L'enjeu de la conformité à la réglementation des données personnelles pour les collectivités territoriales

par Matthieu **Dary**
Avocat Senior Counsel, De Gaulle Fleurance & Associés

Nina **Gosse**
Avocat, De Gaulle Fleurance & Associés

Depuis l'entrée en vigueur, le 25 mai 2018, du règlement général européen sur la protection des données (RGPD) [1], le traitement de données à caractère personnel doit figurer à l'ordre des priorités de la politique générale des collectivités territoriales. Tous les traitements de données doivent ainsi être mis en conformité avec les dispositions du RGPD et de la loi Informatique et libertés modifiée [2].

Cette évolution impacte directement les collectivités territoriales dès lors que ces dernières, dans l'exécution de leurs missions de service public et la gestion du personnel administratif, traitent en continu des quantités importantes de données personnelles, y compris des données dites sensibles [3]. La dématérialisation des services administratifs et le mouvement d'ouverture des données publiques renforcent la nécessité de prendre en compte cet enjeu.
La question de la conformité à la réglementation en matière de données personnelles n'est pas nouvelle, le RGPD se limitant pour l'essentiel à renforcer les dispositions préexistantes de la loi Informatique et libertés précitée. Force est de constater néanmoins que peu d'acteurs étaient entièrement conformes au droit antérieur et qu'il est dès lors nécessaire de déployer un certain nombre de mesures afin de remédier à cette situation, tout en atteignant le niveau de protection supérieur exigé par le RGPD.
Outre la volonté d'une action publique éthique et modernisée, le RGPD a porté le montant des amendes administratives jusqu'à 20 millions d'euros en sus d'autres sanctions, telles que l'arrêt des traitements litigieux. À ces sanctions administratives, peut s'ajouter la réparation du préjudice subi par les personnes dont les données ont été traitées.
Le temps n'est donc plus à s'interroger sur l'utilité d'une mise en conformité, mais sur la manière de la mener avec le plus d'efficacité possible.
Or, cette démarche peut s'avérer complexe en pratique et nécessite des moyens financiers et humains dont les collectivités territoriales ne disposent pas nécessairement. La création d'une dotation spécifique souhaitée par les sénateurs dans le cadre des débats sur le projet de loi modifiant le cadre juridique français, bien que finalement non adoptée [4], témoigne de cette difficulté.
Pour y parvenir, toute collectivité territoriale doit assimiler les principes clés de la réglementation et mener des actions concrètes de mise en conformité.

■ Présentation du cadre réglementaire

Les piliers de la protection des données personnelles

L'objet des réglementations en la matière est d'encadrer **tout traitement de données personnelles des individus.**

Par **« donnée personnelle »**, on entend toute information qui permet d'identifier directement ou indirectement une **personne physique**, notamment par référence à un identifiant, tel que :
- un nom,
- un numéro d'identification,
- des données de localisation,
- un identifiant en ligne,

ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
Pour que des données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée. Toutefois, s'il est possible par recoupement de plusieurs informations ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données seront toujours considérées comme personnelles.

La notion de **« traitement »** est également large puisqu'elle vise toute opération ou tout ensemble d'opérations effectuées, ou non, à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données personnelles, telles que, par exemple, la collecte, l'enregistrement ou la consultation.
La réglementation impose à tout **responsable du traitement**, à savoir celui qui en **détermine les finalités et les moyens** de respecter un certain nombre de conditions afin d'assurer la licéité dudit traitement :

(1) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avr. 2016 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, sur lequel v. not. Dalloz IP/IT 2016. 566.
(2) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
(3) V. not. S. Bonenfant, L'environnement « Informatique et libertés » des collectivités territoriales, une source de contentieux, AJCT 2017. 13 et le dossier consacré aux données personnelles, AJCT 2017. 7.
(4) Art. 19 *bis* supprimé du projet de loi relatif à la protection des données personnelles, n° 490, déposé le 13 déc. 2017.

