

le RGPD et la pratique en centre de documentation et bibliothèque

Les médias nous ont rebattu les oreilles avec le RGPD depuis quelques mois. Ce Règlement général sur la protection des données de l'Union européenne fonde en effet les bases d'une protection renforcée des données personnelles de tout citoyen ressortissant de l'Union.

un point d'histoire

Ce texte n'est pas le premier à régler la question. La loi française date de 1978, créant à la fois des règles de protection des « données nominatives » et la fameuse Commission nationale de l'informatique et des libertés (Cnil). Entretemps une directive européenne avait harmonisé en 1995 la protection de « données à caractère personnel » — terme créé par ce texte — et qui fut transposée dans la loi de 1978 en 2004. Le RGPD quant à lui est entré en vigueur le 25 mai... 2016. Mais les États membres et les organisations disposaient 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. Nous nous arrêtons ici sur quelques aspects pratiques de l'application du

Règlement dans les pratiques quotidiennes de nos métiers. Nous ferons ainsi émerger certains aspects du RGPD qui impactent fortement la vie professionnelle. Nous prendrons pour ce faire l'exemple des fichiers d'usagers et d'emprunteurs d'un centre de documentation ou d'une bibliothèque proposant des recherches et d'autres services aux usagers.

tout est « traitement de données » concerné par le RGPD

Il est évident qu'un fichier nominatif d'usagers, voire d'emprunteurs, dans lequel sont consignés les emprunts, mais aussi les services et documents fournis, constitue un « traitement de données à caractère personnel » au sens de l'article 4 du RGPD, tout comme de l'article 2 de la loi de 1978, toujours en vigueur et mise en conformité avec le Règlement le 20 juin dernier. Jusque-là, sous l'empire de la loi de 1978, il fallait absolument veiller à ce que les traitements automatisés de telles données soient bien encadrés. Dans ce cadre d'ailleurs, une norme simplifiée de la Cnil précisait les données qu'il était possible de consigner concernant les emprunteurs, et surtout la durée de conservation de ces données (norme simplifiée n° 9, aujourd'hui juridiquement caduque). À ce jour les mêmes règles s'appliquent toujours, à ceci près qu'elles concernent autant le traitement numérique que le papier : la loi de 1978 comportait une partie de règles concernant tout type de traitement,

automatisé ou pas, alors que c'est tout le RGPD qui s'applique à tout type de support. Il s'ensuit que tout dossier réuni au nom de tel usager, tout sujet de recherche pour une personne consignée dans un registre papier, toute trace d'emprunt sur un cahier obéissent aux mêmes règles de protection, qu'il nous faut détailler sur quelques points forts.

la protection des données dès la conception

Un concept fort du RGPD est celui de la protection des données pensée dès la conception des outils de traitement des données personnelles (article 25). En d'autres termes, c'est au moment où les fichiers (papier ou informatiques) sont élaborés qu'il faut penser simultanément au moyen de garantir la protection juridique et technique de ces données. Ces fichiers et autres documents doivent aussi permettre de faciliter une demande de droit

repères

À retenir

Le RGPD a alourdi la responsabilité des organisations quant aux traitements de données personnelles dans tous leurs domaines d'activité. Des règles plus complexes et plus exigeantes sont donc à prendre en compte. Et il importe de bien comprendre que tout document papier est soumis aux mêmes règles. ■

d'accès ou de rectification. Ils doivent être conçus pour être inviolables. Les fichiers informatiques doivent être techniquement sécurisés. Mais il en va de même des documents sur papier qui doivent donc impérativement être tenus sous protection, dans un lieu fermé et seulement accessible aux personnes habilitées.

