VIDÉO 4 / 6
L'application concrète des principes du RGPD : minimisation des données, conservation des données et mise en sécurité

Les 6 grands principes du RGPD sont les suivants :

- Le traitement doit être licite
- La finalité légitime du traitement
- Les données strictement nécessaires et pas plus !
- La durée limitée de conservation des données
- La sécurité des données personnelles
- L'information des personnes

Voyons concrètement, comment se traduisent les principes de minimisation des données, de conservation et de sécurité dans les activités quotidiennes d'une collectivité territoriale.

Le principe de minimisation des données

Le principe de minimisation des données signifie que la collecte des données personnelles doit être proportionnée et pertinente par rapport à la finalité du traitement.
On ne doit collecter que les données personnelles strictement nécessaires et pas plus !
En outre, ces données pour être pertinentes lors du traitement, doivent être de qualité et régulièrement mises à jour. Cela implique une organisation au sein de la collectivité pour s'assurer que le processus, de la collecte, jusqu'à l'exploitation, puis, le cas échéant la destruction (ce que l'on appelle le cycle de vie de la donnée) permettra de disposer systématique d'une donnée juste et fiable.
Donc moins il y aura de données, plus cette démarche qualité sera facile à mettre en œuvre.
Le principe de minimisation, au-delà de l'obligation liée à l'usage de la donnée personnelle, est finalement un axe fort d'une gestion administrative simplifiée et efficiente !

Exemple : le numéro de sécurité sociale d'un enfant n'est pas nécessaire pour l'inscription à une activité péri ou extra scolaire, puisqu'en cas d'accident, la prise en charge par les secours sera effective, que l'administration dispose ou non de cette donnée !
La date de naissance n'est pas non plus utile à la collecte d'une base d'administrés pour diffuser la lettre d'information communale. Et si des contenus spécifiques devaient être valorisés, alors seule la tranche d'âge pourrait suffire !

Les questions à se poser

- Quelles sont les données indispensables pour ce que je dois faire (instruire un dossier, organiser un événement, informer des administrés)

- Ai-je le droit de les collecter ? S' il s'agit de données dites sensibles, (santé, appartenance politique, syndicale ou religieuse par exemple) je ne peux le faire que dans des conditions bien spécifiques et très contraintes.

La durée de conservation des données

Les données personnelles collectées ne peuvent être conservées indéfiniment. A l'issue de leur durée d'exploitation, elles doivent être détruites ou archivées si elles représentent un intérêt pour la recherche, l'histoire ou la généalogie.
Dans ce cas, le service départemental d'Archives est votre partenaire pour définir les modalités de cet archivage.

Les durées sont parfois fixées par des textes (par exemple il faut conserver les bulletins de salaire 5 ans ou les images de vidéo-surveillance ne peuvent être conservées qu'un mois maximum) mais le plus souvent ce n'est pas le cas. C'est au responsable de traitement de les déterminer avec l'aide du DPO, de la CNIL qui peut émettre des recommandations et avec les services des archives. On peut retenir la bonne pratique d'une conservation liée à l'usage mais il sera toujours nécessaire de vérifier si d'autres considérations, notamment archivistiques, doivent également être prises en compte.

Focus sur le cycle de vie de la donnée

On considère 3 grandes étapes dans l'usage des données :

1- L'étape de l'utilité courante : la donnée est alors facilement accessible, dans une application métier (par exemple un logiciel, un fichier excel), bien sûr dans cette étape, en fonction de la nature de la donnée et des finalités de traitement, tout agent public n'est pas forcément habilité à les consulter, c'est typiquement l'exemple de l'état civil.

2- L'archivage intermédiaire : il peut être parfois nécessaire de conserver les données personnelles un certain temps après les avoir utilisées, par exemple lorsqu'elles peuvent constituer des éléments importants dans un contentieux. Dans ce cas, elles doivent être conservées sur un support ou dans un espace distinct de celui utilisé dans l'étape d'utilité courante.
On ne peut par exemple conserver dans un même fichier numérique ou dans un même dossier papier, des données "en cours" et les données "pré-archivées". Car les accès aux informations "pré-archivées" sont également plus restreints.

