



Site internet et plateformes municipales : Obligation de conformité et souveraineté des données

À l'ère numérique, la transition des services et des données communales vers le web ne s'improvise pas. Entre simple vitrine d'information et traitement de données sensibles, le cadre légal et technique impose une rigueur absolue pour protéger la collectivité et ses administrés.

Lorsqu'une commune met en place un site internet, un portail citoyen ou un outil de gestion, toutes les pages web et tous les outils ne se valent pas. Il est indispensable de distinguer la simple communication publique des systèmes hébergeant des informations à caractère sensible.

1. Le distinguo fondamental : Site vitrine vs. Données sensibles

- **Le site de présentation au public (Vitrine) :** Il s'agit des pages d'information générale (horaires de la mairie, actualités, présentation du village, formulaires de contact basiques). Les exigences portent principalement sur les mentions légales (LCEN), l'accessibilité et la protection des données personnelles de base (RGPD).
- **Les plateformes de données sensibles et de gestion :** Dès que le site ou le portail manipule des données à caractère personnel des administrés (état civil, dossiers d'urbanisme, inscriptions scolaires, données fiscales locales, correspondances administratives confidentielles ou systèmes ERP municipaux), on bascule sur des **données sensibles** au sens du droit de la protection des données et de la sécurité des systèmes d'information.

2. L'exigence technique majeure : Le stockage sur des hébergeurs SecNumCloud

Pour les données sensibles des collectivités, la législation et les doctrines de sécurité de l'État (notamment la doctrine "Cloud au Centre") imposent des standards très élevés :

- **La qualification SecNumCloud (ANSSI) :** Les données sensibles des mairies doivent être hébergées sur des infrastructures cloud qualifiées **SecNumCloud** par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Cette certification garantit que l'hébergeur est immunisé contre les législations extraterritoriales (comme le *Cloud Act* américain) et qu'il respecte les plus hauts standards de sécurité contre les cyberattaques.
- **Comment vérifier et se renseigner sur les prestataires certifiés ?** Il ne suffit pas qu'un prestataire commercial se dise "sécurisé" ou "français". Pour s'assurer qu'un hébergeur

répond rigoureusement au référentiel SecNumCloud, les élus et les services techniques doivent consulter les sources officielles :

- **Le catalogue officiel des produits et services qualifiés (CPSP) de l'ANSSI :**
Accessible directement sur le site de l'ANSSI (<https://cyber.gouv.fr>), ce répertoire répertorie de manière publique et actualisée la liste officielle de tous les prestataires et solutions ayant obtenu la qualification SecNumCloud.
- **Le site de référencement GIP RECIA ou les centrales d'achat publiques spécialisées :**
Qui exigent et vérifient ces certifications pour les marchés publics informatiques.
- *Règle d'or* : Si un prestataire ne figure pas nommément sur la liste officielle des qualifiés SecNumCloud de l'ANSSI, l'hébergement de données sensibles ou d'administrés est juridiquement et techniquement non conforme.
- **L'interdiction des hébergements grand public non souverains :**
Stocker des fichiers administratifs sensibles ou des données d'administrés sur des serveurs mutualisés classiques (type hébergement web standard bas coût ou grands acteurs américains non souverains) constitue une faille majeure de conformité.

3. Les risques en cas de manquement (pour la Mairie et le Prestataire)

Faire l'impasse sur ces exigences techniques expose lourdement les parties prenantes :

- **Pour la Mairie (l'exécutif local) :**
 - *Sur le plan administratif et de la responsabilité* : Une violation de données ou un stockage non sécurisé expose la commune à des sanctions de la CNIL (pouvant aller jusqu'à de lourdes amendes administratives pour les organismes publics récalcitrants).
 - *Sur le plan de la sécurité* : En cas de fuite de données (ransomware, exfiltration), la responsabilité du maire peut être engagée pour manquement à son obligation de protection des données des administrés.
- **Pour le Prestataire (l'entreprise ou l'intégrateur) :**
 - *Sur le plan contractuel et pénal* : Un prestataire qui s'engage auprès d'une mairie en proposant un hébergement non conforme ou en maquillant la souveraineté de son infrastructure engage sa **responsabilité civile contractuelle** pour manquement à son obligation de conseil et de résultat.
 - *En cas de compromission* : Si l'infrastructure s'avère poreuse et que le prestataire a certifié des garanties qu'il ne respecte pas (notamment l'utilisation de serveurs non certifiés SecNumCloud alors que le marché l'exigeait), sa responsabilité pénale peut être recherchée pour mise en danger ou négligence coupable dans le traitement de données publiques.

Conclusion

La transition numérique d'une commune ne peut reposer sur de l'amateurisme technique. Qu'il s'agisse d'un simple site d'information ou d'une infrastructure de gestion hébergeant des données sensibles, la transparence, le respect des qualifications de l'ANSSI (SecNumCloud) et la rigueur contractuelle sont les seuls remparts contre l'arbitraire et l'insécurité numérique.