- **définir les objectifs du fichier :** ces finalités limitent la manière dont le responsable pourra utiliser ou réutiliser ces données ;

- **vérifier la pertinence des données :** seules les données strictement nécessaires à la réalisation de l'objectif peuvent être traitées. Certaines données sensibles (par exemple, liées à la santé) font l'objet d'une protection renforcée. Il en va de même pour les données relatives aux infractions, condamnations et mesures de sûreté ;

- **limiter la conservation des données :** les données ne peuvent, en principe, être conservées que pour la durée nécessaire à la réalisation de l'objectif poursuivi, sauf obligation légale de les conserver pour une durée plus longue ;

- **respecter les droits des personnes :** les personnes dont les données sont traitées doivent être informées au préalable de cette opération. Dans certains cas, cette obligation d'information s'accompagnera de la nécessité de recueillir leur **consentement**. Ces dernières disposent également de certains droits qu'elles peuvent exercer auprès de l'organisme détenant leurs données ;

- **sécuriser les données :** le responsable de traitement doit prendre des mesures appropriées afin de garantir la sécurité des données mais aussi leur confidentialité.

Les collectivités territoriales, en ce qu'elles déterminent les finalités et les moyens de nombreux traitements de données relatives à des administrés, leurs personnels[5] ou des prestataires, sont tenues de se conformer à cette réglementation.

> Cela concerne, par exemple, la gestion de l'état civil, de la liste électorale, de l'exploitation de systèmes d'information, du développement de télé-services, etc.[6]

Outre le responsable du traitement, un traitement de données peut être effectué par un **sous-traitant**. Ce dernier intervient pour le compte du responsable du traitement, conformément à ses instructions. Cela est, par exemple, le cas lorsqu'une collectivité fait appel à un prestataire tiers pour des activités d'hébergement d'infrastructure informatique. Le responsable du traitement doit s'assurer que ses sous-traitants présentent des garanties suffisantes pour assurer la sécurité des données qui leur sont confiées.

Enfin, dans le cas où des **transferts de données personnelles à destination d'un pays tiers à l'Union européenne** seraient mis en œuvre, des impératifs spécifiques doivent être respectés. En effet, il convient de vérifier l'existence de garanties appropriées pour encadrer ces transferts.

Les nouvelles obligations consécutives au RGPD

À ces obligations existantes, s'ajoutent de nouvelles obligations, **depuis le 25 mai 2018**, découlant du RGPD.

La désignation d'un délégué à la protection des données (DPD)[7] **ou *data protection officer* (DPO),** en charge de contrôler et coordonner les pratiques de traitement de données personnelles et de communiquer vers l'extérieur. Sa nomination est notamment obligatoire lorsque le traitement est effectué par une autorité publique ou un organisme public. Les anciens correspondants informatique et libertés (CIL) pourront assumer ce rôle, à condition de disposer des compétences nécessaires à la fois techniques et juridiques[8].
Pour les collectivités qui sont susceptibles d'avoir des préoccupations similaires, la mutualisation de la fonction semble tout à fait adaptée. Elle permet de limiter les coûts en des temps de rigueur budgétaire et de bénéficier de professionnels disposant des compétences et de la disponibilité nécessaires à un bon pilotage de la conformité. Cette mutualisation est encouragée par la CNIL, qui invite à capitaliser sur les services proposés par les structures de mutualisation informatique (SMI), les centres de gestion et les établissements publics de coopération intercommunale (EPCI). De manière générale, les collectivités ont tout intérêt à mutualiser leurs efforts, ce qui devrait être facilité par l'article 31 de la loi modifiant le cadre juridique français[9].

Le principe d'*accountability* (RGPD, art. 5.2) – En vertu du principe d'*accountability*, le responsable du traitement doit désormais documenter l'ensemble des actions de sa politique de protection des données personnelles afin de démontrer sa conformité au RGPD, tant auprès des autorités de contrôle que des personnes concernées.
Une des illustrations de ce principe est l'allégement des formalités[10]. Les formalités préalables auprès de la CNIL sont désormais limitées (sauf rares exceptions[11]) ; en contrepartie de cet allègement, le responsable de traitement doit dorénavant tenir un registre de ses activités de traitement, destiné à permettre à l'autorité de contrôle de vérifier que les obligations de l'organisme sont bien remplies.