Exemple : Un registre sous forme d'un cahier consignait les demandes de recherches d'informations des divers usagers, surtout si certaines recherches portent sur des données dites sensibles (voir ci-dessous). Ce registre, du fait qu'il porte des données concernant les personnes, même dans un cadre professionnel, doit être soigneusement rangé dans un endroit fermé et son accès doit être limité aux seules personnes habilitées.

attention aux données sensibles

Toute donnée personnelle est protégée par le RGPD. Mais certains types de données le sont plus encore, du fait des éléments intimes de la vie privée de la personne qu'ils portent. 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.
- Il s'ensuit que lorsque des recherches d'information commandées par un usager portent sur de telles données, il y a lieu de craindre qu'elles soient liées à sa personne. C'est pourquoi la norme simplifiée n° 9 de la Cnil sur les prêts d'ouvrages limitait la trace des emprunts, sur la fiche du lecteur, à 4 mois afin de préserver le traçage des opinions et autres données sensibles. On peut conserver les règles suggérées par cette norme, même si elle est devenue caduque. Mais surtout, lorsqu'un usager commande une recherche sur des données sensibles, il importe de se couvrir en lui faisant contresigner la demande d'un accord pour poursuivre le traitement.

les obligations d'information demander l'aide du DPD

Toute personne fournissant des données la concernant doit être informée de toute une série d'éléments concernant le traitement qui va être fait de ces données, notamment :

- responsable du traitement (le chef d'entreprise) ;
 - finalités poursuivies (emprunts, recherches, diffusion sélective d'information...);
 - coordonnées du DPD (délégué à la protection des données) s'il existe ;
 - personnes habilitées à accéder aux données ;
 - durée de conservation des données ;
 - droits d'accès, de rectification, d'effacement, de limitation, d'opposition et de portabilité des données ;
 - droit de retirer son consentement à tout moment ;
 - droit de saisir la Cnil en cas de litige.
- On le voit, les mentions à porter sur les formulaires d'inscription — par exemple — se sont largement allongées. On aurait aussi intérêt à faire apparaître ces informations dans le règlement intérieur du centre de documentation ou de la bibliothèque.

la durée de conservation des données

Quels que soient les types de services prévus, il convient de bien prévoir des durées de conservation qui n'excèdent pas celles de la finalité visée (article 5, 1, e). En d'autres termes, lorsque l'utilisateur n'emprunte plus de documents pendant un an (selon la norme simplifiée n° 9) ou qu'il a quitté l'entreprise, il y a lieu de supprimer ses données des fichiers d'emprunteurs. De même, lorsqu'une recherche d'information est terminée, les données n'ont plus à être conservées — sauf si l'utilisateur demande une veille sur la thématique donnée —, mais elles ne le seront pas au-delà de cette veille elle-même. Les mêmes durées de conservation s'appliquent aussi à tout document papier qui comporterait des données concernant un usager. Les armoires et placards vont donc devoir se vider...

Selon le RGPD, la plupart des entreprises doivent se doter d'un Délégué à la protection des données (DPD, que les maniaques du français nomment DPO : Data protection officer), qui est une personne aux pouvoirs et aux missions plus étendus que l'ancien Correspondant informatique et libertés (Cil). Une de ses missions est de conseiller les services de l'entreprise ou de la collectivité publique sur leurs pratiques du RGPD. Ne pas hésiter à travailler avec lui pour mettre toutes les activités de son service en conformité.

des sanctions salées...

Rappelons que l'une des clés du succès du RGPD, ce sont les « amendes administratives » que la Cnil peut prendre en cas de non-respect du Règlement, jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial de l'entreprise (article 83 du RGPD). Une bonne raison pour s'intéresser à ces règles qui au fond sont une garantie de protection pour nous tous en tant que citoyens. ■

Didier Frochot

→ www.les-infostrategies.com

repères

Références

- Règlement général sur la protection des données n° 2016-679 du 27 avril 2016, consultable sur EUR-Lex : eur-lex.europa.eu/legal-content/FR/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FRA
- Loi n° 78-17 du 6 janvier 1978 mise en conformité avec le RGPD par la réforme du 20 juin 2018, sur Légifrance : www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000886460
- Site de la Cnil qui fournit une foule de conseils et de documents pour se mettre en conformité avec le Règlement : www.cnil.fr