Le RGPD : petit guide à l'usage des bibliothécaires

I. Contexte et éléments de définition

Le RGPD est le texte européen de référence relatif à la protection des personnes physiques en matière de gestion et de circulation des données personnelles. C'est un cadre qui définit ce qui est attendu en matière de protection/conservation/circulation des données personnelles récoltées.

Il est entré en vigueur le 25 mai 2018.

- Sont considérées comme des données personnelles : toutes informations se rapportant à une personne physique identifiée ou identifiable (nom, prénom, âge, localisation, identifiant en ligne...) ;
- Les données personnelles dites "sensibles" sont 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… . Leur traitement est interdit sauf exception prévue par la réglementation ;
- Sont considérées comme des données anonymes : les données ne permettant plus, de manière irréversible, l'identification des personnes concernées.

Le RGPD n'est pas un "Big bang", il s'inscrit dans la continuité d'autres textes relatifs à la protection des données personnelles tout en symbolisant leur nécessaire adaptation/évolution. En premier lieu, en France a été adoptée la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cette loi française sur la protection des données a largement inspiré la réglementation européenne et s'est adaptée à ses évolutions. Elle est toujours en vigueur après ses modifications successives par la loi du 6 août 2004 et la loi du 20 juin 2018 complétée par l'ordonnance du 12 décembre 2018 et le décret 29 mai 2019

Il serait illusoire de croire qu'une simple solution technique permettra aux organisations de se mettre en conformité avec le RGPD.
Le RGPD nécessite une attention et un travail continu à plusieurs niveaux (humain, organisationnel, technique).

Enfin, le RGPD est un règlement. Il est directement applicable dans les États membres de l'UE.
Néanmoins, le texte accorde une certaine latitude aux États membres pour certaines dispositions comme, par exemple, l'âge où un mineur peut consentir seul à une offre directe d'une société d'information, à définir entre 13 et 16 ans (ex : inscription à un réseau social)

II. Objectif(s) du RGPD

Vers une uniformisation des règles de protection des données personnelles

L'axe majeur et incontournable du texte est de protéger les données personnelles des individus.

Pourquoi un règlement et non une directive ? Parce que le règlement est juridiquement d'application directe et ne nécessite pas de loi de transposition (autant d'adaptations potentielles dans chaque État membre). Le but est donc d'uniformiser et non de simplement harmoniser.

D'une logique de déclaration à une logique de démonstration de sa conformité

L'approche en matière de protection des données se veut également plus pragmatique et substitue à l'ancienne logique déclarative (loi « informatique et libertés ») la notion de responsabilisation (*accountability*) des acteurs traitant des données.

Le responsable du traitement doit pouvoir démontrer :

- Que le traitement respecte les principes fondamentaux suivants (article 5) :
  - Une base légale parmi la liste des bases légales possibles (article 6) ;
  - Des finalités explicites, déterminées, légitimes ;
  - La minimisation des données à caractère personnel ;
  - L'exactitude des données ;
  - La limitation de conservation des données ;
  - La sécurité et la confidentialité des données (article 32).

Il s'agit alors de prouver la conformité RGPD de son organisation à travers, notamment, une documentation écrite qui liste les actions mises en œuvre et démontre que l'on assure une protection continue des données (« registre des activités de traitement »).

III. Obligations du RGPD

Obligations principales du responsable du traitement

Le RGPD définit le responsable du traitement comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ». **En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal**.
Ce responsable doit prendre **des mesures techniques et organisationnelles adaptées** au traitement au regard de la portée, du contexte, des finalités et/ou des risques pour la vie privée des personnes.

Encadrer la sous-traitance de données personnelles

Le sous-traitant est la personne physique, morale, l'autorité publique, le service ou l'organisme qui traite, sur instruction pour le compte du responsable de traitement des données personnelles.
Les sous-traitants (fournisseurs de SIGB/CMS, prestataires, plateformes de ressources numériques…) **sont également soumis au RGPD** et co-responsables avec le responsable du traitement.

Un contrat doit nécessairement régir le traitement effectué par un sous-traitant (article 28) : des clauses concernant la protection des données doivent y être intégrées.

Désigner un DPO (ou DPD : Délégué à la Protection des Données)

L'article 37 précise que le responsable du traitement doit désigner un *Data Protection Officer* (DPO).
C'est ce **référent autonome** qui sera le chef d'orchestre de la protection des données personnelles au sein d'une organisation et de la conformité avec le droit européen.
Tout organisme public a l'obligation d'avoir un DPO.

Établir un registre des activités de traitement

Le registre des activités de traitement permet de **recenser vos traitements de données** et de **disposer d'une vue d'ensemble** de ce que vous faites avec les données personnelles.
En savoir plus : https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

Se conformer à l'obligation d'information des personnes

Les personnes concernées par vos traitements de données **doivent être informées** de la finalité, du ou des auteurs de la collecte, des données collectées, de leurs destinataires, de leur durée de conservation et des droits qu'elles détiennent sur ces données.
Les Conditions Générales d'Utilisation (CGU) doivent être simplifiées, claires et lisibles. Les supports faciles à lire et à comprendre sont à privilégier.

Organiser un recueil du consentement conforme

Lorsque la base légale du traitement est le **consentement** de la personne : celui-ci doit **être libre, spécifique, éclairé et univoque.** L'article 7 précise : « *la demande de consentement est présentée sous une forme qui la*

distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. ».
Le consentement appartient à l'utilisateur, **il doit pouvoir le retirer simplement et à tout moment**.

