CONCOURS EXTERNE D'ATTACHÉ TERRITORIAL

SESSION 2018

ÉPREUVE DE NOTE

Durée : 4 heures – Coefficient : 4

SPÉCIALITÉ : ANALYSTE

INDICATIONS DE CORRECTION

Rappel du sujet :

Attaché territorial, vous êtes chargé(e) du numérique à la direction générale de la communauté d'agglomération d'Admicom (150 000 habitants et délégué(e) à la protection des données. La collectivité est engagée dans une démarche de « ville intelligente » (smart city). Vous êtes chargé(e) de coordonner les actions de la collectivité face aux enjeux de la transition numérique et d'assurer la mise en conformité avec la nouvelle réglementation.
À ce titre, le Directeur général des services (DGS) vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, une note sur la sécurité du système d'information et la protection des données au sein de la collectivité.

1) Présentation du sujet

L'entrée en application du Règlement général pour la protection des données (RGPD) en mai 2018 a rendu obligatoire la désignation d'un délégué à la protection des données (DPO) pour toutes les administrations. Cette nouvelle réglementation tend à responsabiliser les acteurs et oblige les organismes à mettre en place des procédures internes ainsi qu'une gouvernance de la sécurité du système d'information (SI) et de la protection des données à caractère personnel.
Les enjeux liés à l'exploitation de la donnée sont également à l'ordre du jour avec des projets de ville intelligente, de big data, d'intelligence artificielle, d'objets connectés, etc… Ces sujets obligent les collectivités à analyser les risques que peuvent faire porter de tels projets sur les libertés individuelles. Les collectivités doivent également, au regard des dernières attaques informatiques d'envergure internationale (tel que Wannacry), s'emparer des sujets de sécurité numérique.
C'est dans ce contexte que le candidat est amené à analyser les enjeux et modalités d'une organisation interne fondée sur les grands principes édictés par le Règlement tels que le Privacy by design, la conformité ou les études d'impacts.

2) Analyse des éléments du dossier

Le dossier est constitué principalement de deux types de documents : des articles de presse qui synthétisent les nouveaux droits et les nouvelles obligations issues du Règlement général pour la protection des données (RGPD) mais également des documents produits par les autorités de contrôle que sont la Commission Nationale de l'Informatique et des Libertés (CNIL) ou l'Agence Nationale de la Sécurité des systèmes d'information (ANSSI). Ces derniers apportent des éléments concrets d'organisation ou des exemples d'actions à mettre en place. Ces documents sont complétés par des extraits de documents législatifs ou normatifs.
La difficulté réside dans le fait qu'il y a peu de retour d'expérience sur la mise en place d'une telle gouvernance au sein des collectivités car le sujet est nouveau. Le candidat devra rester synthétique et ne pas vouloir faire un catalogue d'actions et bien rester sur les principes généraux. Le dossier ne présente pas de documents techniques.

Document 1

Ce document est un article de la Gazette des communes sur la cyber sécurité dans les collectivités territoriales. Cet article fait le constat que les collectivités n'ont pas encore pris la mesure de ces risques et dresse un panorama des différents cas que pourraient rencontrer une collectivité avec en illustration quelques exemples concrets. Cet article met également en avant les impacts de telles attaques sur les collectivités et les sanctions possibles. Il évoque certaines obligations qui vont peser sur les collectivités dès l'application du RGPD et notamment la notification aux victimes et la traçabilité des actions mises en œuvre pour assurer la sécurité des systèmes d'information (régime d'accountability).

Document 2
Ce document est un extrait de l'étude publiée par la CNIL sur les Smart City. Ce 5ème Cahier IP de la CNIL intitulé « La plateforme d'une ville – Les données personnelles au cœur de la fabrique de la smart city » explore les enjeux politiques et sociaux qui émergent autour de la place croissante des données dans la ville. Ce cahier entend contribuer aux débats et questionnements en cours sur la smart city, à travers un prisme de lecture et un éclairage propres à la CNIL : l'accompagnement de l'innovation couplé à la protection des données et des libertés individuelles en contexte urbain. Il s'adresse notamment aux collectivités territoriales, qui font face à ces nouvelles problématiques.

Document 3
Ce document est une communication de l'ANSSI, structure rattachée au SGDSN, sur les risques numériques. Cette fiche s'adresse notamment aux collectivités territoriales et vise à les aider à appréhender la question de la sécurité numérique à travers quelques exemples et recommandations pratiques.

Document 4
Ce document est un extrait du Règlement européen à la protection des données. Il met en avant les articles relatifs à la sécurité des données à caractère personnel :
Article 32 : sécurité du traitement :
Article 33 : notification des violations à la CNIL
Article 34 : notification aux personnes concernées par la violation
Article 35 : analyse d'impact relative à la protection des données.

