

Résumé du règlement RGPD / DPRG (Règlement Général de Protection des Données ou Data Protection Regulation General)

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel des résidents de l'Union Européenne et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Ses objectifs

Renforcer les droits des personnes (pour les résidents européens.), notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
Responsabiliser les acteurs traitant des données (responsables de traitement et soustraitants) ;
Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

Étapes

Le Règlement sera applicable à partir du 25 mai 2018 dans tous les pays de l'Union Européenne. Il s'applique à toutes les entreprises (y compris leurs comités d'entreprise), les administrations et les associations, qui traitent des données à caractère personnel. Les fichiers déjà mis en oeuvre à cette date devront, d'ici là, être mis en conformité avec le Règlement.

Responsabilités

un représentant légal désigné

Le représentant légal de votre structure est le point de contact de l'autorité. Il a mandat pour « être consulté en complément ou à la place du responsable du traitement sur toutes les questions relatives aux traitements ».

des sous-traitants respectueux du RGPD

Le sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière d'accountability. Il a notamment une obligation de conseil auprès du responsables de traitement pour la conformité à certaines obligations du règlement (analyse d'impact, failles, sécurité, destruction des données, contribution aux audits).

Sécurité et notifications de violation

Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements.

Sécurité et confidentialité

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.

des obligations de déclaration de violation auprès de la CNIL

Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données la violation dans les 72 heures. L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.