Retranscription à l'identique de la copie remise par la/le candidat·e

MEILLEURE COPIE

Examen professionnel d'avancement de grade de **TECHNICIEN·NE PRINCIPAL·E DE 1ère CLASSE TERRITORIAL·E**

Session 2019

Spécialité *Ingénierie, informatique et systèmes d'information*

RAPPORT AVEC PROPOSITIONS OPÉRATIONNELLES

Communauté d'Agglomération de Techniagglo
Direction des systèmes d'information

le 11/04/19

Rapport technique
à l'attention du directeur des systèmes d'information

Objet : le règlement général sur la protection des données (RGPD) et sa mise en œuvre dans la collectivité.

Référence : Règlement (UE) n°2016/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des données physiques

Les collectivités territoriales gèrent de plus en plus de données, dont une majeure partie sont confidentielles. C'est pourquoi l'Europe a voté une loi en 2016, permettant de sécuriser la gestion et les accès aux données : le règlement général sur la protection des données (RGPD).

Cependant, ce règlement inquiète de nombreux élus, de par ce qu'elle impose dans sa mise en œuvre.

C'est pourquoi nous verrons, dans une première partie, ce qu'est le RGPD, puis dans une seconde partie, nous élaborerons des propositions opérationnelles afin de mettre en place le RGPD dans la communauté d'agglomération.

I / Le règlement général sur la protection des données (RGPD)

Le R.G.P.D exige de nouvelles obligations de sécurité des données et la nomination d'un délegué (A). Pour le respecter, il convient de mettre en place de nouvelles priorités et de sensibiliser l'humain (B).

A/ Le RGPD et le rôle du DPO.

Le RGPD est issu de la loi europèenne de 2016, pour une application au 25 mai 2018. Il a pour vocation d'homogénéiser et de renforcer la protection des données personnelles lors de leur traitement. Le retard dans sa mise en œuvre est risqué pour la collectivité : risque en terme d'image, risques judiciaires, administratifs, voire disciplinaires. C'est une contrainte pour la collectivité, mais une protection pour le citoyen. En outre, la responsabilité des élus est engagée. De plus, la collectivité ne bénéficie pas d'aides de l'Etat pour sa mise en œuvre. Cela est donc d'autant plus difficile pour les petites collectivités, qui peuvent cependant réfléchir à la mutualisation de leur système d'information.

Le RGPD impose la mise en place d'un délégué à la protection des données (DPD ou DPO) pour Data Protection Officer). Le DPD, qui peut être mutualisé avec d'autres collectivités, a pour rôle d'informer, de conseiller et de contrôler. Il est l'interface entre la collectivité et la CNIL, les agents, voire les habitants. Il établit une cartographie de toutes les données de la collectivité, et etablit le registre, en lien avec tous les services de la collectivité. Il met à jour les documents, notamment les mentions de consentement, les contrats avec les prestataires. Il est complémentaire au RSSI (responsable de la sécurité des systèmes d'information qui lui protège la collectivité. Ils doivent travailler ensemble.

B/ Les enjeux techniques et humains

Le RGPD exige des mesures techniques afin de garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement. Pour celà, la collectivité doit veiller à pouvoir démontrer son respect du principe de responsabilité en rendant transparent les traitement de données et en documentant ses décisions technologiques. Elle doit mettre en place des fonctionnalités de chiffrement et de pseudonymisation, cités par les articles 32 et 34. Elle doit également mettre en place des contrôles d'accès adaptés, par une autorisation et authentification fortes. En outre, en analysant régulièrement les logs des serveurs et applications et en les stockant de façon responsable, elle permettra de fournir la mesure de sa conformité. Enfin, une mise à jour des systèmes à l'aide de correctifs permettra de maintenir le système à jour.

Le second aspect est humain : la collectivité, par le biais de son DPO, doit sensibiliser et informer l'utilisateur manipulant des données. Cela est d'autant plus important dans le cadre du télétravail et de la mobilité des agents, qui se connectent à distance au réseau. Pour cela il convient d'utiliser des points d'accès sécurisés et de créer un réseau dédié aux activités professionnelles. L'email (ou courriel) ètant un vecteur d'attaque très utilisé par les criminels, il est nécessaire que les agents

l'utilisent avec prudence. Enfin, la collectivité intéragit avec l'usager, qui a un droit de regard nouveau vis à vis de ses données.

Le RGPD, qui vise à protéger les données, impose de nouvelles contraintes à la collectivité en terme de sécurisation et de protection de données. Dans cette seconde partie, nous élaborons des propositions opérationnelles visant à mettre en conformité le système d'information de la communauté d'agglomération avec la nouvelle réglementation.

Ⅱ / Propositions opérationnelles visant à mettre en conformité le S.I.

Pour la mise en conformité du SI, la première étape consiste à étudier l'existant et nommer un DPO (A), puis à mettre en œuvre le RGPD.

A/ Etude de l'existant et nomination d'un DPO

Pour mettre en place le RGPD, il convient de créer un comité de pilotage (COPIL), composé d'élus, de directeurs de service, de représentants de prestataires exterieur. Le COPIL aura pour mission d'établir les objectifs, de valider les étapes du projet.

Un DPO (délégué à la protection des données) doit être nommé, conformément au RGPD. Sa première tâche consiste à établir un diagnostic de l'existant, en rencontrant tous les services, sur l'utilisation des données.

Il est nécessaire de prévoir un budget, et de rechercher des subventions (autre que l'Etat, puisqu'il ne subventionne pas la mise en conformité). En outre, l'expérience des autres collectivités de taille similaire peut nous être utile. On peut également prévoir à mutualiser le DPO, avec les collectivités de la communauté d'agglomération, ou avec d'autres agglomérations.

Enfin, il est nécessaire de communiquer avec les agents (journal interne, intranet…) et les usagers via le service communication (journal de l'agglomération, site internet,…)

B/ Mise en œuvre du RGPD

Une fois le diagnostic établi par le DPO, il convient de sensibiliser les usagers manipulant des données. Un quiz sur l'Intranet de l'agglomération peut permettre aux agents de se situer sur leur connaissances en matière de sécurité. Ce quiz doit être suivi de résultats, et mis régulièrement à disposition des agents.

Des formations, en lien avec le service RH peuvent être organisées. Les documents doivent également être mis à jour : réalisation d'une charte informatique, signée par les agents.

Les documents administratifs doivent aussi être modifiés, en y apportant les mentions obligatoires.

Les prestataires, à qui on achète ou loue les applications métiers doivent également modifier ces applications et nous fournir les patchs correctifs, afin notamment de sécuriser les identifiants et mots de passe d'accès à ces applications.

Les postes de travail doivent être sécurisé avec des identifiants et mots de passe unique à chaque utilisateur.

Les serveurs doivent être sécurisé, avec un accès restreint à Internet.

Les sauvegardes doivent être contrôlées et verifiées régulièrement.

Enfin, des réunions régulières sur l'Etat d'avancement du projet permettent de corriger les erreurs rencontrés.

La mise en place du RGPD peut paraitre longue et fastidieuse, mais elle permettra à terme de sécuriser le SI et de réaliser des économies.