Document 5
Extrait du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Document 6
Ce document est un extrait du référentiel général de sécurité 2.0 publié par l'ANSSI. Le chapitre 7 est consacré aux recommandations relatives aux bonnes pratiques en matière de méthodologie, de procédures et d'organisation. Ce document évoque le rôle du RSSI dans l'organisation et propose la mise en œuvre d'une gouvernance de la sécurité du SI. Il dresse également un panorama d'actions concrètes à mettre en place au sein de la collectivité comme des actions de sensibilisation, la problématique du Cloud ou encore la mise en œuvre d'audits.

Document 7
Ce document est issu du site de la CNIL dont une rubrique est consacrée aux impacts du RGPD sur les collectivités. Il synthétise les enjeux de cette réglementation et les nouvelles obligations des collectivités. Ce document décrit également le rôle du DPO dans la mise en œuvre de la démarche de conformité de la collectivité.

Document 8
Ce document est une infographie de la CNIL sur les PIA (Privacy Impact Assessment) permettant d'avoir une vue d'ensemble sur les principes et la méthode des études d'impact sur la vie privée rendue obligatoire par le RGPD dès lors qu'un organisme met en place un traitement considéré comme sensible.

Document 9
Ce document est un article de la Gazette des communes qui explicite deux notions clés du RGPD à savoir le privacy by design et le privacy by default. En effet le responsable doit être capable de démontrer qu'il a pris les mesures techniques et organisationnelles appropriées aux risques (privacy by design). Par ailleurs les moyens mis en œuvre devront assurer que, par défaut, seules les données à caractère personnel nécessaires aux finalités seront traitées (privacy by default). Cet article décrit également deux mesures permettant de mettre en œuvre ces principes : la minimisation des données et la pseudonymisation.

Document 10
Ce document est un article du Journal Globbsecurity qui fait suite à l'édition du Mois Européen de la Cybersécurité en 2017. Il donne des pistes concrètes à mettre en place au sein des organisations pour sensibiliser les salariés aux risques de menaces informatiques en donnant l'exemple de la fausse campagne de phising du Ministère de l'Economie. Cet article précise également la notion de violation de données à caractère personnel dont la notification est une obligation introduite par le RGPD et rappelle les sanctions.

Document 11
Ce document issu de la revue *Smartcitymag* traite des menaces liées au développement des smartcities : les risques sur les données personnelles et le « risque cyber », accru par la présence d'objets connectés.

Document 12
Ce document est une note de la CNIL relative à l'entrée en vigueur de la « nouvelle loi Informatique et libertés » du 20 juin 2018 destinée à mettre en conformité le droit national avec le nouveau cadre juridique européen.

3) Proposition de plan détaillé

Avertissement : *il s'agit d'une proposition de plan. D'autres plans sont possibles, au correcteur d'évaluer dans quelle mesure le plan proposé restitue les principaux axes de questionnement et les articule de manière cohérente.*

En-tête

Rappel du cadrage : le rapport doit adopter la forme suivante et reprendre les informations que le candidat trouve en première page du sujet dans la commande et la liste signalétique des documents au dossier.

Communauté d'agglomération d'Admicom

Le 22 novembre 2018 (date du concours)

NOTE
à l'attention de M. le Directeur général des services

Objet : la sécurité du système d'information et la protection des données au sein de la collectivité

Références : uniquement celles des principaux textes juridiques ou officiels fondant la note
- Règlement (UE) 2016/679 du 27 avril 2016 (RGPD)
- Loi n°2018-493 du 20 avril 2018
- Décret n°2010-112 du 2 février 2010

Introduction

Rappel du cadrage : le rapport doit comporter une introduction d'une vingtaine de lignes, qui s'apparente à celle d'une composition ou dissertation (entrée en matière, reformulation du sujet, présentation de la problématique dans son contexte) et doit impérativement comprendre une annonce de plan.

Eléments pouvant être abordés en introduction :
- Le Règlement général pour la protection des données (RGPD) est entré en application en mai 2018
- Augmentation du nombre et de l'ampleur des cyberattaques dans un contexte de développement des démarches de villes intelligentes qui accroissent la vulnérabilité des collectivités

Plan détaillé

Rappel du cadrage : le développement est organisé en parties et en sous-parties. Le plan est impérativement matérialisé par des titres comportant des numérotations en début des parties et sous-parties.

I. Les enjeux de la transition numérique des collectivités territoriales

A. Des téléservices à la smart city : des opportunités non exemptes de risques

- 1) Une opportunité pour les territoires et les citoyens (Document 1 - Document 7)

Le développement de l'e-administration constitue un levier majeur de la modernisation de l'action publique. De ce fait, les collectivités recourent de plus en plus aux technologies et usages numériques : téléservices, open data, objets connectés, démarche de territoires intelligents (smart city).
Par ailleurs, le digital est aujourd'hui une opportunité pour les collectivités locales de simplifier certains services au public et de gagner en efficience, dans un contexte très contraint financièrement. Cette transformation numérique est devenue un véritable enjeu d'optimisation pour les territoires et d'attractivité pour les entreprises.