Le principe du *privacy by design* et *privacy by default* (RGPD, art. 25.1 et 2) – Il s'agit pour le responsable du traitement de mettre en place des mesures permettant de garantir *ab initio* une protection des données personnelles et une minimisation de leur traitement (y compris de leur collecte) durant toutes les étapes de vie des projets, y compris sur les aspects informatiques, physiques et logiques.

La gestion des violations de données (RGPD, art. 33) – En cas de violation de données, celles-ci devront en principe être notifiées à la CNIL dans les 72 heures, et aux individus touchés dans les meilleurs délais, si la violation présente un risque élevé pour eux ou sur ordre de la CNIL.

L'analyse d'impact (RGPD, art. 35). Le responsable de traitement devra effectuer une analyse d'impact préalablement à la mise en œuvre de traitements présentant des risques particuliers d'atteinte

(5) V. not. P. Salen et R. Perray, Les collectivités locales à l'épreuve de la protection des données personnelles de leurs agents, AJCT 2017. 17.
(6) S. Bonenfant, L'environnement « Informatique et libertés » des collectivités territoriales, une source de contentieux, préc.
(7) V. V. Langlet, Nom de code : délégué à la protection des données, JT 2018, p. 29, n° 207.
(8) A. Carrera Mariscal, Le CIL : modèle type du futur délégué à la protection des données ?, Dalloz IP/IT 2018. 233.
(9) Art. 31 relatif à la mutualisation des moyens des collectivités territoriales.
(10) Exemples : acte réglementaire unique RU-030 relatif aux téléservices locaux, norme simplifiée n° 46 concernant la gestion des ressources humaines. V. S. Bonenfant, Les obligations déclaratives des traitements de données à caractère personnel des collectivités territoriales, AJCT 2017. 8.
(11) Outre les cas d'autorisations préalables maintenus dans le RGPD, les États peuvent prévoir au niveau national de soumettre certains traitements à l'accomplissement de formalités préalables.

aux droits et libertés individuelles. Les traitements à risques concernent notamment :
- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- le traitement à grande échelle de données personnelles sensibles ou relatives à des condamnations pénales et à des infractions ;
- la surveillance systématique à grande échelle d'une zone accessible au public.

La mise en œuvre d'un *privacy impact assessement* (PIA) requiert le respect d'un certain formalisme, pouvant mener dans certains cas sensibles à une consultation de la CNIL (RGPD, art. 36).

De plus, le RGPD instaure, vis-à-vis des tiers une obligation de **transparence** à la charge des responsables conjoints, une **responsabilité directe** des sous-traitants ainsi qu'une **solidarité** des responsables de traitement et des sous-traitants. Par ailleurs, l'article 28 énumère les clauses devant désormais figurer obligatoirement dans les contrats de services conclus entre responsables du traitement et sous-traitants.

■ Mise en conformité : comment faire ?

Afin d'identifier les changements nécessaires au respect de la nouvelle réglementation, la première action à mener est d'établir une cartographie des traitements de données personnelles, qui mènera à l'établissement d'un plan d'action.

La cartographie des traitements

Tout chantier de mise en conformité commence par la **réalisation d'un diagnostic**, qui consiste à dresser un état des lieux des traitements réalisés afin d'évaluer l'écart entre leur niveau de conformité actuel et celui à atteindre pour respecter la réglementation.

