Centre de Gestion de la Meuse

FONCTION PUBLIQUE TERRITORIALE 55

C I R C U L A I R E 5.2018 - avril 2018

APPLICATION DU RGPD

Références : *règlement de l'union européenne n° 2016/679 du 27avril 2016 relatif à la protection des données à caractère personnel,*
loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés,
loi n° 84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale,
décret n° 85-643 du 26 juin 1985 relatif aux centres de gestion institués par la loi n° 84-53 du 26 janvier 1984,
décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données abroge la directive 95/46/CE (règlement général sur la protection des données).

Ce texte organise et harmonise la protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel.

La disposition européenne est en cours de transposition dans notre droit interne. Ceci se traduira par une modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

I – QUELQUES DEFINITIONS

Ces définitions sont issues de l'article 4 du RGPD, relatif aux définitions :

- **données à caractère personnel :** toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; une personne physique est identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

- **traitement :** toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

- **responsable du traitement :** la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union européenne ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union européenne ou par le droit d'un État membre ;

- **représentant :** une personne physique ou morale établie dans l'Union, désignée par écrit par le responsable du traitement ou le sous-traitant, en vertu de l'article 27 et qui le représente en vertu du présent règlement ;

- **sous-traitant** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

II - LES OBLIGATIONS DES COLLECTIVITES

1) La protection des personnes physiques

Le RGPD pose le principe de la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant, du respect de leurs libertés et droits fondamentaux. Les autorités publiques sont soumises au respect de ces obligations pour toutes les personnes : agents, administrés, élus, …

2) La sécurisation des données informatiques

L'article 25 relatif à "la protection dès la conception et protection des données par défaut" définit les concepts et les niveaux de certifications des sécurisations nécessaires pour la protection des données à caractère personnel (pseudonymisation, anonymisation, cryptage des données, …), de même que l'obligation de mise en place.

3) La sécurisation des données sur support matériel

L'article 32 relatif à "la sécurité du traitement" visant à garantir la sécurisation des données sur support matériel.

4) Etablissement de la cartographie des traitements et rédaction du registre des traitements

L'article 30 impose un "registre des activités de traitement" ; une cartographie des traitements doit être réalisée en aval et un registre édité par traitement.

5) Eventuelles études d'impact sur la vie privée

Le chapitre IV section 3 du RGPD relatif à "l'analyse d'impact relative à la protection des données et consultation préalable", prévoit un logiciel fournit par la CNIL nommé PIA (Privacy Impact Assesment)

6) Communication des violations de données à caractère personnel

Les articles 33 et 34 sur la violation des données à caractère personnel, rappellent que le responsable de Il impose l'obligation de tenir un registre des violations de données à caractères personnel.

7) Droits spécifiques

Le responsable de traitement doit s'assurer du respect du chapitre III, section 3 "Rectification et effacement".

8) Editions de procédures

Conformément au chapitre III, section 3 et aux articles 33 ; 63 et suivants, le délégué à la protection des données met en place des procédures permettant à la collectivité ou à l'établissement public de se mettre en conformité avec les textes.

III - LE DELEGUE A LA PROTECTION DES DONNEES (DPD)

Au chapitre IV, la section 4 du RGPD est dédiée au délégué à la protection des données.

1) Article 37 relatif à la désignation du délégué à la protection des données :

   - toute administration a l'obligation de nommer un DPD,
   - le DPD peut être désigné en interne ou être mutualisé,
   - le DPD est nommé sur la base de ses qualités professionnelles et en particulier sur ses connaissances en droits et en sécurité informatique(formations spécifiques) .

2) Article 38 relatif à la fonction du DPD :

   - le responsable du traitement permet au DPD d'accomplir sa mission en lui fournissant les ressources nécessaires,
   - le DPD ne peut être relevé de ses fonctions ou pénalisé par le responsable de traitement dans le cadre de ses missions,
   - le responsable de traitement veille à ce que le DPD ne soit pas en situation de conflit d'intérêts.

3) Article 39 relatif aux missions du DPD :

