

# Données personnelles : mutualiser pour se mettre en conformité

Les collectivités doivent appliquer depuis le 25 mai le nouveau règlement général sur la protection des données (RGPD). Zoom sur des bonnes pratiques.

**R**GPD. Ce sigle ne signifiait rien voici encore quelques mois dans beaucoup de collectivités (1). Et pourtant, les communes sont concernées par le règlement général européen sur la protection des données (RGPD), comme tous les organismes publics des 28 États membres, car elles gèrent des données sensibles comme l'état civil, l'action sociale ou encore les élections. Aussi la priorité est-elle à l'information sur les nouvelles obligations. À l'Agence landaise pour l'informatique (Alpi), parallèlement à des webconférences, le syndicat mixte a sensibilisé les agents « car, via les applications métiers qu'ils gèrent, ils sont les premiers impactés par le RGPD », explique Renaud Lagrave,

**250** collectivités sur les 570 qui adhèrent au syndicat mixte Alpi ont choisi un service de DPD mutualisé.

son directeur. « Sans oublier les élus car ce sont eux qui décideront des actions à entreprendre », ajoute Lionel Jouneau, maire de Saint-Perreux (56) à l'initiative d'un partenariat original associant Morbihan énergies, l'Université Bretagne Sud, l'Association des maires du Morbihan et le Centre départemental de gestion de la fonction publique territoriale. Le CDG 56 est au centre du dispositif car c'est la structure choisie pour accueillir le délégué à la protection des données personnelles (DPD) mutualisé. Ce DPD, rendu obligatoire par la réglementation, est mis à disposition de l'ensemble des collectivités qui le souhaitent. Lionel Jouneau est très satisfait d'avoir réussi à trouver « un mouton à cinq pattes, car le DPD doit

associer des compétences juridiques, informatiques et financières, pour ne pas pousser les collectivités à faire des investissements inconsidérés ». Le DPD mutualisé s'est également imposé à l'Alpi et sur ses 570 collectivités adhérentes, plus de 250 ont déjà choisi cette option. Le correspondant informatique et libertés (CIL) déjà en place sera bientôt épaulé par une seconde personne pour faire face à l'accroissement de la charge de travail.

## Le DPD ne peut être le DSI

L'Alpi propose une offre groupée intégrant la conformité administrative RGPD, un audit de sécurité et un accompagnement pour l'ouverture des données publiques. À Parthenay (79), la fonction de CIL était assumée par le directeur des systèmes d'information pour la commune et l'EPCI. « Pour éviter les conflits d'intérêt, le RGPD impose que le DPD ne soit pas un DSI. Aussi avons-nous décidé de recourir à un prestataire externe qui va initier la mise en conformité et former le futur DPD », explique François Gilbert, vice-président en charge des technologies de l'information et de la télécommunication de la communauté de communes de Parthenay-Gâtine. Ce prestataire, qui bénéficie du label CNIL, doit aider les communes à « documenter » leur conformité par la création d'un registre et d'une cartographie des applications. « Il s'agit de lister qui a accès à quelles applications pour quelles finalités, que cela soit depuis un ordinateur, un mobile ou une tablette », précise Lionel Jouneau. Mais il y a aussi un volet technique qui prend la forme d'un audit de sécurité des systèmes d'information. Pour faciliter la tâche des communes, l'Alpi a élaboré un questionnaire. « Il balai-



Avis d'expert

**Patrick Molinoz,** maire de Venarey-les-Laumes (21), président du Gip e-bourgogne-franche-comté, vice-président de l'AMF

« Pour le RGPD, nous proposons un accompagnement reposant sur un site internet dédié permettant une compréhension des enjeux. Aux explications générales sont associés des outils de suivi (recensement, registres, actions entreprises). Nous traitons par exemple l'état civil, la fiscalité locale, les info-lettres, l'aide sociale... Notre approche est assez ludique avec des « recettes », une sorte de Top Chef du RGPD ! Ensuite, la mise en conformité des communes exige du temps car il s'agit de recueillir, assimiler et analyser dans chaque commune les informations nécessaires au respect du RGPD... C'est une charge nouvelle à absorber pour laquelle il ne semble pas y

avoir d'accompagnement financier dédié de la part de l'État. Pour passer à cette étape, les communes ont besoin d'aide méthodologique et d'outils simples. Beaucoup de collectivités sont démarchées par des prestataires dont les messages, parfois alarmants, poussent à l'achat de « solutions » dont la validité n'a pas été éprouvée. Nos messages incitent à la prudence car il n'y a pas de retour d'expérience, c'est encore bien trop tôt. Nous allons animer un réseau de DPD afin de partager les pratiques et expériences régionales, notamment avec les centres de gestion qui, pour certains, proposent aux communes un DPD mutualisé comme nous l'envisageons aussi. »

