

Le RGPD

Informations de base

À l'intention des petites bibliothèques

RGPD RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Règlement européen du 25 mai 2018

Principe : ne collecter que les données personnelles nécessaires / pouvoir démontrer la conformité de l'organisme à la CNIL.

Le RGPD différencie les traitements et le temps de conservation des données selon leur finalité

LES ACTEURS DU RGPD EN BIBLIOTHÈQUE



LE RGPD : INFORMATIONS DE BASE

1- Le RGPD ?

Le RGPD est le Règlement général sur la protection des données. C'est une réglementation européenne en vigueur depuis le 25 mai 2018.

Elle concerne les organismes de toutes sortes et de toutes tailles, dès qu'ils recueillent 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.

Même si votre bibliothèque municipale est dans une commune de moins de 2 000 hab. ou si elle est associative, vous êtes concernés et devez donc adapter vos pratiques à la RGPD.

2- Le RGPD : une attitude générale à adopter

Il n'y a plus de « déclaration CNIL », mais on respecte la réglementation et la CNIL reste l'autorité administrative référente du RGPD en France.

Le RGPD n'a pas révolutionné mais a précisé, renforcé et uniformisé la législation précédente. L'attitude générale est de ne collecter que les données personnelles dont on a besoin. Ensuite, on informe, on demande, on protège et on enregistre pour démontrer que l'on est en conformité.

A chaque fois que l'on utilise une liste de données personnelles, sous forme papier ou numérique, on est en présence d'un **traitement de données**. La RGPD oblige à différencier les traitements selon leur finalité. Ex : Un traitement de données pour la gestion des prêts, un second pour l'utilisation de l'espace multimédia etc.

3- Les informations que l'on collecte pour le fonctionnement de la bibliothèque

On peut obliger la personne qui s'inscrit à fournir des données qualifiées de nécessaires, parce qu'elles seront utiles à la gestion des prêts, la récupération des documents et l'élaboration de statistiques utiles à l'amélioration du service :

- Noms, Prénoms
- Adresse
- Année de naissance
- CSP : mais seulement si on les utilise en vue d'améliorer le service
- N° de téléphone

Lors du prêt ou de la réservation, on associe à la personne inscrite, des informations identifiant les documents en cours d'emprunt (titre, auteur, N° d'exemplaire etc.).

Cette association est confidentielle, elle doit être protégée.

Collecter des données personnelles en bibliothèques peut être nécessaire à la gestion d'autres activités que le prêt de documents : l'inscription aux animations, à l'espace multimédia (si indépendant de l'inscription à la bibliothèque), la connexion wifi, le prêt de matériel (tablettes, liseuses, etc.).

Ensuite, on conserve durant le temps réglementaire et pas au-delà, soit :

- Les inscriptions doivent être radiées d'office **1 an** après le dernier retour de document
Pour chaque document, les informations des précédents emprunteurs doivent être effacées **4 mois** après le retour du document.
- Pour chaque document, les informations des précédents emprunteurs doivent être effacées **4 mois** après le retour du document.

Votre logiciel de bibliothèque doit vous permettre de gérer facilement ces délais.

Au-delà de ces données nécessaires on peut collecter des données facultatives afin de proposer des services supplémentaires à ceux qui le veulent. On devra cependant demander, pour chacune d'elle, le consentement explicite du lecteur, après lui avoir exposé l'utilisation précise que l'on en fera.

Ex : vous demandez le mail mais de manière facultative et vous précisez que vous l'utiliserez pour la newsletter.

Il en sera également question si vous avez des services à distance (paragraphe 7)

4- La bibliothèque n'est pas seule

Pour chaque organisme concerné par la RGPD, l'autorité administrative devient le **responsable du traitement des données** :

- Pour la bibliothèque municipale : le Maire.
- Pour la bibliothèque associative avec délégation de service public de la commune (convention) : le Maire.
- Pour la bibliothèque associative non conventionnée : le Président de l'association.
- Pour la bibliothèque intercommunale : le Président de l'EPCI.

Chaque responsable du traitement doit désigner un **DPO** (Délégué à la Protection des Données, en français).

C'est la personne référente pour la protection des données (normalement, ce n'est pas un informaticien car il serait à la fois juge et partie). Elle peut être mutualisée entre plusieurs petites collectivités territoriales. Dans tous les cas, votre hiérarchie doit pouvoir vous orienter vers elle.