Cependant les collectivités brassent de plus en plus de données dont certaines s'avèrent particulièrement sensibles.

- 2) Mais des risques potentiels de sécurité (Document 1- Document 2 – Document 3 – Document 10 – Document 11)

Comme tout organisme qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes de cyber attaques. Leur présence sur internet, notamment au moyen de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Les collectivités peuvent être victime d'attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. Le hameçonnage est également une pratique de plus en plus courante permettant de contaminer une machine en introduisant un virus par le biais d'une pièce jointe et potentiellement de prendre le contrôle du système d'information de l'organisation.
En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent.

- 3) Et des risques d'atteinte à la vie privée (Document 2 –Document 7 – Document 11)

Les nouveaux services et applications proposés par les collectivités traitent de plus en plus de données personnelles et font courir des risques sur la vie privée des personnes. Au-delà des risques liés à la sécurité (utilisation de solution en SAAS, hébergement des données dans le cloud), c'est également des risques croissants d'inférences liés au modèle prédictifs ou la possibilité d'identifier les personnes malgré des garanties d'anonymat.
La multiplication des systèmes interconnectés d'acteurs publics mais aussi privés donne le sentiment d'une perte de contrôle sur les données.
Par ailleurs les citoyens sont de plus en plus soucieux de la manière dont leurs données sont utilisées et nécessite pour les collectivités plus de transparence sur les traitements qui sont mis en œuvre.

B. Quelles garanties pour les citoyens ?

- 1) De la loi Informatique et libertés au RGPD (Document 1 -Document 4 - Document 7 – Document 12)

Les nouveaux services numériques, pour créer de la confiance auprès des administrés doivent donc répondre aux exigences de protection des données dont la sécurité est une des composantes essentielles. La loi informatique et Libertés encadre les traitements de données à caractère personnel depuis 1978 et c'est la CNIL qui veille au respect de cette dernière. La Loi pour une République Numérique votée en 2016 vient renforcer ses compétences.
Le Règlement général pour la protection des données à caractère personnel qui est entré en application en mai 2018 vient modifier ce cadre au niveau européen et renforcer les droits des personnes mais également les obligations des organismes qui traitent des données. Si les grands principes déjà présents dans la loi Informatique et libertés ne changent pas, un véritable changement de culture s'opère. On passe en effet d'une logique de contrôle a priori basé sur des formalités administratives à une logique de responsabilisation des acteurs.
La loi du 20 juin 2018 a modifié la loi Informatique et libertés afin de mettre en conformité le droit national avec le cadre juridique européen.

- 2) La Règlementation du SI - Le RGS (Document 1 – Document 5 – Document -)

Les collectivités sont également soumises depuis 2010 à l'obligation d'homologuer leurs téléservices afin de garantir aux utilisateurs que leurs systèmes d'information sont protégés conformément aux objectifs de sécurité fixés par le Référentiel Général de Sécurité (RGS). C'est le décret n°2010 du 2 février 2010 pris pour l'application des articles 9, 1 et 12 de l'ordonnance n°2005-1516 du 8 décembre 2005 qui fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer. Et ce pour assurer la sécurité des informations échangées et notamment leur confidentialité, leur intégrité ainsi que la disponibilité de ces systèmes. C'est l'ANSSI qui concourt à l'élaboration de ce référentiel. Au-delà de l'analyse de risques et de l'homologation, l'ANSSI recommande l'adoption de bonnes pratiques relatives à la méthodologie, aux procédures et à l'organisation.

- 3) Les impacts et sanctions pour les collectivités (Document 1 – Document 7)

Les collectivités qui ne prendraient pas en compte ces nouvelles menaces et ces nouveaux risques s'exposeraient à des impacts plus ou moins graves. Tout d'abord, sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à plusieurs millions d'euros. La loi prévoit également la possibilité de sanctionner pénalement les responsables de traitements à savoir les maires ou les présidents de conseils régionaux ou départementaux en cas de manquement grave.

Les conséquences peuvent également être dramatiques sur le fonctionnement du service public. Par exemple une commune piratée récemment a perdu un certain nombre de données paralysant pendant plusieurs jours les services de la collectivité.

Par ailleurs, lorsqu'une violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable de traitement a l'obligation de notifier cette violation aux personnes concernées. Le risque d'impact sur l'image de la collectivité et des élus peut être lourd de conséquence pour les équipes en place. C'est là l'un des principaux risques encourus.