3- L'archivage : dans la seule hypothèse où le service des Archives considère un intérêt patrimonial à ces données, elles ne seront pas supprimées. Dans tous les autres cas, elles doivent être détruites à l'issue de leur utilisation.

La sécurité des données personnelles

Les données personnelles doivent être protégées de plusieurs risques :
- la cyberattaque
- la panne

- le sinistre
- les erreurs
- les accès non autorisés

Compte tenu des impacts que leur altération, disparition ou communication, peuvent avoir sur la vie des personnes (ne plus percevoir une aide financière, des soins ou être exposé à des manipulations ou pressions), les collectivités doivent être vigilantes à leur protection.
La sécurité sera bien sûr proportionnée aux finalités et aux catégories de données concernées et l'on n'exige pas les mêmes modalités pour un service de police municipale que pour un service d'animation et de loisirs.
La sécurité doit être une démarche au long court : c'est un processus continu et permanent, qui concerne autant des données numériques que des documents papiers.
La mise en sécurité des données s'appuie à la fois sur des mesures techniques et organisationnelles.

Les mesures techniques : la sécurisation des locaux par verrou ou alarme, la protection des locaux des risques incendie, le verrouillage des sessions sur les ordinateurs, une bonne gestion des mots de passe, les sauvegardes régulières pour assurer une continuité de service en cas de perte ou indisponibilité, le chiffrement ou la pseudonymisation des données lors des transmissions…

Les mesures organisationnelles : la gestion des droits d'accès aux données (avec un suivi des arrivées-départs au sein de la collectivité pour éviter de laisser des accès "actifs" si l'agent n'est plus dans la collectivité), la sensibilisation de l'ensemble des agents sur les risques, l'examen systématique de toute demande de transmission de données personnelles…

Des guides de la CNIL et de l'ANSSI sont disponibles pour accompagner les démarches de sécurisation des données.

Les questions à se poser

- Les comptes utilisateurs internes permettant d'accéder à des données personnelles sont-ils protégés par des mots de passe d'une complexité suffisante ?
- Les accès aux locaux sont-ils sécurisés ?
- Des profils distincts sont-ils créés selon les besoins pour accéder aux données ?
- Existe-t-il une procédure de sauvegarde et de récupération des données en cas d'incident ?

Focus sur les droits d'accès

Il est important de s'assurer au sein d'une commune que seules les personnes habilitées, agents ou élus, puissent avoir accès aux données personnelles.
Par ailleurs, en cas de demande de transmission par des tiers, il est capital de procéder à des vérifications :

- ce tiers est-il autorisé, par un texte, à demander ces données ?
- l'identité de la personne à l'origine de la demande est-elle fiable ? (on peut par exemple systématiquement rappeler le standard de l'organisme et vérifier ainsi les fonctions et l'existence du demandeur)

La transmission des données sollicitées doit se faire dans les meilleures conditions de sécurité technique. On ne pourra pas par exemple envoyer par simple mail des données sensibles.

Bonnes pratiques

Lors de l'envoi de mails en grand volume depuis une messagerie, et à des destinataires qui n'ont pas de lien entre eux, c'est le champ "CCI:" et non "CC:" ou "A:" qui doit être utilisé ! Ainsi il n'y a pas accès aux mails destinataires de l'envoi.

Si vous utilisez des outils de mailing, un lien de désabonnement ou un mail de contact doit être prévu afin que la personne puisse s'opposer à l'envoi.

On n'écrit jamais un mot de passe sur un post-it laissé à la vue de tous !

À RETENIR

Les grandes principes du RGPD sont finalement liés à la finalité du traitement et en fonction de celle-ci :

- On ne doit collecter que les données personnelles strictement nécessaires et pas plus !
- On doit avoir une vision claire de la durée de conservation des données et de leur éventuelle destruction, en partenariat avec le service départemental des Archives qui seul pourra se prononcer sur l'intérêt patrimonial d'une conservation
- On doit enfin assurer la sécurité des données contre tout risque de perte, d'altération ou de "détournement" d'usage.

Retrouvez toutes les vidéos du Parcours RGPD sur osinumterritoires.fr

Ressource pédagogique produite par **Médias-Cité** et **INNIZ**

avec le soutien de

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

anct agence nationale de la cohésion des territoires

FRANCE RELANCE

Financé par l'Union européenne
NextGenerationEU