Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DU JURA

Lons le Saunier, le 25 JAN. 2018

DIRECTION DE LA CITOYENNETÉ ET DE LA LÉGALITÉ

Bureau des Relations avec les Collectivités Locales et de l'Expertise Juridique

Circulaire n° 3

TRANSMISSION PAR MESSAGERIE

Le Préfet du Jura

à

- Mesdames et Messieurs :
  - les Maires
  - les Présidents des Communautés d'Agglomération
  - les Présidents de Communautés de Communes
  - les Présidents de Syndicats Intercommunaux et de Syndicats Mixtes

(Pour attribution)

- Monsieur le Sous-Préfet de Dole
- Madame la Sous-Préfète de Saint-Claude
- Monsieur le Président de l'Association des Maires des communes du Jura
- Monsieur le Président du Centre de Gestion de la Fonction Publique Territoriale du Jura
- Mesdames et Messieurs les Trésoriers

(Pour information)

OBJET : La protection des données personnelles et la refonte de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Référence : 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Le Parlement européen et le Conseil ont adopté le 27 avril 2016 un « paquet européen de protection des données », dont le **règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD)** du 27 avril 2016, qui sera directement applicable au sein des Etats membres le 25 mai 2018.

Un projet de loi, visant à adapter en conséquence la loi de 1978 sans l'abroger, a été déposé le 13 décembre à l'Assemblée nationale. Son entrée en vigueur est prévue en même temps que le règlement européen, au **25 mai 2018**. Les acteurs publics et notamment les collectivités territoriales sont directement concernés par ces évolutions.

Le nouveau régime de protection de la donnée renverse la logique actuelle de déclaration *a priori* des traitements de données à la Commission nationale de l'informatique et des libertés (CNIL) et instaure un mécanisme de responsabilisation des acteurs assorti de sanctions alourdies : **il appartiendra désormais à l'autorité publique de prendre toutes mesures afin de garantir la conformité des traitements de données personnelles qui relèvent de sa responsabilité**. En cas de manquement de la structure à ses obligations, des sanctions pourront être infligées par la CNIL.

Pour être prêtes au 25 mai 2018 à remplir ces nouvelles obligations, les collectivités devront mettre en place les actions suivantes :

- Désigner un délégué à la protection des données

La nomination d'un correspondant à la protection des données à caractère personnel était facultative : désormais, la nomination d'un délégué à la protection des données (DPD) devient obligatoire pour toute autorité publique effectuant des traitements de données (art. 37 du règlement et art. 8 du projet de loi). Un décret en Conseil d'Etat fixera les conditions d'application de cette obligation.

A noter que le règlement européen prévoit la possibilité pour les organismes publics de désigner un seul DPD pour plusieurs organismes, compte tenu de leur structure organisationnelle et de leur taille : les petites collectivités pourront dès lors se regrouper pour désigner un DPD commun et mutualiser ses fonctions.

Indépendant (art. 38 du règlement) et spécialiste de ces questions, le DPD sera chargé d'informer, de conseiller l'administration et ses agents sur les obligations qui leurs incombent et de contrôler la mise en œuvre de la réglementation au sein de la structure. Il sera l'interlocuteur de la CNIL au sein de son organisation (art. 39 du règlement).

- ***Recenser les traitements de données personnelles***

Le RGPD prévoit, en complément de la nomination d'un DPD, l'obligation de faire l'inventaire des applications susceptibles de contenir des données à caractère personnel et de tenir à cet effet une documentation interne complète (registre listant les traitements concernés, prévu à l'art. 30 du règlement).

- ***Identifier et évaluer les risques en fonction de la nature, de la portée, du contexte et des finalités du traitement***

Une fois les traitements de données recensés par les collectivités, il importera d'identifier ceux susceptibles de générer des risques élevés pour les droits et libertés des personnes concernées. Dans ce cas, une analyse d'impact devra être menée (art. 35 du règlement).

- ***Mettre en œuvre les mesures nécessaires pour atténuer les risques et assurer la sécurité du traitement***

En fonction des évaluations menées et des risques identifiés, les administrations devront assurer la sécurité des traitements en mettant en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque : anonymisation, chiffrement des données à caractère personnel, … (art. 32 du règlement).

Si une collectivité identifie un risque et est d'avis que ce risque ne peut être atténué par des moyens raisonnables compte tenu des techniques disponibles et des coûts de mise en œuvre, elle devra consulter la CNIL avant le début des opérations de traitement (art. 36 du règlement).

- ***Informer la CNIL et la personne concernée en cas de violation de données à caractère personnel***

Si une violation de données à caractère personnel est identifiée et susceptible, selon la collectivité, d'engendrer un risque pour les droits et libertés des personnes physiques, elle devra le notifier à la CNIL ainsi qu'à la personne concernée (art. 33 et 34 du règlement).

Telles sont les informations que je souhaitais porter à votre connaissance.

Le Préfet,
Pour le Préfet et par délégation,
Le Secrétaire Général,

Stéphane CHIPPONI