Règlement Général de Protection des Données

Qu’est-ce qu’on protège ? Comment ? Et combien ça coûte ?

25 mai 2018

Principe - Objectifs

Cadre unifié de protection des données au sein de l’UE.

Ancienne norme datant de 1995

Droit des personnes :

savoir ce que les entreprises font

Contrôler ce que font les entreprises avec les données

Harmoniser au niveau européen

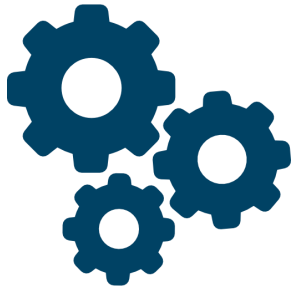
Données concernées - Création de compte

Prénom & Nom

Email

Téléphone

Adresse livraison/facturation



Identifiant compte

Lors du paiement

Données bancaires (si enregistrement d’une carte pour un prochain achat)

Historique d’achat

Navigation

Adresse IP

Tracking de suivi (les analytics)

Avis / Support

Commentaires sur le site

Message via formulaire de contact

Données sensibles

Origine ethnique

Opinions politiques

Convictions religieuses

Orientation sexuelle

Données de Santé

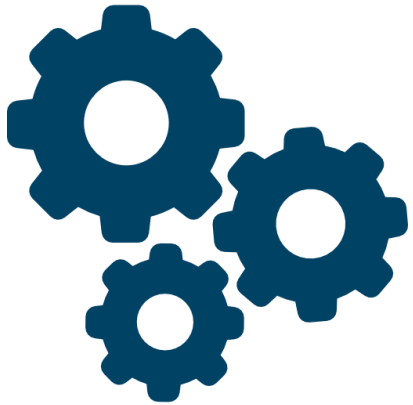
Appartenance Syndicale

Données génétiques

Données Biométriques

Conditions d’utilisation

Accord explicite de l’utilisateur



Info nécessaire pour le bon fonctionnement de l’appli (doctolib)

Légalité d’utiliser ce type d’informations

Source

Droits

Droit à l’information

Droit d’accès

« droit à l’oubli »

Qu’est-ce qu’on va sauvegarder ?

Qu’est-ce qu’on a en stock ?

Tout effacer

Droit d’opposition

Droit à la portabilité

S’opposer à la réutilisation (cookies marketing)

Récupérer les datas au format exploitable

CRM – récolte via formulaire

Être transparent sur la finalité de la récolte + droit à la modification / export des données / suppression

CRM – Veille commerciale (B2B)

Nom & Prénom

Entreprise & Fonction

Coordonnées Pro

Notes commerciales

Pas de données personnelles ni sensibles !

Obligations lors de l’utilisation du CRM

Prévenir le contact du stockage des infos dans un CRM (les petites lignes du mail de contact)

SI 0 contact (pas de réponse) -> Suppression (2 ou 3 ans)

Si utilisation d’un compte sur le site web

Suppression au bout de maximum 2 ans sans connexion (à mettre dans la politique de confidentialité)

Mailing liste

Ne pas abonner par défaut l’internaute !

Cookies

Demander le consentement AVANT de déposer les cookies (exemple : tarte au citron, Complianz, CookieYes)

Chiffrement obligatoire - recommandé

Obligatoire	Recommandé	Obligatoire
Mots de passe / Données bancaires	Le reste	Protocole HTTPS

Raison de se faire sanctionner 1/2

Absence/mauvaise information des personnes

- Absence de consentement
- Durée de conservation excessibe

Raison de se faire sanctionner 2/2

Sécurité insuffisante

Pas de registre de traitement

Refus d’accéder aux demandes des personnes (suppression, accès, etc…)

Pas de notification en cas de violation de données

Sanctions

Avertissement

(ex: pas de consentement pour la Newsletter, pas de bannière cookies)

Mise en demeure

Ignorer la demande de suppression

(amende, conservation des infos trop longues)

Amende

BDD Non protégées ou faille de sécurité béante