Protection des données personnelles : Une nouvelle réglementation applicable dès le 25 mai prochain

Un règlement européen « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », dit « RGPD », va entrer en vigueur le **25 mai prochain** (Règlement UE 2016/679)[1].
Il est donc nécessaire d'examiner dès maintenant ses impacts sur votre organisation.

⚠ **Avertissement préalable**
Attention aux démarchages frauduleux ayant pour but de vendre des services de mise en conformité au règlement :
Communiqué de la CNIL :
https://www.cnil.fr/fr/vigilance-mise-en-conformite-rgpd

Quel est l'objectif du RGDP ?

Il est de renforcer la protection des données personnelles et les droits des personnes physiques. Il s'agit de protéger la vie privée est de permettre à la personne concernée de garder la maîtrise de ses données personnelles.

Par ailleurs, le RGPD remplace le système de contrôle a priori, basé sur les régimes de déclaration et d'autorisation préalable, par un **système de contrôle a posteriori dans une logique de responsabilisation**. L'entreprise doit être en mesure de démontrer à tout moment qu'elles respectent les principes relatifs aux traitements des données personnelles.
L'obligation de déclaration préalable à la CNIL est donc supprimée.

En outre, les pouvoirs de la Commission nationale de l'informatique et des libertés (CNIL) sont renforcés, et les sanctions nettement plus élevées

A qui cette nouvelle réglementation est-elle applicable ?

A tout organisme, privé ou public, qui gère ou stocke des données à caractère personnel, quand bien même leur activité principale est sans lien avec la collecte ou la gestion de données.

Votre librairie est donc concernée et ce, quelle que soit sa taille.

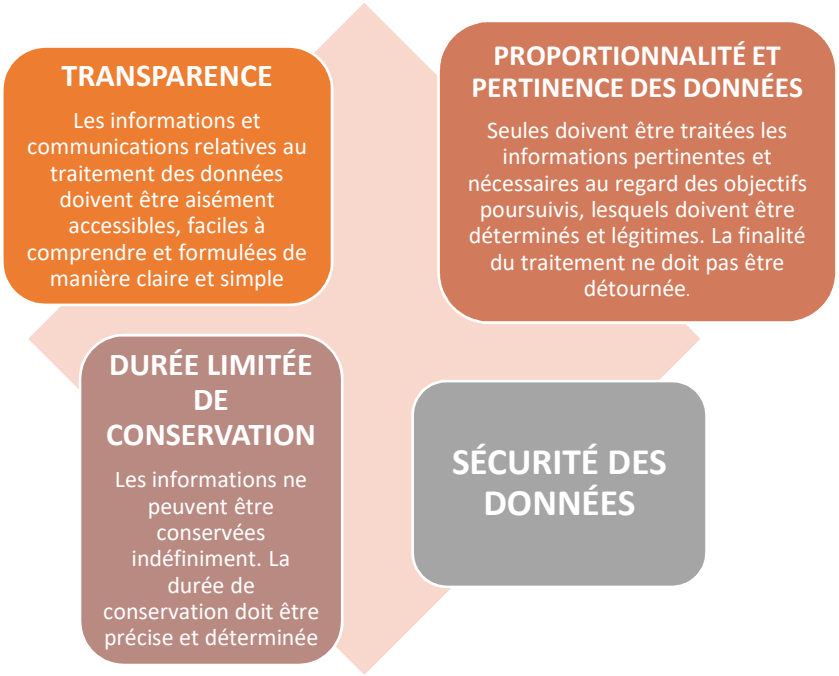
[1] Parallèlement, un projet de loi relatif à la protection des données personnelles est en discussion à l'Assemblée Nationale (info. au 7/02/2018).

A quelles données s'appliquent la nouvelle réglementation ?

Il s'agit de toute information relative à une **personne physique**[2] identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Par exemple, cela peut concerner les consommateurs, prospects, salariés, contractants et contractuels, fournisseurs…

A l'inverse, le RGPD ne s'applique pas aux données rendues anonymes.

Quels sont les principes fondamentaux de la réglementation ?



