Question écrite de M. Toussaint relative à l'adoption du RGPD par la commune

Le 25 mai dernier, le RGPD (Règlement général sur la protection des données) est entré en vigueur pour mieux protéger les informations/données privées du traitement qu'en font les entreprises mais aussi le secteur non marchand.

Gérant un grand nombre de données, que ce soit dans le cadre de leur mission de base (état civil, population, enrôlement des taxes,…), de la gestion de leur propre personnel, de l'organisation de services à la population ou encore de la communication vers le citoyen, les communes et les CPAS sont clairement concernés.

Sur base de ce qui précède, je souhaiterais savoir ce qui a été mis en œuvre concrètement par notre commune (non pas de manière exhaustive mais dans les grandes lignes) pour se conformer à ce nouveau règlement ?

Vous remercie par avance pour vos réponses/précisions.

Cordialement.

Réponse:

Les actions suivantes ont été réalisées ou sont en cours de réalisation :

Information au CODIR

Présentation au CODIR des principes du RGPD et de la sécurité de l'information (17/11/2017)

Analyse de conformité RGPD/sécurité de l'information

A partir du 14/12/2017, interview des différents départements pour évaluer la conformité générale au RGPD et la présence de mesures destinées à garantir la sécurité des données à caractère personnel.

Deux rapports ont été réalisés : l'un pour le RGPD (sur base de la règlementation), l'autre pour la sécurité de l'information (sur base des contrôles de la norme ISO/IEC 27001). Un plan de mise en conformité est inclus dans ces rapports.

Les rapports ont étés remis fin mars 2018, présentés et approuvés le 20/04 par le CODIR.

Les premières actions recommandées pour la partie RGPD :

- choix d'un guide, pilote, chef de projet interne pour ce programme
- nomination d'un DPO (Data Protection Officer)
- établissement du registre des traitements
- identification des non-conformités pour les traitements critiques / concernant les citoyens
- mise en place d'un processus de gestion des demandes des personnes
- mise en place d'un processus de traitement des incidents et notification des brèches
- rédaction et publication d'une politique « protection des données / vie privée » générale

Les deux analyses ont été réalisées par le CIRB.

RGPD – pilotage de la mise en conformité

Un groupe (temporairement nommé « Groupe de pilotage pour la protection des données ») a été constitué et se réunit régulièrement depuis le début de l'année. Les points d'actions sont suivis de manière structurée et les réunions sont prévues pour avoir lieu toutes les 2 semaines, en pratique elles ont lieu chaque semaine.

Ce groupe est actuellement informel, une proposition va être faite au CODIR et au collège pour officialiser l'organisation encadrant la protection des données.

RGPD – nomination d'un DPO

Un DPO externe (CIRB/IRISTeam) a été désigné et officialisé auprès de l'autorité de protection des données (anciennement CPVP).

RGPD – registre des activités de traitement

Au minimum un membre de chaque service a reçu une information sur le registre et a été invité à créer les fiches de traitement qui le constituent. Ces fiches sont revues par le DPO.

Une liste de traitements « classiques » pour les administrations communale a été fournie, elle est enrichie en continu en fonction de l'augmentation de la connaissance dans différents AC.

Actions en cours

- Publication sur le site web d'une déclaration « protection des données »
- Mise en place du processus de gestion des demandes d'exercice des droits des personnes concernées (droit d'accès, d'effacement, de limitation du traitement, de correction)
- Mise en place de l'organisation supportant la gestion de la sécurité de l'information et de la protection des données
- Création d'un plan d'action (à 3 ans pour la sécurité de l'information, à 1 an pour la conformité RGPD) adapté à l'AC sur base des propositions contenues dans les rapports initiaux