RGPD ET CYBERSECURITE

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DES PYRÉNÉES-ORIENTALES

RÉFÉRENCES JURIDIQUES

Règlement Général sur la Protection des Données (RGPD)
·Directive NIS 2 (Network and Information Security Directive)
·Loi Informatique et Libertés
·CNIL - Guide de la sécurité des données personnelles
ANSSI - Bonnes pratiques en cybersécurité

COLLECTIVITÉS ET CYBERSÉCURITÉ

Les collectivités territoriales gèrent quotidiennement un grand nombre de données personnelles, ce qui les rend particulièrement vulnérables aux cyberattaques. Le respect du RGPD et de la directive NIS 2 implique de mettre en place des mesures de cybersécurité afin de protéger ces informations et d'assurer la conformité réglementaire.
L'augmentation des cyberattaques contre les mairies et les administrations locales est une réalité.

Les menaces les plus courantes incluent :

- **Le phishing** : tentatives d'hameçonnage pour dérober des données sensibles.
- **Les ransomwares** : blocage des systèmes informatiques avec demande de rançon.
- L'exploitation des **failles de sécurité** des logiciels et applications.

Face à ces risques, les collectivités doivent adopter des pratiques strictes pour garantir la sécurité des données personnelles des citoyens.

LA PROCÉDURE

Le RGPD et la directive NIS 2 imposent des mesures de sécurité strictes pour la protection des données personnelles et des systèmes d'information critiques. Parmi les obligations principales :

· **Gestion des accès** : Limiter l'accès aux données aux seuls agents habilités.
· **Chiffrement et anonymisation** : Rendre les données illisibles en cas de vol.
· **Mise à jour des systèmes** : Appliquer régulièrement les correctifs de sécurité.
· **Sensibilisation du personnel** : Former les agents aux bonnes pratiques en matière de cybersécurité.
· **Plan de réponse aux incidents** : Prévoir une procédure en cas de cyberattaque pour réagir rapidement.
· **Mise en conformité avec la directive NIS 2** : Renforcement des exigences de cybersécurité, notamment pour les infrastructures critiques et les administrations publiques.

LA RESPONSABILITÉ DES AGENTS ET ÉLUS DES COLLECTIVITÉS

Les acteurs des collectivités territoriales doivent appliquer ces mesures :

· Adopter une **politique de mots de passe** robustes et ne pas les partager.

· Ne pas ouvrir de **mails suspects** ou cliquer sur des liens non vérifiés.

· Effectuer des **sauvegardes régulières** et les stocker sur un support sécurisé.

· Signaler tout **incident de sécurité** au RSSI ou au DPO (Délégué à la Protection des Données).

· Conformité avec NIS 2 : **Déclaration obligatoire** des incidents majeurs auprès des autorités compétentes.

CAS PARTICULIER

Usage des outils numériques :

- Privilégier des solutions souveraines ou conformes au RGPD.
- Restreindre l'utilisation des services cloud non conformes.

Protection des données des administrés :

- Informer les citoyens sur la sécurité de leurs données.
- Permettre l'exercice de leurs droits (accès, rectification, suppression).

COMMENT GÉRER UN INCIDENT DE CYBERSÉCURITÉ ?

1. Identifier rapidement l'incident et isoler les systèmes impactés.
2. Informer le DPO et les autorités compétentes (CNIL en cas de fuite de données, autorités de régulation pour NIS2)
3. Analyser l'origine de l'attaque et renforcer les mesures de sécurité.
4. Communiquer en toute transparence avec les administrés si leurs données sont concernées.

EN CONCLUSION ?

La cybersécurité est un enjeu majeur pour les collectivités territoriales. L'adoption de bonnes pratiques et le respect du RGPD ainsi que de la directive NIS 2 permettent de protéger efficacement les données des citoyens tout en préservant la conformité réglementaire.

QUE RISQUE-T-ON EN CAS DE NON-RESPECT DU RGPD ET DE LA CYBERSÉCURITÉ ?

Sanctions financières : Jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial pour une collectivité en cas de violation grave.

Responsabilité juridique des agents et élus : Possibilité d'engagement de leur responsabilité en cas de faute.

Atteinte à la confiance des citoyens : Une fuite de données peut entacher l'image de la collectivité et provoquer une perte de confiance.

Perte de bases de données des collectivités : Une cyberattaque peut entraîner la destruction ou l'altération irréversible des données essentielles au fonctionnement des services publics.

Obligation de déclaration sous NIS 2 : En cas de manquement, des sanctions spécifiques peuvent être appliquées aux infrastructures critiques et administrations concernées.

INFORMATIONS IMPORTANTES

Droits et devoirs des administrés :
Droit à l'information sur la collecte et l'utilisation de leurs données.
Possibilité de demander la suppression ou la correction de leurs données.
Signalement des violations de données à la CNIL en cas de non-respect.