Phase 1 : détermination des acteurs de la cartographie – Il est recommandé de mettre en place un groupe de travail qui sera en charge de la mise en conformité au RGPD. Au sein de ce groupe, pourront figurer le CIL s'il en existe un, des représentants de la direction juridique (s'il en existe une également), de la direction des ressources humaines et de la direction des services informatiques. Le diagnostic peut être réalisé par ce groupe, éventuellement avec l'assistance de tiers (avocat, consultant en sécurité informatique, etc.). La collecte d'informations pour procéder au diagnostic sera réalisée auprès des différents services de la collectivité territoriale. Au sein de chacun des services, il faudra identifier les personnes en charge des traitements qui pourront utilement répondre aux questions.
Les autres membres du service pourront être entendus dans un second temps afin de vérifier leur compréhension des enjeux et confirmer ou préciser les informations obtenues.

Phase 2 : l'établissement de questionnaires – Afin de collecter le plus d'informations possible utiles à la réalisation du diagnostic, des questionnaires pour chacun des services vont pouvoir être établis.
Ces questionnaires devront permettre de répondre aux interrogations suivantes de façon détaillée :
- **Quels sont les traitements auxquels la collectivité territoriale procède ?** – Si un CIL avait été nommé, il conviendra de se référer au registre de traitement qu'il tenait. À défaut, il faudra se référer aux formalités faites auprès de la CNIL. Cette dernière a mis en ligne l'ensemble des formalités réalisées par les organismes depuis 1979[12] ;
- **Qui est en charge du recensement des traitements ?** – Existence d'un CIL, d'une ou de plusieurs personnes en charge des données personnelles et des formalités auprès de la CNIL et/ou du suivi des relations avec la CNIL ;
- Quelle est la **finalité** du recueil des données ? – Fichiers de l'état civil, liste électorale, fiscalité locale, fichiers sociaux, recensement de la population, gestion des demandes d'attestation d'accueil, vidéosurveillance, associations, logements vacants, gestion RH,...
- **Quelles sont les personnes concernées par les traitements ?** – Fonctionnaires, contractuels, usagers, etc. Sont-ils informés des finalités du traitement et de leurs droits ? Ont-ils donné leur consentement ?
- **Quelles sont les données recueillies ?** – Catégories de données, telles que données d'identification, situation financière, situation familiale, données de santé, données de connexion ou de géolocalisation, ...
- **Comment sont recueillies les données ?** – Formulaires papiers ou en ligne, profilage, recueil direct ou indirect, ...
- Sur quelle **base légale** repose chaque traitement ? – Exécution d'un contrat, exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, consentement de la personne concernée,...
- **Quelles sont les personnes destinataires des données ?** – Au sein de la collectivité territoriale et/ou des tiers, comment l'accès à ces données est-il assuré ?
- **Quelle est la durée de conservation des données ?** – En fonction des données recueillies ; qu'advient-il des données par la suite ?
- **Comment les droits des personnes sont-ils exercés ?** – Personnes en charge de la gestion, difficultés rencontrées...
- **Où sont stockées les données ?** – Auprès de serveurs internes à la collectivité territoriale ou auprès de sous-traitants hors ou intra-UE ;
- **Comment la sécurité des données est-elle assurée ?** – Quelles sont les mesures de sécurité existantes ? Existe-t-il des procédures de gestion des incidents de sécurité ?

Phase 3 : la réalisation d'interviews – Afin de s'assurer de la coopération des différents interlocuteurs, un message préalable du responsable de l'exécutif expliquant la démarche et rappelant les enjeux facilitera l'intervention du groupe de travail.
Ces interviews sont à réaliser de préférence individuellement pour faciliter les échanges et permettre d'obtenir le plus d'informations possible.
Pendant les interviews, il convient de lister les documents probants que la personne devra remettre, afin de lui permettre de les transmettre à bref délai (contrats, formulaires, mentions légales proposées sur les sites internet, procédures particulières telles que recueil des consentements, etc...).

Phase 4 : l'établissement d'un rapport – Une fois les réponses aux questionnaires obtenues ou interviews réalisés, il convient de les étudier et de les synthétiser, pour faire le bilan de l'existant.