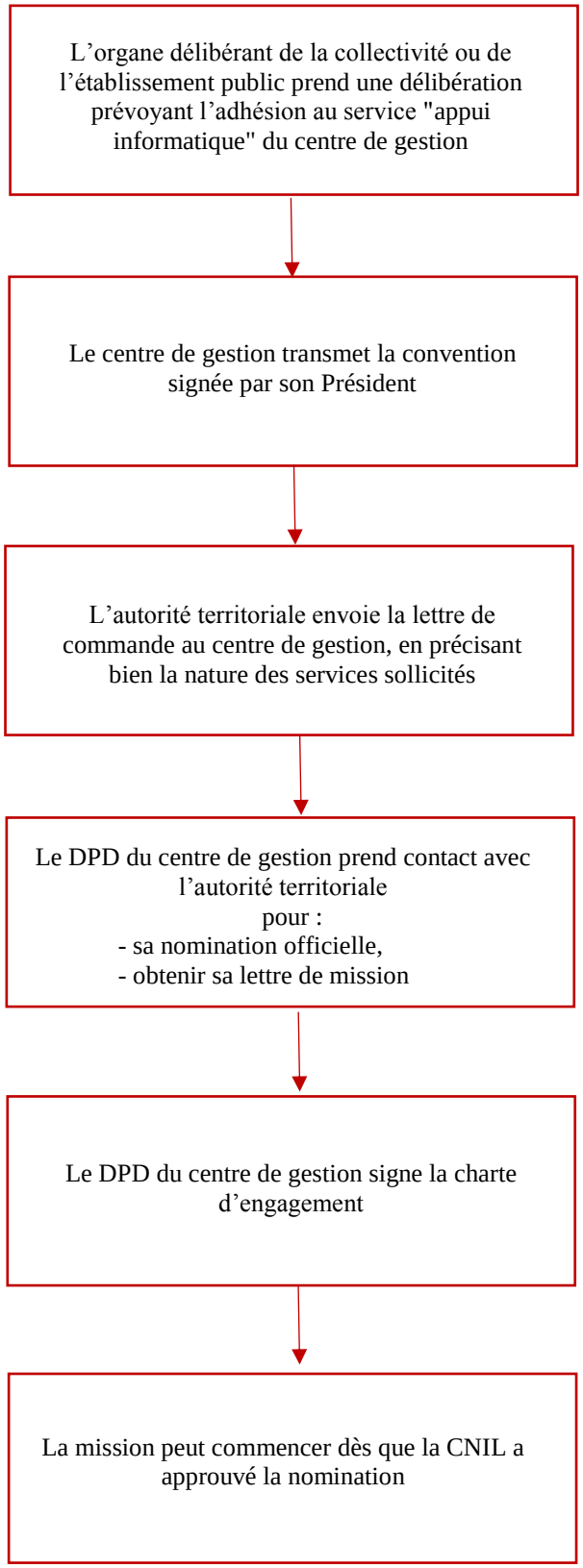
L'objectif principal de l'action d'un DPD est de faire en sorte que le responsable de traitement qui l'a désigné soit en conformité avec le cadre légal relatif aux données à caractère personnel, à savoir :

- informer et sensibiliser sur la culture "Informatique et liberté ",
- présenter la mise en conformité et la sécurisation des traitements de données à caractère personnel, informatisées ou non, sous un angle positif, plutôt que sous celui de la contrainte,
- veiller au respect du cadre légal,
- réaliser un inventaire de l'existant et définir selon les fournisseurs leurs rôles de cotraitants ou de sous-traitants. Il soumet ses avis documentés au responsable de traitement et note les décisions qui en ressortent. Il est obligatoirement consulté avant la mise en œuvre d'un nouveau traitement pour faire des recommandations,
- informer et responsabiliser, alerter si besoin le responsable de traitement,
- informer sans délai le responsable de traitement de tout risque que les initiatives des opérationnels ou le non-respect de ses recommandations feraient courir à l'organisme et à ses dirigeants,
- mener, de façon maîtrisée et indépendante, toute action permettant de juger du degré de conformité de l'organisme, de mettre en évidence les éventuelles non-conformités (gravité, impacts possibles pour les personnes concernées, origine, responsabilité, etc.), de vérifier le respect du cadre légal ou la bonne application de procédures, méthodes ou consignes relatives à la protection des données personnelles,
- établir et maintenir une documentation relative aux traitements de données à caractère personnel, dont le registre des traitements, et assurer son accessibilité à l'autorité de contrôle,
- assurer la médiation avec les personnes concernées par un litige,
- recevoir les réclamations des personnes concernées par les traitements de données à caractère personnel et veiller au respect du droit des personnes,
- traiter ces réclamations et plaintes avec impartialité, ou mettre en œuvre les procédures propres à assurer leur bon traitement,
- rendre compte de son action en présentant chaque année un rapport à son responsable de traitement. Ce dernier est le reflet fidèle de son action au cours de l'année écoulée et fait état des éventuelles difficultés rencontrées,
- interagir avec l'autorité de contrôle,
- être le point de contact privilégié de l'autorité de contrôle (CNIL), avec laquelle il communique en toute indépendance sur les questions relatives aux traitements mis en œuvre par l'organisme qui l'a désigné, y compris la consultation préalable visée à l'article 36 du RGPD, et mener des consultations, le cas échéant, sur tout autre sujet.

IV - LE SERVICE PROPOSE PAR LE CDG

Le centre de gestion met à disposition, dans le cadre de la possibilité de mutualisation prévue par les textes, son délégué à la protection des données.

Pour bénéficier de ce service, il convient de suivre la procédure suivante :



A NOTER :

- Le DPD du centre de gestion fait l'objet d'une nomination par le Président valable uniquement pour l'application du RGPD au sein du centre de gestion ; l'agent doit donc être nommé par chaque autorité territoriale auprès de laquelle il est mis à disposition. Cette désignation est transmise à la CNIL qui valide.

- L'adhésion au service informatique permet de solliciter, à tout moment et par lettre de commande, toute mission relevant du service. Seuls les services effectués sont facturés. Aucune cotisation n'est due au titre de l'adhésion.

- Les documents utiles sont disponibles dans l'intranet de notre site :

  ➢ Les plus du CDG
  ➢ Informatique
  ➢ Documents

- Les collectivités et établissements publics disposant de leur propre délégué à la protection des données peuvent utiliser les modèles de lettre de mission et de charte d'engagement, en les adaptant à leur situation.