

Fichiers d’administrés et d’électeurs : que peuvent faire les collectivités ?

À l’heure où la protection des données personnelles constitue un enjeu central dans les relations entre l’administration et les citoyens, les collectivités territoriales sont de plus en plus confrontées à des questions pratiques : peut-on utiliser une liste de participants à une réunion publique pour une campagne d’information ? Est-il possible d’envoyer une newsletter institutionnelle aux électeurs nouvellement inscrits sur la liste électorale ? À quelles conditions un élu peut-il conserver les coordonnées d’un administré avec lequel il a été en contact ?

Cet article vise à clarifier les règles applicables et à identifier les bonnes pratiques à adopter pour concilier proximité avec les administrés, efficacité politique et respect du droit.

Un cadre juridique strict

L’utilisation des données personnelles des administrés ou électeurs par les élus s’inscrit dans un cadre juridique rigoureux se composant du RGPD (Règlement (UE) 2016/679) et de la loi n° 78-17 du 6 janvier 1978 dite « Informatique et libertés ». Toute information permettant d’identifier une personne – nom, adresse, participation lors d’un événement communal – constitue un « traitement » soumis aux principes de licéité, proportionnalité, finalité déterminée, limitation de la durée de conservation et sécurité (articles 5 et 6 du RGPD). En collectivité, le responsable de ce traitement est en règle générale la Commune, sauf si un élu constitue un fichier pour un usage personnel : dans ce cas, il en devient personnellement responsable.

S’agissant plus précisément de la gestion de la liste électorale, [la CNIL rappelle](#) que les listes électorales, extraites du Répertoire Électoral Unique géré par l’INSEE depuis le 1er janvier 2019, contiennent des données nominatives (nom, date et lieu de naissance, adresse, bureau de vote). Dans ce cadre, la CNIL recommande notamment les bonnes pratiques suivantes :

- Lorsque la communication de la liste électorale est sollicitée, il convient d’informer des finalités lors de sa remise et de veiller à ce que le demandeur respecte les obligations "Informatique et libertés" (ex. éviter usage commercial ou discrimination par tri ethnique, religieux ou origine, interdit par article 226-19 du Code pénal) ;
- informer les personnes concernées sur l’origine des données (la liste électorale) et leurs droits, incluant un droit d’opposition gratuit ;
- garantir une stricte séparation fonctionnelle et technique entre fichiers municipaux institutionnels, fichiers électoraux et usages politiques.

Les pratiques à risque en l’absence de précautions

Dans le fonctionnement quotidien des collectivités territoriales , certaines pratiques, bien qu’ancrées dans une logique de proximité, peuvent contrevenir au RGPD si elles ne s’accompagnent pas des [précautions juridiques nécessaires](#). C’est notamment le cas du croisement de fichiers à des finalités distinctes – par exemple, l’utilisation d’un fichier de participants à une réunion publique ou d’usagers d’un service municipal à des fins de communication électorale. Une telle réutilisation constitue un détournement de finalité prohibé par l’article 5, §1, b) du RGPD, sauf à recueillir le consentement explicite des personnes.

Or, compte tenu de la période préélectorale qui s'ouvrira le 1^{er} septembre prochain, un enjeu essentiel concerne la distinction entre communication institutionnelle (ex. newsletter municipale à partir d'un fichier administratif) et communication politique ou électorale (ex. promotion du mandat de l'élu sortant à l'approche d'un scrutin). En effet, la tentation est forte d'utiliser une base de contacts institutionnelle pour diffuser, en période électorale, un message politique ou un bilan de mandat. La CNIL l'a rappelé à plusieurs reprises : les fichiers constitués dans le cadre d'une mission de service public **ne peuvent pas servir des finalités personnelles ou électorales** sans violer les principes de loyauté, de transparence et de neutralité du service public.

Autre dérive fréquente : la conservation indéfinie de données (courriels d'administrés, fiches de rendez-vous, historiques d'intervention) sans limitation de durée. Or, en vertu de l'article 5, §1, e) du RGPD, les données doivent être conservées uniquement pour la durée strictement nécessaire à la finalité poursuivie.

Bonnes pratiques : sécuriser les usages

Pour prévenir tout risque juridique, les collectivités territoriales doivent adopter quelques règles simples mais essentielles. D'abord, séparer strictement les fichiers selon leur finalité : un fichier utilisé pour des actions institutionnelles ne peut servir à des fins politiques sans base légale distincte, le plus souvent le consentement de la personne intéressée doit être sollicitée.

Ensuite, informer systématiquement les administrés sur l'usage de leurs données (identité du responsable, finalité, durée, droits), conformément aux articles 13 et 14 du RGPD. Cette transparence est une condition de licéité du traitement.

Par ailleurs, tenir à jour un registre des traitements et identifier un interlocuteur en lien avec le DPO de la collectivité permettent d'assurer la traçabilité des pratiques et de répondre à tout contrôle.

Enfin, sensibiliser les membres du cabinet et les élus à ces enjeux est indispensable. Des supports de la CNIL existent (notamment sur les fichiers électoraux), et une charte ou une formation rapide en début de mandat peut suffire à prévenir les dérives.

En définitive, une gestion rigoureuse et transparente des données personnelles par les collectivités territoriales garantit non seulement la conformité juridique, mais aussi la confiance durable des administrés dans l'action publique locale.

David Conerardy , Avocat à la Cour,
Cabinet **Seban et Associés**

