Le RGPD

Définition :

L'acronyme RGPD signifie « Règlement Général sur la Protection des Données ». C'est une règlementation européenne entrée en vigueur le 25 mai 2018, qui s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978.

Elle renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant et la protection, conservation et circulation des données personnelles.

Sont considérées comme données personnelles toutes informations se rapportant à une personne physique identifiée ou identifiable, dont les principaux sont : nom, prénom, âge, localisation, identifiant en ligne.

Sont considérés comme données personnelles dites "sensibles" celles qui révèlent l'origine ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé, l'orientation sexuelle, les données génétiques ou biométriques...

Sont considérées comme des données anonymes : les données ne permettant plus, de manière irréversible, l'identification des personnes concernées.

Cette réglementation concerne tous les organismes qui recueillent des données personnelles, comme les bibliothèques, peu importe la taille de la commune.

En France, la CNIL (Commission Nationale Informatique et Libertés) est l'autorité administrative référente de ce dispositif.

Le RGPD précise, renforce et uniformise la législation précédente :

- Loi informatique et libertés de 1978 ;
- Directive européenne du 24 octobre 1995 ;
- Loi du 6 août 2004.

Objectifs :

- Uniformiser les règles de protection des données personnelles afin de protéger les données personnelles des individus ;

- D'une logique de déclaration à une logique de démonstration/certification : le responsable du traitement doit pouvoir démontrer que la personne a donné son consentement pour l'utilisation de ses données et que le traitement est effectué conformément au présent règlement ;
- Mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que le traitement des données personnelles devient une exception et celui des données anonymisées, la norme.

Obligations pour les bibliothèques :

- **Identifier le responsable du traitement**

Ce responsable doit prendre et appliquer les mesures nécessaires afin de démontrer que le (s) traitement(s) dont il a la responsabilité sont effectués en conformité avec le RGPD. C'est généralement le représentant légal de la collectivité (le maire ou le président de la communauté de communes).

- **Identifier un Délégué à la protection des données (DPO)**

Il est désigné par le responsable du traitement. C'est cette personne qui organise la protection des données personnels au sein de la collectivité ou de la structure.

- **Recenser les différents traitements de données mis en œuvre par la bibliothèque**

Il est indispensable d'identifier et recenser tous les documents, bases de données et fichiers contenant des données personnelles.

Les données collectées en bibliothèques concernent principalement les informations associées à l'inscription pour l'usage d'un service (comme le prêt de document, la participation à une animation ou l'utilisation du réseau wifi).

Toutes les données périmées doivent être supprimées. Seuls les données strictement nécessaires peuvent être conservées. Pour finir, les données destinées à des fins statistiques doivent être anonyme.

Les durées de conservation réglementaires selon le type de données sont les suivantes :

- 1 an à compter de la date du dernier prêt pour les données collectées d'inscription ;
- 3 mois à compter de la restitution du document pour les données collectées lors du prêt ;
- 1 an pour les données collectées lors de la connexion sur un le réseau internet de la médiathèque ;
- Dès la fin de l'évènement pour les données collectées pour une animation.

Les logiciels de bibliothèque permettent généralement de traiter facilement ces données.

- **Vérifier auprès du fournisseur ou prestataire de logiciel que la norme simplifiée n°9 de la CNIL est bien respectée**

Elle concerne les traitements relatifs à la gestion des prêts de documents et les données enregistrées relatives à l'emprunteur.

- **Lister les différents opérateurs impliqués dans les traitements des données**

Outre le service informatique de la collectivité, plusieurs acteurs interviennent dans les traitements de données d'une bibliothèque (fournisseurs : SIGB, portail, ressources en ligne, logiciel de gestion des EPN…). Cette liste permettra au DPD d'établir un registre des sous-traitants précis et à jour.

- **Préciser la finalité de ces divers traitements de données, les durées de conservation et les lieux de stockage**

Concrètement…

Sur le formulaire d'inscription :

- Mettre les mentions légales .
- Pour les mineurs, obtenir un consentement du tuteur légal pour l'inscription au service.
- Dans le cas d'in formulaire d'inscription à un évènement/service particulier, s'assurer de ne pas conserver les données au-delà un temps nécessaire à la réalisation de l'évènement ou du service.

