Generali Protection Numérique

GENERALI

Règlement général sur la protection des données

Note d'information

Qu'est-ce que le Règlement général sur la protection des données ?

Le règlement européen dit « Règlement général sur la protection des données » (RGPD) doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique*. Ce règlement **entrera en application le 25 mai 2018.**

Les **objectifs clés du RGPD** sont les suivants :

Quelles sont les nouvelles obligations et responsabilités de l'entreprise ?

Renforcement du contrôle des citoyens européens sur l'utilisation de leurs données personnelles

- Consentement explicite : toute personne doit accepter explicitement que ses données fassent l'objet d'un traitement.
- Profilage : toute personne a le droit de ne pas faire l'objet d'une décision la concernant fondée exclusivement sur un traitement automatisé, y compris le profilage.
- Portabilité : toute personne a le droit de récupérer les données qu'elle a fournies pour, si elle le souhaite, les transférer à un tiers.
- Droit à l'oubli : toute personne a le droit d'obtenir du responsable du traitement l'effacement des données la concernant dont la conservation ne se justifie pas ou plus.

Sécurisation des données

- Protection des données dès la conception : le responsable de traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées à la protection des données.
- Protection des données par défaut : il doit garantir que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont recueillies et traitées.
- Analyse des risques et études d'impacts : pour tout traitement susceptible d'entraîner un risque, une étude d'impact (PIA) doit être effectuée.

Désignation d'un « Data Protection Officer »

Cette nouvelle **fonction clé au sein des entreprises** sera chargée :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant,
- de contrôler le respect de la réglementation relative à la protection des données,
- de conseiller l'entreprise sur la réalisation de PIA et d'en vérifier l'exécution,
- de coopérer avec l'autorité de contrôle compétente et d'être son point de contact.

** Règlement 2016/679 - Journal officiel de l'Union européenne L119 du 4 mai 2016.*

Traçabilité documentaire

Pour assurer une protection des données en continu, l'entreprise doit **assurer la mise à jour régulière :**

- d'un registre recensant les traitements de données personnelles qu'elle effectue,
- des documents, mentions-type et procédures visant à informer les personnes sur le recueil de leur consentement et l'exercice de leurs droits,
- des contrats entre les personnes effectuant les traitements qui définissent les rôles et les responsabilités des acteurs.

Notification des violations des données à caractère personnel

Le responsable de traitement est tenu de notifier une violation de données à caractère personnel à l'autorité de contrôle **72 heures au plus tard** après en avoir pris connaissance.

La personne concernée doit, elle aussi, être informée dans les meilleurs délais lorsque la violation est susceptible d'engendrer **un risque élevé pour les droits et libertés de la personne physique.**

Quelles sont les sanctions en cas de non-respect de ces nouvelles obligations ?

Le règlement va remplacer et/ou faire évoluer de nombreuses formalités à réaliser auprès de la Commission nationale de l'informatique et des libertés (CNIL).

- La responsabilité des organismes effectuant les traitements de données sera renforcée et les régulateurs auront le pouvoir d'appliquer des sanctions financières plus élevées qu'elles ne le sont aujourd'hui.
- En cas de non-respect, ces sanctions pourront aller **jusqu'à 4 % du chiffre d'affaires mondial annuel** d'une entreprise ou **20 millions d'euros,** le montant le plus élevé étant retenu.

Le RGPD en un coup d'œil

PORTÉE

Toutes les entreprises du **MONDE** traitant les données personnelles de citoyens européens

OBLIGATIONS

Les entreprises doivent notifier les violations de données **DANS UN DÉLAI DE 72 HEURES**

SANCTIONS

Jusqu'à **4 %** **DU CHIFFRE D'AFFAIRES MONDIAL**

CALENDRIER

25

Entrée en application en **MAI 2018**

Pour davantage d'informations sur le RGPD, rendez-vous sur le site de la CNIL : https://www.cnil.fr/professionnel

GA6L26A - Juin 2017 - Gestion des Imprimés