[2] Les personnes morales ne sont donc pas concernées par le RGPD (l'Etat, les Départements, les municipalités, les établissements publics, les associations déclarées, les sociétés commerciales, les fondations). On les distingue des personnes physiques, c'est-à-dire des individus.

Quels sont les droits dont disposent les personnes concernées ?

INFORMATION

- Quiconque met en place un fichier ou un traitement de données personnelles est obligé d'informer les personnes concernées de :
  - son identité,
  - de l'objectif de la collecte d'informations,
  - de son caractère obligatoire ou facultatif,
  - des destinataires des informations,
  - des droits reconnus à la personne,
  - des éventuels transferts de données vers un pays hors de l'Union Européenne.

ACCES

- Toute personne peut prendre connaissance de l'intégralité des données la concernant en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction. La personne concernée doit récupérer les données fournies sous une forme aisément réutilisable.

OPPOSITION

- Toute personne a la possibilité de s'opposer à ce que des données la concernant figure dans un fichier, et peut refuser, sans avoir à se justifier, que les données soient utilisées à des fins de prospection commerciale.
- Le consentement donné au préalable peut être retiré.
- Le RGPD prévoit des **dispositions spécifiques concernant le consentement des mineurs**. D'après le projet de loi, ce consentement doit être donné par le détenteur de l'autorité parentale pour les mineurs de moins de 15 ans (cet âge est à confirmer lorsque la loi sera promulgée - le RGPD prévoit 16 ans réductible jusqu'à 13 ans par les législations nationales.

RECTIFICATION

- Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant.

DROIT A L'OUBLI

- Droit à l'effacement des données

PORTABILITÉ DES DONNÉES

- Ce droit permet à une personne :
  - De récupérer les données la concernant, pour son usage personnel dans un format couramment utilisé qui permet leur réutilisation.
  - De transférer ses données personnelles d'un organisme à un autre. Les données personnelles peuvent ainsi être transmises au nouvel organisme soit par la personne elle-même, soit directement par l'organisme qui détient les données, si ce transfert direct est « techniquement possible ».
- Quelles données sont concernées par la portabilité ? Il s'agit des données informatiques, les fichiers papiers ne sont pas concernés. Les données personnelles qui sont dérivées, calculées ou inférées à partir des données fournies par la personne concernée, tel le profil d'un utilisateur créé grâce à l'analyse des données brutes produites par un compteur « intelligent », sont exclues du droit à la portabilité, dans la mesure où elles ne sont pas fournies par la personne concernée, mais créées par l'organisme.
- Le responsable du traitement[3] ne peut pas faire payer la fourniture de données personnelles sauf s'il arrive à démontrer que la demande est manifestement infondée ou excessive, « *notamment en raison de (son) caractère répétitif* ».

Que faut-il faire concrètement ?

1. *Se préparer*

- Désigner un **responsable de traitement**[3] qui sera en charge de la mise en œuvre du RGPD,
- **Identifier** les données que vous recueilliez/utilisez qui sont soumises à la nouvelle réglementation, («Pseudonymiser» dès que possible : pour rappel, dans ce cas, le RGPD ne s'applique pas).
- Prendre en compte les **impacts** des nouvelles exigences sur l'organisation :
  - → Identifier les salariés qui vont être en charge de traiter, participer, travailler sur les données concernées,
  - → Afin de s'assurer qu'ils maîtrisent bien les enjeux de la nouvelle réglementation et de leur rôle dans le processus, les (faire) former, les informer, leur fournir les outils nécessaires pour ce faire… Ils doivent connaître les notions de protection de la vie privée et comprendre que les données personnelles sont constituées de tout ce qui peut être lié à une personne physique.
- Etablir des **outils d'informations** pour les personnes concernées (salariés, clients…) sur les données récoltées, les modalités d'accès à l'information, et leurs droits : les informations doivent être claires, intelligibles et aisément accessibles aux personnes concernées, y compris les mineurs de moins de 16 ans.
- Définir le mécanisme de **consentement** de la personne concernée (cf. schéma ci-dessous)
- Si vous utilisez des systèmes de **profilage**, s'assurer que l'utilisation des données ne soit pas discriminante (basée notamment sur l'origine, l'orientation sexuelle, l'état de santé, les opinons politiques, religieuses ou syndicales).
- Fixer des **délais d'effacement** des données.
- Dans les entreprises de plus de 250 salariés uniquement, tenir un « registre des traitements ». Toutefois, si l'effectif de votre librairie est inférieur à ce seuil, cela ne vous dédouane pas de bien conserver les justificatifs de tout ce que vous avez mis en place pour pouvoir, le cas échéant, prouver la conformité de l'entreprise au RGPD.