II. Quel mode de gouvernance mettre en place dans les collectivités ?

A. Les acteurs

1) Le rôle DPO et le RSSI (Document 7 – Document 3)

Le délégué à la protection des données personnelles (DPO) est la pierre angulaire de la mise en conformité de la collectivité. Il remplace le Correspondant Informatique et Libertés et est devenu obligatoire pour toutes les collectivités territoriales avec un niveau de compétence requis.

Le rôle du RSSI dans la collectivité, complémentaire au rôle du DPO est également essentiel. C'est un spécialiste de la sécurité numérique, qui pourra élaborer une politique de sécurité des systèmes d'information (PSSI) et participer à la chaîne fonctionnelle SSI afin des gérer les moyens et les mesures de sécurité.

2) Instance de gouvernance (Document 6 – Document 7)

La collectivité devra organiser les responsabilités liées à la sécurité des systèmes d'information. Cette organisation doit disposer des moyens matériels nécessaires à la réalisation de ses missions et de la capacité à gérer les risques, les crises ou les incidents qui pourraient en résulter.

Une instance de pilotage de la sécurité des systèmes d'information et de la protection des données est indispensable afin de rechercher une amélioration continue des procédures mises en œuvre.

Les instances décisionnelles de la collectivité doivent être impliquées.

3) Le principe de privacy by design et by default (Document 6 – Document 7- Document 9)

Un des principes clés de cette nouvelle réglementation repose également sur le principe de la protection des données dès la conception (privacy by design) et par défaut (privacy by default). La collectivité doit intégrer le plus en amont possible dans la définition dans les outils utilisés et les paramétrages par défaut, les règles d'or de la protection des données (ex : pseudonymisation, habilitations strictes, mécanisme automatique de purge, etc…).

Il en va de même de la sécurité qui doit être prise en compte dès la phase de définition des objectifs fonctionnels des systèmes d'information, notamment pour limiter les coûts du développement de mesures de sécurité tardives.

B. Les actions prioritaires à engager

1) Sensibiliser (Document 3 – Document 6 – Document 10)

Les agents doivent être sensibilisés voire formés aux bonnes pratiques de l'informatique et devenir acteurs de la sécurité numérique de la collectivité. Cette sensibilisation doit permettre de réduire les risques liés à la méconnaissance des principes de base et des règles élémentaires de bonne utilisation de l'outil informatique.

La sensibilisation peut également passer par des exercices de gestion de crise afin de vérifier les procédures mises en place et les comportements des agents face à des menaces informatiques. La sensibilisation doit être régulière. A cet effet la CNIL et l'ANSSI publient de bonnes pratiques pour l'application des principes de base en matière de sécurité numérique. Cette mission fait également partie des missions du DPO.

2) Anticiper les risques (EIVP) et réaliser des audits (Document 3 - Document 4 – Document 6 – Document 8)

Il est essentiel de savoir quels sont les systèmes d'information les plus cruciaux pour le bon fonctionnement de la collectivité afin de pouvoir traiter les risques susceptibles de les fragiliser.

La collectivité doit réaliser ou faire réaliser des audits réguliers de ses téléservices ou systèmes d'information. La collectivité doit recourir à des prestataires agrées.

Conformément à l'article 35 du RGPD, lorsqu'un type de traitement comporte des données à caractère personnel et qu'il est susceptible d'engendrer un risque élevé pour les droits des personnes, la collectivité doit également réaliser une étude d'impact sur la vie privée (EIVP). Cette étude doit permettre d'apprécier les risques et de déterminer des mesures afin de rendre ces risques acceptables, et ce avant la mise en œuvre du traitement.

3) Documenter sa conformité : accountability (Document 1 – Document 6 – Document 7-Document 9)

La collectivité devra conserver une trace des moyens techniques et organisationnels des mesures qu'elle a mises en œuvre pour assurer la sécurité des données et afin de démontrer à tout instant sa conformité. C'est le principe de l'accountability. Cela nécessite par exemple de tenir un registre des traitements réalisés.

La collectivité devra s'assurer que ses sous-traitants offrent des garanties suffisantes au regard du RGPD. Ainsi elle devra intégrer la sécurité dans les marchés publics et notamment prendre en compte la chaîne de sous-traitance (hébergement, maintenance, etc.) et le partage des responsabilités.

La collectivité devra également avoir recours à des produits et des prestataires labellisés qui attestent la sécurité des services et les compétences des professionnels.

La collectivité devra enfin formaliser des politiques de confidentialité et des procédures internes (droit d'accès, notification de violation, etc.)

Conclusion

Rappel du cadrage : la conclusion est facultative. Elle peut toutefois utilement souligner l'essentiel, sans jamais valoriser des informations oubliées dans le développement.