BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS

ÉPREUVE U.3 :
ANALYSE ÉCONOMIQUE, MANAGÉRIALE ET JURIDIQUE DES SERVICES INFORMATIQUES

Épreuve commune aux deux spécialités

SESSION 2021

Durée : 4 heures
Coefficient : 3

AUCUN MATÉRIEL AUTORISÉ

Dès que le sujet vous est remis, assurez-vous qu'il soit complet.
Le sujet se compose de 11 pages numérotées de 1/11 à 11/11

CONTEXTE

SOCIETE OUEST PROG

La société OUEST PROG, créée en 2001 dans la région nantaise, est spécialisée dans l'hébergement de données.
Son offre destinée initialement à des entreprises industrielles s'étend depuis 2012 à une nouvelle clientèle : les professionnels de santé (médecins, pharmaciens, opticiens lunetiers, kinésithérapeutes…), qui peuvent ainsi se concentrer sur leur métier. La localisation de ses serveurs sur le territoire français constitue un gage de confiance pour ses clients.

Pour s'adresser à cette clientèle, la société OUEST PROG détient un agrément spécifique délivré par le ministère français des Solidarités et de la Santé. Cet agrément arrive bientôt à terme et oblige la société à se conformer à une nouvelle réglementation qui lui impose d'obtenir une certification[1] HDS (Hébergeur de Données de Santé) pour maintenir son offre auprès des professionnels de santé.

Face aux enjeux importants que représente cette certification, un comité de pilotage interne a été constitué. Il réunit notamment le dirigeant, le directeur des systèmes d'information. Le directeur des ressources humaines, le directeur financier et le directeur commercial. Il a en charge le suivi du projet, ainsi que la coordination avec l'organisme de certification : AFNOR Certification[2].

En tant que technicien réseau au sein de la société OUEST PROG, vous intégrez le comité de pilotage et participez aux différentes étapes de mise en œuvre de la certification.

Le comité élabore un diagnostic sur l'impact de la certification pour les différents acteurs concernés **(mission 1),** en vue de définir une nouvelle ligne stratégique pour la société (**mission 2)**.
En parallèle de l'élaboration de ce diagnostic, la société a déclenché la procédure de certification et un audit préalable est réalisé par AFNOR Certification. Ce dernier a mis en évidence la nécessité pour la société OUEST PROG de renforcer la sécurisation des données hébergées **(mission 3)**.

Enfin, la **mission 4** s'appuiera sur votre travail de veille juridique.

À l'aide de vos connaissances, du contexte et des annexes vous traiterez les missions 1 à 4.

Liste des Annexes

Annexe 1 : Données numériques de santé : les hébergeurs en marche vers la certification.
Annexe 2 : La certification HDS (hébergeur de données de santé) et la norme ISO 27001.
Annexe 3 : La procédure de certification HDS.
Annexe 4 : Certification hébergement données de santé : un nouveau modèle pour les infogéreurs.
Annexe 5 : Hébergeur de Données de Santé (HDS), pourquoi tout le monde s'y met ?
Annexe 6 : Entre cloud et installation en propre, l'offre pour l'hébergement de données de santé se diversifie.
Annexe 7 : RSE. « Le bien-être des salariés, une priorité » pour une majorité de décideurs.
Annexe 8 : Intervention du directeur des ressources humaines de la société OUEST PROG lors de la réunion du comité de pilotage.
Annexe 9 : Sanction à l'encontre de la société SERGIC.
Annexe 10 : RGPD – Extrait du guide du sous-traitant publié par la CNIL.
Annexe 11 : Sanctions pour non-respect de la charte informatique.

[1] Certification : procédure destinée à faire valider par un organisme tiers indépendant le respect des normes et règlements en vigueur

[2] AFNOR Certification : organisme qui assure les activités de certification du groupe AFNOR (Association française pour la normalisation)

MISSION 1 : Les conséquences de la certification HDS (Hébergeur des données de santé). (12 points) - (Annexes 1 à 6)

Le cadre réglementaire relatif à l'hébergement des données de santé à caractère personnel a été modifié (décret du 26 février 2018). Une certification HDS (Hébergeur de Données de Santé) devra être obtenue pour permettre à la société OUEST PROG de poursuivre cette activité.
Le comité de pilotage dont vous faites partie analyse les impacts de la certification.

1.1. Présenter les avantages de la certification HDS pour les différents acteurs concernés (la société OUEST PROG, les professionnels de santé et les patients).

1.2. Montrer que la certification HDS constitue une barrière élevée à l'entrée sur le marché de l'hébergement des données de santé.

1.3. Analyser les conséquences de l'évolution du cadre réglementaire sur l'offre d'hébergement des données de santé.

MISSION 2 : Le virage stratégique de la société OUEST PROG (10 points). - (Annexes 7 et 8)

Le diagnostic réalisé par le comité de pilotage a mis en évidence de nouvelles menaces pour la société. Le directeur commercial suggère donc dans un premier temps de renforcer la communication auprès des professionnels de santé, puis dans un second temps d'envisager d'élargir l'offre de services de OUEST PROG en leur proposant un logiciel de téléconsultation médicale.

2.1. Présenter les avantages pour les établissements de santé d'externaliser l'hébergement des données de santé de leurs patients auprès de la société OUEST PROG.

2.2. Identifier la nouvelle stratégie globale envisagée, puis exposer ses avantages et inconvénients pour la société OUEST PROG.

2.3. Montrer que la politique RSE[3] de la société OUEST PROG peut contribuer à la réussite de son évolution stratégique.

