RGPD

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

la ligue de l'enseignement
un avenir par l'éducation populaire

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 règlementation 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.

QUELLES DONNÉES ?

- Nom / prénom
- Adresse email contenant le nom d'une personne physique
- Numéro de téléphone
- Adresse postale
- Adresse IP / données GPS (données de localisation)
- Cookies
- Identifiant unique d'un téléphone mobile
- Numéro d'identification ou identifiants
- Toutes données permettant d'identifier de manière unique une personne
- Données sensibles : informations relatives à l'identité physique, psychique, médicale, génétique, économique, philosophique, sensibilité religieuse, engagement politique ou syndical, appartenance ethnique, orientation sexuelle, données biométriques. Et toute données pouvant donner lieu à de la discrimination ou des préjugés.

OBLIGATIONS

- Obtenir le **consentement préalable des utilisateurs « opt-in »** (et en conserver la preuve)
- Créer et mettre à jour un **registre des activités de traitement des données**
- Désigner un **DPO/DPD** (Data Protection Officer ou Délégué à la Protection des Données) : responsable du traitement des données (recommandé ou obligatoire dans certains cas)
- « **Privacy by design** » : Obligation de concevoir des produits/services qui veillent au respect de la protection des données
- Informer les utilisateurs sur
  - L'objectif / finalité de la collecte
  - Les catégories de données utilisées
  - Qui a accès aux données (sous-traitance ou non)
  - 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).
- 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

LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

DPO / DPO

LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

- **Missions**
  - Informer et conseiller la structure sur le traitement des données personnelles (direction et salariés)
  - Contrôler le respect du RGPD
  - Coopérer avec la CNIL
- **Conflits d'intérêt**
  le DPO/DPD ne peut être un responsable de traitements (rôle généralement porté par la direction d'une structure). Fonctions traditionnellement non compatibles : direction, chef de service en charge de la création de traitement de données, responsable RH, responsable informatique.
- Sa fonction doit pouvoir être exercée en tout indépendance (hiérarchique ou autre)
- Sa responsabilité ne peut être engagée en cas de nos respect du RGPD par l'organisme

OBLIGATION DE DÉSIGNER UN DPO ?

- **Obligatoire pour**
  - Les autorités, établissements et organismes publics
  - Les structures dont les activités de base les amènent à réaliser **un suivi régulier et systématique des personnes à grande échelle**
  - Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites sensibles ou relatives à des condamnations pénales et infractions. Les établissements traitant des données médicales, quelle que soit l'échelle.
- **Non obligatoire**, mais recommandée pour les autres structures
- Le DPO peut-être externalisé
- Déclaration de l'identité et des contacts du DPO à faire sur le site de la CNIL.

LE REGISTRE DE TRAITEMENT DES DONNÉES

LE REGISTRE

- **Page de synthèse**
  - Coordonnées de l'organisme et de son responsable de traitement des données (direction), ainsi que du DPO
  - Liste synthétique des activités pour lesquelles vous traites des données personnelles
- **Fiche de registre d'une activité**
  - Dates de création et de mise à jour
  - Nom du responsable (direct ou conjoint) du traitement
  - Nom du logiciel utilisé
  - Objectifs du traitement (exemple : organisation de sessions de formation)
  - Catégories de personnes concernées (exemple : usagers, clients, prospects…)
  - Liste des données collectées en spécifiant si elles contiennent des données dites sensibles
  - Durée de conservation des données
  - Destinataires de ces données (organismes externes ou sous-traitants, entité ou service, catégories de personnels…)
  - Mesures de sécurité prévues (contrôle d'accès aux données, traçabilité, cybersécurité…)

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 en France 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 1er accès au site)
  - Pour tous les formulaires collectant des données

- **De manière segmentée,** pour chaque formulaire (recommandé) :
  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 DES FAILLES DE SÉCURITÉ

- Pour les sites web : logiciel CMS (Wordpress, Joomla…) et logiciels en ligne toujours à jour
  - **Chiffrement de l'échange des données** : certificat SSL/TLS (https://....)
- Systèmes d'exploitation non obsolètes et à jour (windows, linux, macOS, android, IOS…)
- Logiciels non obsolètes et à jour avec leurs derniers patchs de sécurité (cf cert.ssi.gouv.fr)
- Vérification de la présence d'un antivirus actif et à jour sur chaque appareil

SÉCURISER LES ACCÈS ET FORMER

- **Sécuriser les accès et l'identification :**
  - Obligation d'un accès à minima par mot de passe (avec politique de mots de passe forts)
  - Mise en place d'une authentification double facteur pour les accès à caractère critique (administration, données sensibles…)
  - Clé wifi renforcée
  - Non communication de la clé Wifi aux personnes extérieures (accès wifi invité)
  - Gestion des accès physiques aux serveurs et machines physiques

- **Former les salariés à la cybersécurité :**
  - Bonnes pratiques sur sollicitations (emails, sms, appels téléphoniques…)
    Ne jamais répondre à une sollicitation par l'intermédiaire de la demande mais par ses propres moyens indépendants. Dans le doute, ne rien faire et demander conseil.
  - Pas d'accès administrateur généralisé sur les postes (blocage de l'installation de logiciels)
  - Proscrire l'usage des ordinateurs ou clés usb personnelles sur le réseau de l'entreprise
  - Ne pas autoriser l'usage des accès distants de type VPN sur des postes personnels
  - Verrouillage des postes informatiques en cas d'absence même courte.