Mentions légales :

Les informations personnelles recueillies dans ce formulaire, avec votre consentement explicite, ont pour finalité votre inscription et l'accès aux services proposés par la bibliothèque. Vous pouvez à tout moment retirer votre consentement en mettant fin à votre adhésion. Les données personnelles fournies font l'objet d'un traitement informatique. Elles sont conservées [préciser la durée maximale de conservation des données : 1 an pour les données d'inscription et 3 mois pour les prêts].

[La mairie de…./la bibliothèque de….] est le responsable du traitement et les destinataires des données sont [insérer les services destinataires et/ou les tiers ou « exclusivement les services de la bibliothèque »…]. Aucune donnée collectée ne fait l'objet d'un transfert en dehors de l'Union européenne. Conformément au Règlement général de Protection des Données, RGPD, et à la Loi informatique et Libertés modifiée, vous bénéficiez d'un droit d'accès, de rectification des informations qui vous concernent. Vous pouvez également définir le sort de vos données après votre décès. Vous pouvez vous opposer au traitement informatique de vos données mais cela entraînera votre désabonnement. L'ensemble de ces demandes doivent être adressées, en justifiant de votre identité, par voie postale à l'adresse suivante : [adresse postale complète], ou par mail à l'adresse xxx@xxxx.fr. Vous pouvez aussi contacter le Délégué à la Protection des Données de la [mairie/communauté de communes de XXXXX] à l'adresse xxxxx@xxxx.fr. Vous pouvez également introduire une réclamation auprès de la CNIL (3, place Fontenoy – TSA 80715 – 75334 Paris cedex ou www.cnil.fr

Dans la lettre d'information :

- S'assurer de demander le consentement explicite pour l'inscription à une lettre d'information.
- Mettre en œuvre les mesures nécessaires à la bonne gestion des désabonnements à la lettre d'information.
- S'assurer que chaque lettre d'information contient un lien de désabonnement.
- Organiser le nettoyage régulier de la base de contact pour ne conserver que les abonnés inscrits.
- Lors de l'envoi des lettres d'information, toujours s'assurer que les destinataires son invisibles.

Dans la gestion des services numériques :

- S'assurer que les usagers ont pris connaissance et acceptent les conditions générales d'utilisation ou la charte qui définissent les conditions d'usage du service. Elles doivent être acceptées explicitement à chaque connexion.
- Il n'y a pas d'obligation de collecter l'identité des personnes qui utilisent les postes publics ou le réseau wifi. Si elle est collectée, elle doit être conservée un an comme les données de trafic
- S'assurer de collecter les données trafic : adresse IP de l'ordinateur, adresse mac, date, heure et durée de chaque connexion.
- S'assurer de ne pas collecter des données portant sur le contenu des correspondances échangées ou des informations consultées. Supprimer celles qui auraient été conservées.
- S'assurer que les données collectées soient accessibles uniquement aux administrateurs techniques et transmises aux autorités uniquement dans le cadre de la réquisition d'un juge.
- Veiller à la conformité des outils utilisés pour la gestion des services informatiques.

Dans la sécurité des données :

- S'assurer de la sécurité d'accès aux équipements informatiques contenant des données sensibles : sauvegardes protégées, sécurisation des postes informatiques, choix de mots de passe complexes et régulièrement renouvelés, sécurisation du wifi…

Avec les sous-traitants :

- Veiller à ce que l'ensemble des sous-traitants impliqués dans chaque traitement de données soit signalées au registre.
- Établir un contrat de sous-traitance avec l'ensemble des fournisseurs ou faire un avenant aux marchés en cours.
- S'assurer que les prestataires impliqués dans la collecte et le traitement des données sont en conformité avec la RGPD et la loi informatique et Libertés modifiée.

Pour aller plus loin : https://www.cnil.fr/fr/reglement-europeen-protection-donnees