GDPR - General Data Protection Regulation -

le point sur
LA NOUVELLE RÉGLEMENTATION EUROPÉENNE

C'est le nouveau texte de **référence européenne** en matière de **protection des données à caractère personnel.**

applicable à partir du 25 mai 2018, entrée en vigueur totale en mai 2020

son but

- protéger toutes les données qui permettent d'identifier un individu
- garantir aux citoyens le contrôle de leurs données personnelles (accès, portabilité, droit à l'oubli, gestion des consentements,...)
- améliorer la confiance dans les systèmes numériques
- adapter votre entreprise à ces nouveaux usages

Les piliers de la Réglementation

1. Garantir le droit des ressortissants européens

2. Renforcer la protection des données afin de **réduire les risques de cyberattaques** et sécuriser le nouvel environnement de travail des entreprises.

3. Protéger les entreprises juridiquement : elles pourront démontrer leur volonté de mise en conformité, par le biais d'une documentation justifiant l'ensemble des traitements et processus mis en place (logique de responsabilisation), ainsi que celle de leurs sous-traitants utilisant ces données (coresponsabilité).

4. Garantir le traitement éthique des données : application de la réglementation dès la conception d'un produit ou d'un service utilisant ces données *(privacy by design)* jusqu'à leur exploitation et leur conservation dans le temps.

Donnée personnelle

Toute information permettant de caractériser un individu : son identité, n° sécurité sociale, coordonnées, etc., mais aussi caractéristiques physiques, culturelles, sociales, ainsi que les informations liées au monde digital (identifiants, mots de passe, adresses IP, habitudes de navigation, etc.)

Traitement de données

Toute opération sur les données, automatisée ou non, telle que la collecte, l'enregistrement, la modification, l'extraction, la consultation, l'utilisation, la diffusion, et aussi l'effacement et la suppression.

CONTACT
www.certilience.fr
04 28 29 72 50
contact@certilience.fr

Les risques en cas de non-conformité

Sanctions financières :
Amende administrative pouvant représenter 4% du CA mondial ou 20M d'€ (le montant le plus élevé est retenu)

Perte de notoriété :
Impact sur l'image de marque de l'entreprise et dégradation de la réputation

Votre projet en pratique

1 Impliquer les interlocuteurs clés de l'entreprise

département juridique, DSI, direction financière, DRH

Nommer un Data Protection Officer (DPO) :
ses compétences juridiques et techniques lui permettent de conseiller les différents interlocuteurs de manière objective, de déterminer le plan d'actions et de le mettre à exécution.

2 Cartographier les traitements

Travail préliminaire qui permet de **recenser précisément tous vos processus de traitements de données personnelles,** puis de les soumettre à une **étude d'impact** *(PIA pour Privacy Impact Assessment).*

Cela permet de calculer leur niveau de conformité, d'évaluer les risques proportionnels à chaque données et donc organiser le traitement des données les plus vulnérables en priorité.

3 Établir un plan d'actions

Sur la base de cet état des lieux, **déterminez les étapes clés de votre projet.**

- Cette mise en conformité devra concerner : la sécurisation des données (anonymisation ou chiffrement), les modalités d'exercice des droits des individus concernés, du recueil du consentement au droit à l'oubli, la finalité de chaque traitement, la durée de conservation des données,....
- Intégrez également vos partenaires au processus, ils sont considérés comme co-responsables :
  → les sous-traitants (revoir les contrats pour intégrer des clauses correspondant aux nouvelles obligations),
  → les partenaires basés hors de l'UE (qui gèrent des données de citoyens européens)
- Enfin, mettez en place un dispositif de surveillance et de contrôle afin d'assurer le suivi à la conformité dans le temps.

4 Organiser les processus de l'entreprise

- **Instaurez des procédures internes claires et précises** afin de minimiser la collecte des données et de garantir leur intégrité tout au long de leur cycle de vie
- Intégrez la gestion d'un haut niveau de protection des données dès la conception d'un nouveau traitement (Privacy by Design)
- Élaborez un plan d'action en cas d'incident ou de fuite de données
  Tout incident devra être déclaré à la CNIL dans les 72 h
- Mettez en place toute la documentation nécessaire afin de prouver votre conformité

5 Sensibiliser tous les collaborateurs

Les nouveaux enjeux de la GDPR doivent être partagés par tous.

Afin que chacun puisse acquérir de nouveaux réflexes et mettre à jour ses connaissances, formez les collaborateurs et instaurez des campagnes de sensibilisation régulièrement .

CONTACT
www.certilience.fr
04 28 29 72 50
contact@certilience.fr