Répondre aux demandes d'exercices de droit des personnes concernées

1. Respecter **les obligations d'information des personnes**

2. **Répondre dans un délai d'un mois** (après la réception de la demande) **aux personnes qui souhaitent faire valoir leurs droits** sur leurs données (accès, modification, opposition…). Un délai de 2 mois supplémentaires est possible si l'on prouve que la demande est complexe.

3. **Nouveaux droits** des personnes concernées : **droit à l'effacement**, **droit à la limitation du traitement**, **droit de ne pas faire l'objet d'une décision automatisée**, **droit à la portabilité** des données (un individu peut récupérer les données qu'il a fournies). Concernant la portabilité, les données devront alors être transférées à la personne « *dans un format structuré, couramment utilisé et lisible par machine* » (article 20).

Veiller à la sécurité des données et notifier les violations auprès de la CNIL

La sécurité du traitement : **des mesures de sécurité techniques et organisationnelles appropriées doivent être adoptées** « *compte tenu des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques […] pour les droits et libertés des personnes physiques* » (article 32).
ATTENTION : **les failles de sécurité devront être notifiées à l'autorité de contrôle et aux personnes concernées dans les 72h.**

Connaître les contrôles et sanctions

En France, l'autorité de contrôle est la CNIL. Les sanctions financières pourront aller jusqu'à 4% du chiffre d'affaire des entreprises. Concernant les personnes publiques, les choses sont moins claires car les pays membres de l'UE ont la liberté de définir eux-mêmes leurs barèmes de sanctions.

En savoir plus : https://www.cnil.fr/fr/la-procedure-de-sanction-de-la-cnil

IV. Et les bibliothécaires dans tout ça ?

Comme l'explique Thomas Fourmeux dans cet article sur la cartographie des traitements de données personnelles : « **Les bibliothèques, en tant qu'institutions publiques qui collectent des données personnelles, sont évidemment concernées par ce nouveau règlement (le RGPD). »**

Nous avons essayé de recenser et structurer en plusieurs étapes les tâches que les bibliothécaires vont devoir accomplir afin de s'assurer de la conformité de leurs pratiques en matière de récolte / gestion / protection des données personnelles.

ÉTAPE 1 : état des lieux

- **Identifier le DPD** (ou DPO) au sein de sa collectivité ou le référent CNIL. Connaître les personnes ressources au sein de son organisation est essentiel et vous fera gagner beaucoup de temps. En outre, les services ont tout à gagner d'un partage des bonnes pratiques en matière de protection des données, le DPD est tout indiqué pour coordonner ce travail.
- **Recenser les différents traitements de données mis en œuvre par la bibliothèque :**
  - **notice adhérent (base de données SIGB) : nature et détail des données personnelles ;**
  - **connexion WIFI ;**
  - **gestion des tablettes ;**
  - **gestion des PC et / ou salle multimédia ou Espace Public numérique (EPN) ;**
  - **connexion au site de la médiathèque et aux plateformes des fournisseurs de ressources numériques ;**
  - **inscription à des animations / cours / événements… (formulaire informatique ou papier) ;**
  - **…**

- **Lister les différents opérateurs** impliqués dans ces traitements de 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 les finalités** de ces divers traitements de données, les durées de conservation et les lieux de stockage.

Une fois l'étape 1 effectuée, vous avez déjà une bonne matière à apporter au DPD. Vous pourrez alors réfléchir avec lui. / elle aux mesures techniques et organisationnelles à prendre pour protéger les données personnelles et la vie privée des individus (cependant, rien ne vous empêche d'y réfléchir en amont !).

ÉTAPE 2 : mise en place de mesures pratiques à court terme

- **Toiletter vos mentions d'information afin de garantir les droits des personnes et de respecter l'obligation d'information (finalité, nature des données collectées, durée de conservation… voir la partie « obligations ») ;**

- **S'assurer que le site de la bibliothèque est bien en HTTPS (certificat TLS 1.2 et 1.3) :**
  « Le RGPD impose de sécuriser les données qui sont échangées entre l'internaute et le site web qu'il visite. Autrement dit, c'est la fin du HTTP et la standardisation du HTTPS. Si cela ne rend pas un site infaillible, cela permet d'assurer un certain niveau de confidentialité. Le nom de domaine du site de la médiathèque est géré par votre collectivité, votre prestataire de bibliothèque ne peut pas faire la démarche parce qu'il n'est pas propriétaire du nom de domaine. » (source : biblio numericus) ;

- **Proposer un formulaire de contact à destination des utilisateurs qui souhaitent faire valoir leurs droits sur leurs données personnelles ;**

- **Demander le consentement des personnes lorsque c'est la base légale du traitement et leur donner la possibilité, simple et pratique, de retirer cet accord.**

ÉTAPE 3 : mise en place de mesures de sécurité (adaptées au service et avec l'aide des divers opérateurs ou personnes ressources : DPD, DSI, RH, fournisseurs…)

- **Mettre en place les mesures de sécurité préconisées par la CNIL ;**

- **Vérifier que les clauses des contrats avec les prestataires sont complètes et à jour** (confidentialité, conseil, sécurisation…) ;

- Travailler avec la DSI ou les prestataires pour effectuer une **analyse du ou des système(s) d'information et des fichiers qui** y sont stockés ;

- **Participer** à la réalisation du **registre des activités de traitement** en vérifiant que le recensement et la description des traitements de données effectués par la médiathèque sont exhaustifs et justes ;

- Participer à, ou **organiser une étude d'impact** sur les données à risque ou « sensibles » le cas échéant.

V. Pour en savoir plus

Ce document a été réalisé, pour une très large part, à l'aide des articles suivants :

https://www.cnil.fr/fr/comprendre-le-rgpd
https://biblionumericus.fr/2018/03/14/rgpd-et-bibliotheques-cartographie-des-traitements-de-donnees-personnelles/