le développement de son activité.

Par exemple, une entreprise qui vend des meubles n'a aucun intérêt à solliciter le numéro de sécurité sociale de l'individu. En revanche, s'il doit procéder à une livraison de meuble, la collecte de son adresse postale personnelle sera nécessaire pour livrer le bien.

Deuxième réflexe : L'individu doit avoir la possibilité de maîtriser le traitement de ses données personnelles. Cette maîtrise passe par une transparence totale de l'entreprise sur : où trouver ces données ? Comment solliciter leur modification ou suppression ? Quels sont leurs droits et modalités d'exercice de ces droits ? A qui s'adresser ?

La transparence de ces informations passe par la facilité accordée à l'individu de maîtriser le traitement de ses données à caractère personnel.

Troisième réflexe : Il faut fixer un délai strict de conservation des données à caractère personnel. Il n'est pas autorisé, ni même nécessaire de conserver les données à caractère personnel d'un individu plus de temps que nécessaire à l'activité de l'entreprise.

Quatrième réflexe : Il faut s'interroger sur les moyens de conservation sécurisés des données personnelles. Cela passera par une sécurisation physique, informatique ou par tout autre moyen visant à protéger les données personnelles des citoyens européens. Il en va de la responsabilité de l'entreprise de protéger les données qu'elle aura collectées.

Cinquième réflexe : Il faut prendre en compte l'évolution de la collecte des données à caractère personnel et continuellement mettre à jour les mesures mises en œuvre afin de protéger strictement ces données.

Copyright © 2025 Légavox.fr - Tous droits réservés

Dès lors que ces réflexions sont adoptées par l'entreprise, il appartient de se poser la question du « comment » assurer cette conformité au RGPD.

Comment se mettre en conformité ?

Maintenant que l'entreprise a établi son plan d'action en mettant en exergue les réflexes nécessaires à la protection des données personnelles, il faut qu'elle le concrétise.

A ce titre, la CNIL a développé ce passage à l'action en 4 étapes : .

- Première étape du plan d'action : Constituer un registre permettant d'identifier les activités principales de l'entreprise, les objectifs à atteindre, les raisons du traitement de certaines données personnelles et l'identification précise des données qui seront collectées.
- Deuxième étape du plan d'action : Catégoriser les données qui seront traitées par l'entreprise en se demandant toujours si elles sont nécessaires et comment l'individu peut y accéder et exercer ses droits dessus.
- Troisième étape du plan d'action : Elaborer le support sur lequel il y aura les mentions nécessaires à l'information des personnes physiques que ce soit concernant l'objectif du traitement de leurs données, le temps de conservation, comment elles sont traitées et comment ces individus peuvent maîtriser leur traitement.
- Quatrième étape du plan d'action : Prendre les mesures nécessaires pour protéger les données personnelles en passant par l'utilisation d'un antivirus performant, une protection des logiciels utilisés, des mots de passe sécurisés, un chiffrage des données et tout autre moyen visant à éviter un quelconque risque de failles de sécurité.

Lorsque la protection n'est pas informatique mais physique, il en va de l'entreprise de prendre les mesures nécessaires pour assurer cette protection telles que la présence en continu de vigiles, caméras de surveillance et autre mesure.

Il appert évident que le risque zéro n'existe pas mais il en va de la responsabilité de l'entreprise d'adopter ces réflexes, de les mettre en œuvre et surtout de les développer en permanence afin de protéger au mieux les données à caractère personnel des individus des états membres.

A défaut, si l'entreprise n'assure pas une protection des données à caractère personnel qu'elle collecte et traite, elle risque des sanctions pécuniaires pouvant s'élever à 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires annuel mondial.

En outre, ces sanctions peuvent être rendues publiques ce qui nuira lourdement à l'entreprise défaillante.

Enfin, la CNIL est compétente pour :

- Prononcer un rappel à l'ordre ;
- Enjoindre l'entreprise à se mettre en conformité au RGPD et de satisfaire aux demandes des personnes physiques sollicitant l'exercice de certains droits ;
- Limiter ou arrêter le traitement de données personnelles ;

Copyright © 2025 Légavox.fr - Tous droits réservés

- Suspendre les flux des données personnelles ;
- Prononcer une amende administrative.

Les entreprises ont donc tout intérêt à adopter les bons réflexes et surtout à les concrétiser de sorte à être en conformité avec le RGPD.

https://pistrislawfirm.com/

Copyright © 2025 Légavox.fr - Tous droits réservés