2. Sécuriser

- S'assurer que les **mesures de protection des données** en place sont suffisantes. Si des lacunes ou risques sont identifiés, mettre en place les dispositifs nécessaires.
- Lorsque la gestion de tâches informatiques est confiée à un prestataire extérieur (infogérance, prestataire de cloud…), procéder à la **révision des contrats** pour s'assurer que le sous-traitant présente des garanties suffisantes. Le contrat doit comporter l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité, de confidentialité des données et doit prévoir qu'il ne peut agir que sur instruction du responsable du traitement. Dans l'idéal, prévoir des audits de sécurité à intervalle régulier.

3. Mettre en place la procédure de recueil du consentement des personnes concernées

[3] le responsable de traitement est le référent, en charge des opérations relatives à la protection des données personnelles. Il est celui qui va décider de mettre en œuvre un traitement de données personnelles pour une finalité donnée (ex. traitement RH, messagerie d'entreprise, fichiers clients et prospects, etc.) avec ses propres ressources informatiques ou en recourant à celles d'un prestataire tiers

RECUEIL DU CONSENTEMENT DE LA PERSONNE CONCERNEE
(ou du représentant légal pour les mineurs de moins de 15 ans[4])

EN CAS DE COLLECTE DIRECTE/DE VISU DES DONNEES

- Fournir au moment où les données sont obtenues les coordonnées et identité du responsable du traitement et le cas échéant de son représentant
- Préciser les finalités du traitement et la durée de conservation des données
- indiquer qui sont les destinataires ou catégories de destinataires des données
- Faire part de l'intention éventuelle d'effectuer un transfert de données
- Il faut rappeler ses droits à la personne concernée : accès aux données, rectification, effacement, refus, portabilité, possiblité de retarctation à tout moment, d'introduire une réclamation et le cas échéant informations sur le profilage
- Prévoir une déclaration écrite ou des cases à cocher **(l'abstention ne suffit pas)**. Le consentement ne peut être valable que s'il est donné après avoir fourni les informations. Il ne doit pas être ambigu.

EN CAS DE COLLECTE DES DONNEES SUR LES SITES MARCHANDS ET PLATEFORMES DE COLLECTE (à ajouter aux éléments de la collecte directe)

- Pour chaque typologie de traitement des données collectées, donner accès à la politique de confidentialité
- De mentions claires dans les formulaires de collecte ou autres cases à cocher au terme desquelles les internautes donnent leur consentement
- Cookies : les mentions concernant leur finalité doivent être complétées. Par exemple : « *En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de cookies pour mesurer notre audience, vous proposer des contenus et publicités personnalisés, ainsi que des fonctionnalités sociales*" suivi d'un clic "OK" et "*En savoir plus et gérer les cookies*" qui mènera l'internaute vers la page d'informations sur les cookies, la possibilité de désactiver tel ou tel cookie

[4] Comme indiqué ci-dessus, le projet de loi n'étant pas encore promulgué, l'âge est à confirmer

4. A posteriori

- En cas de **faille de sécurité**, si par exemple des données sensibles sont volées, ou parce qu'un salarié se fait dérober son ordinateur professionnel contenant des données personnelles, avertir la CNIL dans les 72 heures, voire les personnes concernées s'il existe un risque élevé pour les droits et libertés.
- Au **départ d'un salarié** ayant accès à des données personnelles, s'assurer qu'il ne peut plus y avoir accès.

Pour les entreprises dont le siège social est en France, l'interlocuteur unique est la CNIL.

Un guide a été élaboré par la CNIL
https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

Texte intégral du RGPD
http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

Contact au SLF
Sylvette Mougey
Chargée des questions sociales et juridiques
s.mougey@syndicat-librairie.fr ; 01 53 62 20 64