

Mise en œuvre du RGPD : comment documenter sa conformité

Par **Élisa Corazza**, avocate, cabinet Goutal, Alibert et associés

Entrée en vigueur

Le règlement général sur la protection des données, relatif à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, sera applicable en France dès le 25 mai.

Mise en conformité

Le RGPD impose aux collectivités de se mettre en conformité avec les règles relatives à la protection des données et de pouvoir démontrer qu'elles les respectent.

Registre des traitements

La documentation de la conformité repose en premier lieu sur l'élaboration et la mise à jour obligatoires d'un registre des traitements.

1 Se sentir concerné et mobiliser ses services avant le 25 mai 2018

Le règlement européen du 27 avril 2016 (règlement général sur la protection des données, RGPD) oblige chaque responsable de traitement de données à caractère personnel à constituer, regrouper et actualiser régulièrement un certain nombre de documents. Cette première étape est souvent décrite, quoi que l'on pense de la qualité de l'expression, comme l'obligation de « documenter ». Une fois la base d'information réunie, ses éléments doivent pouvoir être fournis sur simple demande de l'autorité de contrôle (en France, la Commission nationale informatique et libertés, la Cnil). Toutes les collectivités publiques, quelle que soit leur taille, sont soumises à cet impératif qui prendra effet dès le 25 mai de cette année ; et aucune ne peut s'en considérer exonérée au motif qu'elle ne disposerait d'aucun matériel informatique : dès lors qu'elle dispose de la liste de ses électeurs sur support papier, ou encore d'un fichier sur ses agents, une collectivité réalise des traitements de données à caractère personnel. Il importe d'engager au plus tôt, si cela n'est pas déjà fait, l'élaboration de la documentation requise par le RGPD. Il serait, en particulier, imprudent d'attendre l'adoption du projet de loi relatif à la protection des données personnelles (1). En effet, ce dernier ne fera que préciser ou compléter certaines des prescriptions du RGPD ; les collectivités qui se seront déjà mises en conformité avec le RGPD n'auront à procéder qu'à quelques aménagements mineurs au moment de son adoption – à une date qui reste inconnue.

2 Déterminer les éléments constituant le dossier de conformité

Cette première tâche est compliquée par le fait qu'il n'existe pas de « dossier standard » : le RGPD ne comprend pas de liste exhaustive définissant simplement sa composition. Le registre des traitements (2), document cartographiant précisément les traitements de données mis en œuvre, en constituera cependant la pièce maîtresse. Il est impé-

ratif d'établir ce document en priorité, afin de pouvoir, dans un second temps, identifier et concevoir, selon les caractéristiques des traitements recensés, les autres documents indispensables. C'est pourquoi, on s'attachera ici à donner des conseils pratiques concernant l'établissement de ce document en particulier.

On retiendra pour l'essentiel que devront dans tous les cas faire partie du dossier documentaire, outre le registre des traitements : la description des procédures et moyens adaptés pour la sécurité des traitements (3), les procédures internes en cas de violation de données (4), les informations sur le délégué à la protection des données (5) (description des missions, moyens, etc.), les mentions d'information à la personne concernée, les modèles de recueil du consentement et les procédures mises en place pour l'exercice des droits (6). Selon les cas seront en outre requises les analyses d'impact sur la protection des données (PIA) pour les traitements susceptibles d'engendrer des risques élevés envers les droits et libertés (7) (par exemple : les activités de vidéosurveillance) et/ou les éventuels contrats avec les sous-traitants (8). Le RGPD prévoit également, à titre facultatif, la possibilité pour les responsables de traitement de se voir délivrer une certification, attestant de leur conformité à la réglementation ; il faudra cependant attendre l'adoption du projet de loi relatif à la protection des données personnelles et ses textes d'application pour connaître les modalités de ce dispositif.

3 Établir ou faire établir le registre des traitements propre à sa collectivité

Même lorsqu'elle confie la gestion de ses traitements de données à un tiers (par exemple : centre de gestion de la fonction publique territoriale pour la gestion de certains agents, sociétés de stockage de données, etc.), une collectivité doit disposer d'un registre listant les traitements qui ont lieu sous sa responsabilité (9). Parallèlement, son éventuel sous-traitant devra tenir son propre registre des activités de traitement

réalisées pour le compte du responsable du traitement. Le registre doit donc être établi individuellement pour chaque collectivité et ne pourra pas être mutualisé comme l'est, par exemple, la fonction de délégué à la protection des données (DPD) (10). Il est en revanche concevable de confier la gestion de la documentation à un DPD mutualisé. Ce dernier devra alors tenir un registre pour chaque responsable de traitement par lequel il a été désigné. Concrètement, il est recommandé d'associer à l'établissement du registre l'ensemble des agents des services opérationnels concernés pouvant fournir toutes les informations précises relatives aux traitements. Le DPD ne pouvant être officiellement désigné avant l'entrée en vigueur du RGPD, l'établissement du registre aura plus probablement lieu sous la houlette de son « prédécesseur », le correspondant informatique et libertés (CIL) (11), lorsqu'il existe, ou, à défaut, par une personne – ou une équipe – compétente, désignée à cet effet.

Le registre devra être établi sous forme écrite (le format électronique étant très fortement recommandé) ; s'il n'existe aucun canevas type unique du registre, on conseillera d'y inclure une liste récapitulative des traitements et une fiche individuelle par traitement opéré à la date du