

RGPD

**RÈGLEMENT GÉNÉRAL SUR
LA PROTECTION DES DONNÉES**



PRÉSENTATION GÉNÉRALE

OBJECTIFS

- **Redonner aux citoyens le contrôle de leurs données personnelles**
(protection de la vie privée, droit à l'oubli, ...)
- Inciter les personnes morales à devenir responsables et garantes du respect de la vie privée
- Harmoniser la réglementation européenne et rendre plus cohérente l'action des autorités de contrôle.
- Clarifier les responsabilités des responsables de traitements de données (numériques ou papier) et de leurs éventuels sous-traitants.

OBLIGATIONS

- Créer et mettre à jour un **registre des activités de traitement des données**
- Désigner un **DPO** (Data Protection Officer ou Délégué à la Protection des Données) : responsable du traitement des données
- « **Privacy by design** » : Obligation de concevoir des produits/services qui veillent au respect de la protection des données
Informers les utilisateurs sur
 - L'objectif / finalité de la collecte
 - Les catégories de données utilisées
 - Qui a accès aux données
 - La durée de conservation des données
 - Modalités selon lesquelles les personnes peuvent exercer leurs droits de consultation des archives (délai de 1 mois max pour répondre).
- Obtenir le **consentement préalable des utilisateurs** (et en conserver la preuve)
- Alerter la CNIL dans les 72h en cas de violation des données à caractère personnel
- En cas de non respect : amendes pouvant aller jusqu'à 4% du chiffre d'affaires

QUELLES DONNÉES ?

- Nom/prénom
- Adresse email
- Numéro de téléphone
- Adresse postale
- Adresse IP / données GPS (données de localisation)
- Cookies
- Numéro d'identification ou identifiants
- Les données sensibles : informations relatives à l'identité physique, psychique, médicale, génétique, économique, sensibilité religieuse, engagement politique ou syndical, appartenance ethnique, orientation sexuelle. Et toute données qui peuvent donner lieu à de la discrimination ou des préjugés.



**RGPD ET
SITE WEB**

INFORMER : RÉDIGER UNE POLITIQUE DE CONFIDENTIALITÉ

- L'objectif de la collecte
- Les catégories de données utilisées
- Qui a accès aux données
- La durée de conservation des données
- Rappeler les droits exerçables auprès du DPO :
 - Accès (portabilité des données)
 - Modification
 - Suppression/opposition
 - Modalités d'exercer les droits (nom du DPO + moyens de le contacter)
- Informations sur la gestion des cookies

INFORMER : GESTION DES COOKIES

- **Cookies exemptés de consentement** (sans tracker, ex : sessions...)
- **Cookies nécessitant un consentement préalable** (avec tracker) :
 - Google Analytics
 - Google AdWords
 - Photos / vidéos issues de plateformes (Youtube, Dailymotion, Instagram...)
 - Plugins de réseaux sociaux (likebox Facebook, badge, boutons de partage...)
 - Tout plugin tiers effectuant du tracking et/ou collectant des données

COLLECTER LE CONSENTEMENT PRÉALABLE

- **Pour les mineurs** le consentement est possible à partir de la majorité numérique fixée à 15 ans.
- **De manière globale** (valable une fois pour tout le site) :
 - Pour tous les cookies de tracking utilisés par le site (pop-up lors du 1^{er} accès au site)
 - Pour tous les formulaires collectant des données
- **De manière segmentée** : pour chaque formulaire :
case à cocher, bouton, texte de consentement...
- **Conserver la preuve du consentement** (flou sur la forme) :
 - Pas de limite de validité du consentement
 - De manière claire et sans ambiguïté : bouton « accepter » / case à cocher (opt-in uniquement)

SÉCURISER LES DONNÉES

- **Se protéger contre le piratage et les failles de sécurité** : CMS et plugins mis à jour
- Se renseigner sur la fiabilité d'une application ou d'un plugin avant installation
- **Chiffrement de l'échange de données** : certificat SSL/TLS (<https://...>)
- Politique de **sécurité des mots de passe** administrateurs et utilisateurs
- **Obligation de signalement à la CNIL** en cas de violation / divulgation des données