Petit guide à l'usage des bibliothécaires

Règlement Général sur la Protection des Données – Le RGPD

(Données à caractère personnel : Règlement européen n° 2016/679)

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

Le RGPD s'inscrit dans la continuité d'autres textes relatifs à la protection des données personnelles tout en symbolisant leur nécessaire adaptation/évolution :

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

Le RGPD nécessite une attention et un travail continu à plusieurs niveaux (humain, organisationnel, technique).

Enfin, le RGPD est un règlement et non une directive. Il est donc directement applicable dans l'ordre juridique des pays membres de l'UE.
Néanmoins, le texte donne une certaine latitude aux Etats membres à travers des "options" à activer.

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 Etat membre). **Le but est donc d'uniformiser et non de simplement harmoniser.**

D'une logique de déclaration à une logique de démonstration/certification

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 (RT) doit pouvoir démontrer :

- que la personne a donné son consentement (article 7)
- « *que le traitement est effectué conformément au présent règlement* » (article 24)

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 », voir chapitre suivant, code de conduite, mécanisme de certification…).

L'exception et la norme

Le paragraphe 2 de l'article 25 dispose que « *le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.* »

Le traitement des données personnelles devient une exception et celui des données « anonymisées », la norme.

III. Obligations du RGPD

Le responsable du traitement (RT)

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 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.

ATTENTION : 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.
Ils ont une obligation de conseil et une obligation de sécurisation des données confiées.
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 Délégué à la Protection des Données (DPD ou DPO - Data Protection Officer)

L'article 37 précise que le responsable du traitement doit désigner un (DPD).
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 DPD.

Etablir 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.

S'assurer de la validité du traitement des données personnelles

1. **Traitement licite, loyal et transparent**
2. **Principe de finalité** : la finalité (objectif/but) doit être déterminée, explicite et légitime
3. **Principe de minimisation** : seules les données adéquates, pertinentes et nécessaires à la finalité doivent être traitées
4. Les **données** doivent être **exactes** (et, si nécessaire, tenues à jour)
5. La **durée de conservation** doit être **limitée** par rapport à la finalité
6. La **sécurité des données** doit être **garantie**

Se conformer à l'obligation d'information des personnes et du recueil du consentement

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.

L'objectif est que le consentement soit éclairé (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.

Veiller à la sécurisation et transmission conforme des données

Les transmissions de données à des tiers (sous-traitants, prestataires, fournisseurs de ressources ou d'outils…) doivent être encadrées par un **contrat qui prévoit les garantis de sécurité et de confidentialité** imposées à ces derniers.

ATTENTION : un prestataire ne pourra pas recruter un autre sous-traitant sans votre accord préalable.

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.

Garantir le droit des personnes

1. Respecter **les obligations d'information des personnes et de recueil du consentement éclairé**

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 (modification, suppression…). 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 portabilité** des données (un individu peut récupérer les données qu'il a fourni). Concernant la portabilité, les données devront alors être transférées à la personne « *dans un format structuré, couramment utilisé et lisible par machine* » (article 20).

Contrôle et sanctions

En France, **l'autorité de contrôle est la CNIL (Commission nationale de l'informatique et des libertés).**
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 ?

Les bibliothèques, en tant qu'institutions publiques qui collectent des données personnelles, sont évidemment concernées par ce nouveau règlement (le RGPD).

Voici 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.

ETAPE 1 : état des lieux

Identifier le DPD (ou DPO) au sein de sa collectivité ou, à défaut, le CIL (Correspondant Informatique et Libertés) ou 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.

Vérifier (en interne et auprès du fournisseur/prestataire SIGB, site internet) **que la norme simplifiée n°9 de la CNIL est bien respectée** :

- nature des données personnelles récoltées
- objectifs poursuivis
- durée de conservation des données : Les informations concernant chaque prêt sont conservées jusqu'à la fin du quatrième mois suivant la restitution de l'objet du prêt ; la radiation intervient d'office dans un délai d'un an à compter de la date de fin du prêt précédent.
- destinataires des données
- Information des personnes et respect des droits « informatique et libertés »
- …

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 sur les 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 !).

ETAPE 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 SSL/TLS) s'il y a échange des données entre les internautes et le site Web :

« 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 bibliothèque / 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 et leur donner la possibilité, simple et pratique, de retirer cet accord.

ETAPE 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 ou **organiser une étude d'impact** sur les données à risque ou « sensibles ».