tous les sujets – réseaux, poste de travail, applications métier, serveurs... – et a vocation à être réalisé sur place, par le DPD avec le référent communal », explique son directeur. Parmi les points de vigilance, la sécurité des accès au réseau sans fil et au poste de travail. « Dans une petite mairie où il n'y a qu'un seul ordinateur et une secrétaire de mairie trois heures par semaine, il n'est pas rare que le mot de passe soit inscrit sur un post-it et que tout le monde puisse accéder à tout du fait de la mémorisation des mots de passe dans le navigateur », pointe François Fouillet, directeur des systèmes d'information et de télécommunication de Parthenay. C'est à partir de cet état des lieux que sera

établi le diagnostic de conformité et la liste des actions à entreprendre pour sécuriser le système d'information. Pour certaines communes, l'addition pourrait s'avérer lourde et « sans aide de l'État » comme le souligne le président du GIP e-bourgogne-franche-comté et vice-président du conseil régional en charge du numérique, Patrick Molinoz (lire ci-dessus). Au-delà des logiciels et accès réseau, c'est toute une série de pratiques qui vont devoir évoluer comme l'usage de serveurs non sécurisés pour les mails, les documents, certaines bases de données... Dans les Landes, les communes pourront s'appuyer sur les experts techniques du syndicat mixte Alpi pour la mise en

**Ce que dit la loi** Le règlement a été adopté par le Parlement européen le 14 avril 2016 après 4 ans de négociations et s'est appliqué dans les 28 États européens le 25 mai 2018. La loi relative à la protection des données personnelles, complétant certaines dispositions du RGPD, a été adoptée définitivement par l'Assemblée nationale, le 14 mai. Les députés n'ont pas retenu le régime dérogatoire que le Sénat avait voté pour les collectivités : exonération des sanctions financières (comme l'État) et création d'une aide à la mise en conformité. Ils ont aussi rétabli la majorité numérique à 15 ans et non 16 ans comme le souhaitent les sénateurs. Les sénateurs ont saisi le Conseil constitutionnel le 16 mai, suspendant l'application de la loi, ce qui n'empêche pas le RGPD de s'appliquer.

## En savoir +

- Textes de référence et guides RGPD de la CNIL : <https://www.cnil.fr/fr/rgpd-par-ou-com-mencer>
- Alpi. Tél. 05 58 85 81 90. [www.alpi40.fr/](http://www.alpi40.fr/)
- Parthenay. Tél. 05 49 94 03 77.
- Saint-Perreux. Tél. 02 99 71 19 81.
- Gip e-bourgogne-franche-comté. Tél. 0970 609 909. [www.e-bourgogne.fr/](http://www.e-bourgogne.fr/)

conformité. Mais dans beaucoup de communes, ces ressources techniques font défaut. C'est la raison pour laquelle le partenariat initié dans le Morbihan intègre l'Université Bretagne Sud qui pourra fournir aux communes des étudiants en sécurité des systèmes d'information. Enfin, si la sécurisation a un coût, « elle va bénéficier aussi aux administrés dont il s'agit de protéger les données personnelles », souligne François Gilbert.

## Adopter la protection par défaut

Au-delà de la mise en conformité, le RGPD oblige les communes à intégrer la problématique « données personnelles » à tous leurs projets numériques et à réaliser, si nécessaire, des études d'impact sur la vie privée. Il s'agit en effet de veiller à ne pas créer de nouvelles failles de sécurité lors de la mise en place de nouveaux services. Le principe promu par le RGPD est celui de la « privacy by design », c'est-à-dire d'une protection des données personnelles intégrée lors de la création du logiciel. Pour les applications métiers du marché, ce travail de mise en conformité sera pris en charge, au moins en théorie, par les éditeurs que le RGPD rend désormais coresponsables des traitements. Il devra faire partie des critères de sélection des solutions informatiques dans les marchés publics. Mais cela concerne aussi tous les développements informatiques internes. « À Parthenay, les recommandations du RGPD ont été intégrées en amont à notre logiciel de gestion de la relation citoyen en cours de finalisation », explique le DSI. Mais Parthenay est un cas un peu particulier, étant devenue au fil du temps un laboratoire de la dématérialisation. La prise en compte du RGPD « au quotidien et en continu » est en définitive le véritable défi du règlement. Le réflexe RGPD mettra sans doute plusieurs années à entrer dans les mœurs des collectivités : l'urgence des structures de mutualisation est donc pour le moment que toutes les communes entament le processus. **Olivier DEVILLERS**

(1) Lire l'entretien avec Alice de la Mure, juriste à la Commission nationale de l'informatique et des libertés, dans *Maires de France*, n° 357, mai 2018, p. 27.