(12) https://www.cnil.fr/fr/les-formalites-prealables-accomplies-aupres-de-la-cnil-depuis-1979, ce qui permettra d'avoir une liste des traitements déjà existants au sein de la collectivité territoriale, sous réserve qu'elle ait procédé aux formalités.

Ce rapport sera également l'occasion d'analyser la conformité de chaque traitement effectué par la collectivité territoriale, en identifiant les points d'amélioration.

Le plan d'action

Une fois la cartographie établie et le niveau de conformité mesuré, il convient de prioriser les mesures à entreprendre selon leur complexité, les risques suscités par le traitement mais aussi les urgences propres à chaque collectivité (par exemple, le lancement d'un nouveau projet).
Une **feuille de route** doit ainsi être formalisée afin de lister l'ensemble des chantiers à mettre en œuvre pour se conformer à la réglementation, en lui assignant un **calendrier** et des **contributeurs**.
Si chaque feuille de route est propre à une entité, certaines actions seront dans la majorité des cas indispensables à envisager, outre la **désignation obligatoire d'un DPO** pour les collectivités.

Construction du registre et adoption de procédures internes – Les collectivités doivent mettre en place un registre regroupant l'ensemble des traitements identifiés lors de la phase de cartographie. Les informations devant figurer *a minima* dans ce registre sont celles prévues par l'article 30 du RGPD et correspondent, en réalité, aux champs antérieurement prévus au sein des déclarations classiques de la CNIL. Ce registre, sous forme de fichier informatique, contient les informations nécessaires pour les vérifications de la CNIL en cas de contrôle.

Revue contractuelle – Chaque collectivité doit procéder à une modification de ses contrats conclus avec les tiers amenés à obtenir communication des données traitées. En matière de **sous-traitance de données personnelles**, il conviendra de respecter le formalisme fixé par l'article 28 du RGPD. De même, en cas de **co-responsabilité** de traitement, l'article 26 prévoit certaines exigences.

Modification des mentions informatives – L'administration doit s'assurer que toute personne concernée est informée du traitement de ses données d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Cette information pourra s'accompagner du recueil univoque, libre et spécifique du **consentement** de chaque personne concernée lorsque celui-ci est requis. Les personnes doivent notamment être informées de leurs **droits**, ces derniers étant renforcés par le RGPD, et des moyens de les exercer.

Sécurisation – À l'heure où les cyberattaques et incidents sont de plus en plus nombreux, la sécurisation des données est essentielle car principale source de risques. En matière de téléservices, les collectivités pourront s'appuyer sur leurs obligations relatives au référentiel général de sécurité applicables depuis 2010[13].

Procédures internes et sensibilisation – Il conviendra également d'organiser des procédures internes afin de sensibiliser le personnel de l'administration et d'encadrer au mieux le cycle de vie d'un traitement. Parmi les procédures devant être définies, la gestion des demandes d'exercice des droits et la gestion des éventuelles failles de sécurité sont essentielles. Mener des actions de sensibilisation et de formation des personnels administratifs est également très important pour diffuser une véritable culture de la donnée et éviter toute fuite de données qui serait due à une faute interne.

***

Bien que l'ampleur des travaux à mener suscite souvent des inquiétudes voire des réticences, ceux-ci sont essentiels et de nombreuses actions sont en réalité relativement faciles à mettre en œuvre. La mise en conformité doit être perçue comme une opportunité et non une contrainte, et faire l'objet d'une approche progressive. Elle permettra de mieux connaître les administrés et d'améliorer les services.
Au-delà du respect en tant que tel de la réglementation et des sanctions, les collectivités doivent y voir une occasion de poursuivre sur la voie de la dématérialisation et d'affirmer leur légitimité en gagnant la confiance de l'ensemble des parties prenantes et, en premier lieu, des administrés.

(13) Le Référentiel général de sécurité (Rgs) est prévu par l'ord. n° 2005-1516 du 8 déc. 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Les modalités sont prévues par le décr. n° 2010-112 du 2 févr. 2010.