Fiche Bibliothéconomie 1-10

Le Règlement Général sur la Protection des Données (RGPD)

Introduction

Le RGPD (Règlement général sur la protection des données) de l'Union européenne fonde les bases d'une protection renforcée des données personnelles de tout citoyen ressortissant de l'Union. C'est un cadre qui définit ce qui est attendu en matière de protection, conservation, et circulation des données personnelles récoltées. Ce texte n'est pas le premier à règlementer la question.

En France, la première loi sur le sujet date de 1978[1], créant à la fois des règles de protection des « données nominatives » et la Commission nationale de l'informatique et des libertés (CNIL). Entretemps une directive européenne avait harmonisé en 1995 la protection des « données à caractère personnel » — terme créé par ce texte — et qui fut transposée dans la loi de 1978 en 2004 (Loi 2004-801 du 6 août 2004).

Le RGPD (Règlement Général sur la Protection des Données) quant à lui est entré en vigueur le 25 mai 2016. Les États membres et les organisations ont disposé d'un délai de 2 ans pour s'y conformer et c'est donc le 25 mai 2018 que le texte est devenu pleinement applicable.

Ce nouveau règlement européen renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant et marque l'adaptation du contexte juridique pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne, etc.).

1. Définition du Règlement Général de Protection des Données (RGPD)

Le RGPD (en anglais « General Data Protection Regulation » ou GDPR) encadre donc le traitement des données personnelles sur le territoire de l'Union européenne.

L'ambition de ce règlement est de redonner aux individus une maîtrise sur l'utilisation de leurs données personnelles collectées par les services en ligne qu'ils utilisent. Le RGPD s'applique aux entreprises mais aussi aux administrations.

[1] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés, dite « Informatique et Libertés », disponible sur Légifrance : https://www.legifrance.gouv.fr/loda/id/LEGISCTA000006095896 (consulté le 14/07/2024)

Sont considérées comme des données personnelles toutes les informations se rapportant à une personne physique identifiée ou identifiable (nom, prénom, âge, localisation, etc.).

Certains types de données sont encore plus protégées, car liées à des éléments intimes de la vie privée de la personne. Le RGPD en a allongé la liste.
L'article 9 interdit, sauf accord écrit des intéressés, de collecter des données sur la personne concernée qui font apparaître, directement ou indirectement :

- L'origine raciale ou ethnique ;
- Les opinions politiques philosophiques ou religieuses ;
- L'appartenance syndicale ;
- Les données génétiques ou biométriques ;
- la santé, la vie ou l'orientation sexuelle.

A l'inverse, sont considérées comme des données anonymes celles ne permettant plus de manière irréversible d'identifier une personne.

Bien que conçu pour répondre aux nouveaux besoins liés à l'explosion des usages numériques, tout document papier est soumis aux règles du RGPD.

Par ailleurs, le RGPD introduit une nouvelle démarche : il impose de passer d'une logique déclarative des données traitées par une entreprise ou une administration à une logique de responsabilisation. Cela veut dire que les responsables du traitement des données collectées doivent pouvoir démontrer qu'ils ont mis en œuvre les moyens nécessaires dans leur organisation pour respecter les termes du RGPD.

2. Les obligations du RGPD

2.1. Identifier le 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 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.

2.2. 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.

2.3. Etablir un registre des activités de traitement

Le registre des activités de traitement permet de recenser les traitements de données et de disposer d'une vue d'ensemble de ce qui est fait avec les données personnelles.

2.4. S'assurer de la licéité 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

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

Les personnes concernées par les 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.

2.6. 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 garanties de sécurité et de confidentialité imposées à ces derniers.

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).

2.7. 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 supplémentaire 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)

2.8. Contrôle 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.

3. Quelles conséquences pour les bibliothèques ?

Les bibliothèques et centres de documentation sont, en tant qu'administration et lieux accueillant du public et lui proposant des services, soumises au RGPD, car elles collectent des données personnelles. De nombreuses situations de fonctionnement d'une bibliothèque, plus ou moins évidentes, sont ainsi concernées.

La manière la plus concrète de traiter de ces situations est de présenter sous forme d'étapes ou de vade-mecum les points incontournables à mettre en œuvre pour être en conformité[2]:

2 Cette présentation est issue d'un document pratique rédigé par la Bibliothèque départementale du Val d'Oise de 2018, disponible en ligne : https://www.valdoise.fr/295-protection-des-donnees-rgpd.htm (consulté le 14/07/2024)

3.1. ETAPE 1 : état des lieux

- ✓ Identifier le DPD (ou DPO) au sein de la collectivité ou de l'université ou, à défaut, le CIL (Correspondant Informatique et Libertés) ou référent CNIL. Connaître les personnes ressources au sein de son organisation est essentiel. 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 :

  1. Nature des données personnelles récoltées
  2. Objectifs poursuivis
  3. 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)
  4. Destinataires des données
  5. Information des personnes et respect des droits « informatique et libertés »

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

  1. Notice adhérent (base de données SIGB) : nature et détail des données personnelles
  2. Connexion WIFI
  3. Gestion des tablettes
  4. Gestion des PC et/ou salle multimédia ou Espace Public numérique (EPN)
  5. Connexion au site de la médiathèque et aux plateformes des fournisseurs de ressources numériques
  6. 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 ou de l'université, plusieurs acteurs interviennent dans les traitements de données d'une bibliothèque (fournisseurs : SIGB, portail, ressources en ligne, etc.). 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.

3.2. ETAPE 2 : mise en place de mesures pratiques à court terme

- ✓ Toiletter les 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…).
- ✓ S'assurer que le site de la bibliothèque est bien en HTTPS (certificat SSL/TLS) : Le RGPD impose de sécuriser les données qui sont échangées entre l'internaute et le site web qu'il visite. Si cela ne rend pas un site infaillible, cela permet d'assurer un certain niveau de confidentialité.
- ✓ 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.

3.3. 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 ».

Conclusion

Le respect du RGPD est désormais obligatoire en bibliothèque ou centre de documentation. Il convient donc à chaque professionnel des bibliothèques de s'assurer que sa contribution au fonctionnement de l'institution va dans ce sens, et de veiller à ce que les évolutions de service, notamment numériques, respectent elles aussi les mesures exigées par ce Règlement.

Pour aller plus loin

- La CNIL propose une autoformation gratuite en ligne pour se familiariser avec le RGPD : https://www.cnil.fr/fr/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie (consulté le 14/07/2024)

- Pour les collectivités territoriales, la gazette des communes a préparé un dossier thématique complet sur le RGPD, avec notamment des points juridiques et des informations pratiques pour la gestion des données personnelles : https://www.lagazettedescommunes.com/dossiers/donnees-personnelles-la-marche-a-suivre-pour-respecter-le-rgpd/ (consulté le 14/07/2024)

- Le Ministère de l'économie, des finances et de la souveraineté industrielle et numérique a publié un mode d'emploi sur la gestion des données personnelles sur internet : https://www.economie.gouv.fr/entreprises/reglement-general-sur-protection-des-donnees-rgpd# (consulté le 14/07/2024)