RGPD

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

EN DOUZE POINTS

Des droits renforcés et de nouveaux droits consacrés

Droit à l'oubli, à la portabilité, à la limitation du traitement...

La nomination d'un Data Protection Officer

Obligatoire (art.37) ou fortement conseillée.

Une réglementation unifiée

d'application directe le 25 mai 2018 dans toute l'UE.

Un champ d'application étendu

- À tout traitement réalisé par une entité établie sur le territoire de l'UE, que le traitement soit ou non réalisé dans l'UE.
- À tout traitement de données relatives à tout résident européen, même si le responsable de traitement ou le sous-traitant n'est pas établi dans l'UE (extra-territorialité).

La notification obligatoire des failles de sécurité

Les failles de sécurité devront être notifiées par le responsable de traitement à l'autorité de contrôle dans les meilleurs délais et si possible 72 heures après en avoir été informé sauf s'il y a absence de risque pour les personnes concernées.

La protection des données dès la conception et par défaut

Mise en place de mesures techniques et organisationnelles appropriées. Seules les données nécessaires doivent être traitées.

RG
PD

Un changement de logique avec l'accountability

La réglementation précédente reposait sur la notion de « formalités préalables » /contrôle a priori. Le règlement repose sur une logique de contrôle a posteriori. Il faut donc être en mesure de démontrer cette conformité à tout moment.

Une responsabilisation accrue du sous-traitant

En plus du devoir de conseil, le sous-traitant devra tenir un registre des traitements spécifique et mettre en œuvre des « mesures techniques et organisationnelles appropriées ».

Des analyses d'impact

pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés :
Profilage, traitement à grande échelle de données « sensibles » ...

Des sanctions renforcées

jusqu'à 20 000 000 d'euros ou jusqu'à 4% du CA annuel mondial total de l'exercice précédent.

Des données sensibles élargies

Elles comprennent maintenant les données génétiques et biométriques. L'interdiction du traitement des données sensibles reste le principe.

Une définition des données de santé

L'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée.

cegedim

Document non contractuel - Septembre 2017 - Cegedim tous droits réservés