VIDÉO 2 / 6
Données personnelles, sensibles et traitements : de quoi parle-t-on ?

Pour comprendre le règlement général sur la protection des données personnelles et son application, il est nécessaire de comprendre ce qu'est une donnée personnelle, ce qu'est une donnée sensible, ce que l'on entend par "traitement de données" et "responsable de traitement", ce qu'est un Délégué à la Protection des Données (DPO).

Données personnelles

Sont considérées comme des données personnelles, des données

- directement identifiables : nom, prénom, email, photographie, vidéo
- indirectement identifiables : identifiant ou matricule, téléphone, code postal, numéro de sécurité sociale car en les croisant avec d'autres informations il est possible de retrouver l'identité d'une personne

Exemple : le scan des plaques d'immatriculation dans le cadre du recouvrement des paiements de stationnement est une collecte de données personnelles.

Données sensibles

Sont considérées comme des données sensibles, toutes données en lien avec la santé des personnes, leurs opinions, leur appartenance syndicale, politique ou religieuse, leur origine ethnique, leurs données génétiques, le numéro de sécurité sociale ou les données relatives aux condamnations pénales.
Leur encadrement est très strict. Seules certaines activités très limitées (soins à la personne, évaluation sociale d'une situation, instruction judiciaire par exemple) permettent leur collecte.

Bonne pratique : en matière de restauration scolaire, il est préférable de préciser la conduite à tenir, régime sans viande, plutôt que régime kasher qui fait référence à une appartenance religieuse.

Le traitement de données personnelles

Le traitement recouvre toute opération effectuée à l'aide de procédés automatisés ou pas, appliqués à des données personnelles. Et il y en a beaucoup !
Les inscriptions à la cantine scolaire, les inscriptions à des activités proposées par la mairie, l'envoi de la gazette municipale, l'état civil… ce sont tous des traitements de données personnelles.

Qui sont les responsables du traitement dans une collectivité ?

Il s'agit du maire mais également des éventuels sous-traitants de la commune : par exemple un sous-traitant de la paye des agents, un sous-traitant pour de la vidéo surveillance. Dans ce dernier cas, il convient, au travers d'un contrat, de bien clarifier les responsabilités du responsable et du sous-traitant qui, tous deux, doivent appliquer les principes du RGPD.

Les responsabilités sont dans ce cas à clarifier dans un contrat liant un responsable à un sous-traitant :

- Qui répond à une demande d'une personne dont on traite les données ? (droit d'accès, de rectification ou d'opposition par exemple)
- Qui informe les personnes sur les différents aspects du traitement ?
- Qui réalise les analyses d'impact sur la protection des données personnelles lorsqu'elles sont requises ?
- Qui met en œuvre les principes de sécurité des données personnelles ?

Le responsable de traitement est ainsi le garant, de manière très opérationnelle, du respect des 6 grands principes du RGPD, à savoir :

- La légalité du traitement
- 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

Cela suppose ainsi de "tracer" les événements et de "documenter" les traitements, avec certains outils comme les registres de traitements, les registres d'incidents ou les analyses d'impact sur la protection des données personnelles.

Qui est le Délégué à la protection des données ou DPO et quel est son rôle ?

Le Délégué à la protection des données ou DPO est un acteur clé. Il est obligatoire de le nommer dans toute collectivité, quelle que soit sa taille.
Il remplit quatre missions :

- Informer et sensibiliser sur les principes du RGPD
- Conseiller le responsable de traitement sur les mesures de mise en conformité nécessaires. Il peut, par exemple proposer des mesures techniques et organisationnelles de protection et de mise en sécurité des données, accompagner sur la méthode permettant de réaliser les Analyses d'Impact sur les Données Personnelles (AIDP) que le responsable de traitement peut être amené à conduire, proposer des mentions types d'information...
- Contrôler que les traitements s'appuyant sur des données personnelles sont conformes. A ce titre, il tient un registre des traitements.
- Etre un point de contact, à la fois pour la CNIL mais également pour les personnes qui exercent leurs droits.

Aucun profil, certification ou modalités de désignation ne sont imposés pour nommer un DPO.

Cela peut être un agent de la collectivité, formé pour cela, un avocat, un prestataire mutualisé entre plusieurs collectivités.
Mais la personne exerçant cette responsabilité doit avoir suffisamment de disponibilité, être en situation d'indépendance et disposer de connaissances et de ressources ainsi que d'une forte déontologie.

Bonne pratique : un directeur général, un élu ne peuvent être désignés DPO puisqu'ils participent aux décisions relatives à la mise en œuvre de traitement de données.
De même, nommer un secrétaire de mairie doit rester compatible avec la possibilité d'exercer cette mission et d'être donc disponible.
Un avocat qui défend la collectivité ne peut pas non plus exercer cette mission compte tenu du risque de conflit d'intérêt. Le DPO doit être indépendant dans l'exercice de sa mission.

À RETENIR

Le RGPD pose un principe de protection "par défaut", c'est-à-dire de protection systématique, obligatoire, dont on doit pouvoir prouver la réalité concrète, à n'importe quel moment, lorsque l'on réalise des traitements sur des données personnelles.
Cela impose de documenter ces traitements avec des registres de traitement et des Analyses d'Impact sur les Données Personnelles (AIPD) notamment.

Le responsable du traitement ainsi que ses éventuels sous-traitants doivent appliquer les principes du RGPD. Dans une collectivité, le responsable de traitement est le maire.

Le Délégué à la protection des données doit être désigné dans chaque collectivité car il est le garant de la conformité RGPD au sein de la structure et assiste le responsable de traitement dans sa mission. Le DPO peut éventuellement être mutualisé.

Retrouvez toutes les vidéos du Parcours RGPD sur osinumterritoires.fr

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

avec le soutien de

REPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

anct agence nationale de la cohésion des territoires

FRANCE RELANCE

Financé par l'Union européenne
NextGenerationEU