Votre éditeur de logiciel de bibliothèque (comme vos prestataires de site internet, de ressources numériques) est **sous-traitant** des données personnelles que vous collectez. A ce titre, ils sont également soumis au RGPD et co-responsables avec le responsable du traitement. Ils ont une obligation de conseil et une obligation de sécurisation des données confiées.

5- On commence à s'organiser et on se fait aider

- En début d'adaptation on retire les données gardées inutilement. Ex : lecteurs non actifs
- On échange avec le DPO.
- On vérifie que l'éditeur du logiciel de bibliothèque respecte la **norme simplifiée NS-009** de la CNIL et que sur le contrat qu'on a avec lui figurent des clauses concernant la protection des données.
- En collaboration avec le DPO, on renseigne le **Registre de traitement des données**. Il faut y noter la provenance des données et comment elles ont été recueillies :
 - Qui accède aux données et dans quels cas : service médiathèque, hiérarchie, comptabilité ou Perception si recouvrement etc.
 - Les catégories de données traitées
 - L'utilisation des données (finalité)
 - Les temps de conservation (délais légaux)
 - Comment elles sont sécurisées.

6- Enfin, on informe les lecteurs en expliquant clairement

On porte à sa connaissance. Le message doit être clair et simple (Licéité) et peut figurer sur le formulaire d'inscription. Le site de la CNIL donne des exemples de formulaire.

- L'identité du responsable du traitement des données.
- Pour chaque donnée personnelle demandée au lecteur, on précise :
 - La finalité (ex : gestion et récupération des emprunts)
 - Le caractère obligatoire ou facultatif + consentement
 - Les destinataires des infos et les transmissions envisagées et dans quels cas (ex : recouvrement)
 - La durée de conservation
 - Le droit des personnes sur leurs données personnelles collectées : le retrait du consentement pour les données facultatives, la désinscription, la modification

7- On répond toujours aux sollicitations des lecteurs

En **1 mois** (après la réception de la demande) aux personnes qui souhaitent faire valoir leurs droits sur leurs données pour les modifications, suppressions.

En fournissant des précisions sur les « nouveaux droits » : droit à l'effacement, droit à la portabilité

8- On référence son service à distance

Si votre bibliothèque possède un accès à distance au catalogue, à des ressources numériques en ligne qui nécessitent l'authentification des usagers, le responsable du traitement des données doit respecter les règles définies par le **RGS** (Référenciel Général de Sécurisation).

Il devra référencer son site et ainsi montrer qu'il a évalué les risques, mis en place les moyens de les limiter et qu'il assumera les risques résidentiels.

9- Dans le cadre d'un réseau de bibliothèques

Si votre bibliothèque fait partie d'un réseau intercommunal, les choses se compliquent un peu.

Selon la définition de la CNIL, le responsable du traitement est celui qui met en œuvre la collecte des données personnelles et en définit la finalité et les moyens. Il faut donc, à chaque fois qu'un traitement de données est entrepris, se demander qui l'entreprend et le définit.

Exemple : Considérons un réseau de médiathèques municipales avec une compétence partielle de l'échelon intercommunal qui administre le portail et le logiciel de bibliothèque.

- Pour le traitement des données nécessaires à l'inscription et au prêt de documents. Le Maire est, de fait, le responsable du traitement pour sa médiathèque quand celui-ci a été mis en place avant la mise en réseau. Si le traitement débute avec la mise en réseau, le Président de l'intercommunalité endosse ce rôle dans la mesure où sa collectivité conduit un traitement unifié sur le réseau.
- Pour le traitement des identifiants et mots de passe d'accès au portail. Le Président de l'EPCI est, de fait, le responsable car il remplit, via son personnel, le triple rôle de création de la base, de définition des finalités et de la mise à disposition des moyens.

Maires et Président peuvent également porter collectivement la responsabilité d'un traitement, devenant responsables **conjoint**s du traitement (Art.26).

Dans tous les cas, si les données personnelles circulent au-delà de la collectivité responsable du traitement, on indique ce périmètre au registre et on informe les lecteurs. Ex : « Vos données personnelles seront accessibles aux autres médiathèques du réseau afin de gérer etc »

Cet article est une première approche. Pour les cas plus complexes et pour aller plus loin, vous trouverez les informations complètes et actualisées sur le site de la CNIL www.cnil.fr . Vous trouverez notamment la [norme simplifiée NS-009](#) , spécifique aux bibliothèques.

Vous pouvez également interroger votre référent.e territoire de la médiathèque départementale.