Association Nationale des Directeurs
et Directeurs-Adjoints des Centres De Gestion
de la Fonction Publique Territoriale

FICHE N° 3 /

Archives et RGPD

Fiche n° 3
ARCHIVES ET RGPD

Pourquoi et comment gérer les données à caractère personnel ? Quel(s) impact(s) sur les archives ?

Les données sont considérées à caractère personnel dès lors qu'elles permettent d'identifier directement ou indirectement une personne. Elles doivent être collectées pour atteindre une finalité bien précise, explicite et légitime. En collectivité, on les retrouve dans les activités liées aux ressources humaines, à l'urbanisme, à l'action sociale (...). Le Règlement Général sur la Protection des Données (RGPD) harmonise au niveau européen la législation en la matière. Transposé en droit français le 20 juin 2018, il contraint les responsables de traitements (maires, présidents d'EPCI ou de syndicats) de se mettre en conformité vis-à-vis du texte, de garantir la transparence de leurs traitements, de sécuriser et de protéger les données à caractère personnel des citoyens.

Les collectivités territoriales, quelle que soit leur taille, sont concernées par cette nouvelle loi, comme toutes les personnes morales traitant des données personnelles, sous peine de sanctions administratives, financières et pénales. L'élu et le sous-traitant peuvent faire l'objet de sanctions administratives et de sanctions pénales.
En cas de non-conformité, le risque est aussi ailleurs : réputation, image, perte de confiance, climat social.

Mettre en œuvre le cycle de vie d'un document contenant des données à caractère personnel

1. Cartographier et recenser auprès des services producteurs les typologies documentaires (papiers, documents bureautiques, listings de contacts,...).
2. Définir les délais d'effacement et le sort final des documents.
3. Etablir des tableaux de gestion des données à caractère personnel pour chaque traitement, en mentionnant le type de support sur lequel il est conservé (plan de classement ou logiciel sur serveur informatique, dossier physique,...).

4. Etablir un plan de classement des documents numériques et effectuer un inventaire des archives papier.
5. Mettre en œuvre les procédures d'archivage des documents. (encadrer les versements et les éliminations, la communicabilité des informations, leur accès ultérieur, …).

Je veux mettre ma collectivité en conformité, que dois-je faire ?

- Je nomme obligatoirement un DPO en interne, via un prestataire ou encore une structure mutualisée.
- Je le déclare auprès de la CNIL.
- Je cartographie les traitements de données à caractère personnel papier et numériques (dont les e-mails) existants au sein de mes services.
- J'élabore le registre des traitements obligatoire et je répertorie les actions à mener pour me mettre en règle.
- J'analyse les données sensibles et j'engage, le cas échéant, une étude d'impact en vue d'apporter les améliorations spécifiques nécessaires à une meilleure gestion avant tout traitement.
- J'élabore et je mets en œuvre des procédures internes afin de permettre aux citoyens d'exercer leurs droits auprès de ma collectivité (information, accès,…).
- Je sensibilise les agents aux nouvelles pratiques.
- Je révise les formulaires qui contiennent ou permettent de collecter des données à caractère personnel et je limite leur collecte au strict nécessaire pour atteindre la finalité de la mission (formulaires d'inscription, saisines par voie électronique…).
- J'analyse l'efficacité des processus d'archivage en place (inventaire des archives papier, tableaux de gestion répertoriant également les typologies documentaires contenant des données à caractère personnel, plan de classement informatique, …).
- J'audite le niveau de sécurité de mon système d'information (sécurisation de l'accès aux données sur le serveur informatique par identifiant et mot de passe uniques, gestion des certificats relatifs au site Internet en https://, …).
- Je documente ma conformité.
- Je m'assure que les entreprises sous-traitantes avec lesquelles j'ai contracté stipulent dans leurs contrats les dispositions mises en œuvre pour être en conformité en matière de protection des données personnelles.

Foire aux questions

• Ai-je le droit de ne pas engager ma collectivité dans une démarche de mise en conformité RGPD ?

NON, l'obligation de tenir un registre des traitements concerne tous les organismes, publics comme privés, quelle que soit leur taille, dès lors qu'ils traitent des données personnelles.

Par mesure de protection, certains documents particulièrement fragiles, anciens ou souvent consultés, sont numérisés et mis en ligne sur le site internet de la collectivité. Les originaux ne sont alors plus consultables.

• Les entreprises sous-traitantes avec lesquelles je travaille peuvent-elles aussi être considérées comme responsables du traitement ?

NON, mais votre responsabilité peut être engagée en cas de non-surveillance des activités du sous-traitant. Des clauses spécifiques doivent donc être ajoutées dans les contrats que vous passez avec ces entreprises dans le cas où elles sont amenées à collecter et à traiter des données personnelles pour le compte de votre collectivité.
Doivent être définis l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel collecté, les catégories de personnes concernées, les obligations et les droits du responsable du traitement.

La durée de conservation de ces données doit également être mentionnée clairement. (https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses).

• Suis-je dans l'obligation de nommer un DPO ?

OUI, la désignation d'un Délégué à la Protection des Données est obligatoire pour :

- Les autorités et organismes publics (ministères, collectivités territoriales, établissements publics, ...).
- Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle (compagnies d'assurance, banques pour leurs fichiers clients, ...).

- Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites "sensibles" (données biométriques, génétiques, relatives à la santé, la vie sexuelle, l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale) ou relatives à des condamnations pénales et infractions.

Dans les autres cas, la désignation d'un Délégué à la Protection des Données est encouragée par la CNIL.

• Le maire d'une collectivité peut-il être nommé DPO ?

NON, car en tant que responsable de traitement, le maire d'une commune ne peut pas être désigné comme délégué à la protection des données. Ces deux rôles sont par définition distincts, le responsable du traitement devant désigner le DPO, et les rôles qui leur sont attribués par le RGPD étant différents.

Etant spécifiquement tenu de contrôler la régularité de ces traitements, le délégué doit bénéficier d'une certaine indépendance vis-à-vis du responsable de traitement, et ne pas se trouver en situation de conflit d'intérêts dans l'exercice de sa mission (art. 38).

Liens utiles :

https://www.cnil.fr/fr/RGPD-quel-impact-pour-les-collectivites-territoriales
https://www.cnil.fr/fr/designation-dpo
https://www.cnil.fr/fr/modeles/courrier
https://www.cnil.fr/fr/les-sanctions-penales
https://www.cada.fr