MISSION 3 : La sécurisation des données de santé au sein de la société OUEST PROG. (10 points) - (Annexes 9 à 11)

Dans le cadre de la procédure de certification, AFNOR Certification a réalisé un premier audit sur site.
Cet audit a révélé dans un premier temps un manque de clarté dans la rédaction des procédures à suivre en cas de violation des données de santé à caractère personnel hébergées par OUEST PROG.

En cas de violation des données de santé,

3.1. Présenter les obligations qui pèsent :
- d'une part, sur la société OUEST PROG en tant qu'hébergeur,
- d'autre part, sur les professionnels de santé clients.

3.2. Distinguer les sanctions encourues en cas de non-respect de ces obligations.

[3] Responsabilité sociale des entreprises

Dans un second temps, l'équipe d'auditeurs a constaté que la charte informatique de la société OUEST PROG devait renforcer l'encadrement de l'utilisation des outils informatiques personnels des salariés à des fins professionnelles. Une charte plus complète va donc être rédigée.

3.3. Préciser si le non-respect de cette nouvelle charte informatique par les salariés de la société OUEST PROG peut entraîner une sanction disciplinaire.

MISSION 4 : Veille juridique (8 points)

La société OUEST PROG démarche ses clients professionnels de santé pour leur proposer le logiciel de téléconsultation médicale. La clinique LOSTET accepte l'offre, un contrat est souscrit avec la société OUEST PROG pour l'intégration de ce logiciel au sein de son système d'information.

Lors de la phase finale de l'intégration, des problèmes d'interopérabilité surviennent.
La clinique LOSTET refuse alors de verser le solde de la facture adressée par OUEST PROG tant que ces problèmes ne sont pas résolus. De son côté, la société OUEST PROG invoque la remise par la clinique d'un cahier des charges incomplet quant aux applications utilisées au sein de sa structure.
La société OUEST PROG souhaite assigner la clinique LOSTET en justice.

En vous appuyant sur votre travail de veille juridique, vous déterminerez si la société OUEST PROG peut s'exonérer de sa responsabilité liée à cette prestation.

(Thème de veille juridique paru au Bulletin officiel de l'enseignement supérieur et de la recherche et au Bulletin officiel de l'éducation nationale le 11 janvier 2018 « Les contrats de production et de fournitures de services informatiques »).

ANNEXES

Annexe 1 : Données numériques de santé : les hébergeurs en marche vers la certification.

Sous-effectif, sous-investissement, qualité des soins, crise des urgences, process lourds et peu dématérialisés… Il faut sauver le système de santé français ! C'est l'objet du « *plan de transformation de l'offre de soins* » que le Premier ministre Édouard Philippe et sa ministre des Solidarités et de la Santé, Agnès Buzyn ont présenté mardi 13 février 2018. Ce plan comporte un volet numérique qui fait écho à l'entrée en vigueur, le 1er avril 2018, d'une nouvelle disposition pour les professionnels hébergeant des données de santé à caractère personnel sur support numérique pour le compte d'un tiers (hors archivage électronique) : l'obligation pour eux de se faire certifier en recourant à un organisme accrédité pour cela. Intégrée au code de la santé publique, cette mesure découle d'une ordonnance du 12 janvier 2017 et met un terme à l'actuelle procédure d'agrément. La date du 1er avril 2018 n'est pas une date-couperet : cette évolution sera progressive, selon l'année d'obtention de l'agrément pour les hébergeurs qui en détiennent déjà un, ou qui en ont fait la demande mais l'attendent encore. […]

Avant même la publication du décret n° 2018-137 en février 2018 officialisant la certification HDS, chez AFNOR Certification, on n'a pas attendu pour se mettre en ordre de marche et bâtir une certification qui débouchera, chez l'hébergeur qui remplira tous les critères, sur l'octroi d'un signe distinctif qui vaudra conformité au décret. « *Les professionnels et établissements de santé souhaitant confier à un tiers les données qu'ils recueillent à l'occasion de leurs activités de prévention, diagnostic, soins ou suivi social et médico-social, ont tout à gagner à faire appel à des tiers certifiés. C'est un gage de confiance pour eux et pour leurs patients* », explique Brice Gilbert, chef de produit chez AFNOR Certification. […]

Source : lemagcertification.afnor.org – 14 février 2018

Annexe 2 : La certification HDS (hébergeur de données de santé) et la norme ISO 27001.

Les données personnelles de santé sont des données sensibles. Leur accès est juridiquement encadré pour protéger les droits des personnes. L'hébergement de ces données doit en conséquence être réalisé dans des conditions de sécurité adaptées à leur criticité.
La réglementation définit les modalités et les conditions attendues.

Depuis le 1er avril 2018, la certification Hébergeur de Données de Santé (HDS) est obligatoire pour toute organisation publique ou privée qui héberge des données de santé. Elle vient remplacer la demande d'obtention d'agrément effectuée auprès du ministère français de la santé. Un certificat, valable 3 ans et renouvelable indéfiniment, est ainsi délivré à l'organisation qui en fait la demande, dès lors qu'au travers des audits effectués sur site, il est attesté le bon respect de normes notamment la norme ISO 27001.

La norme ISO/CEI 27001 est une norme internationale (créée en 2005 et révisée en 2013) qui porte sur le système de management de la sécurité des informations. Elle définit l'ensemble des règles et bonnes pratiques à respecter pour maximiser la sécurité des systèmes d'information (identifier et maîtriser les risques liés au système d'information, mettre en place les mesures de protection appropriées afin d'assurer la confidentialité, la disponibilité et l'intégrité de l'information…). Les certificats de conformité ISO 27001 sont reconnus au niveau international.

Source : les auteurs

Annexe 3 : La procédure de certification HDS.

La procédure de certification repose sur une évaluation de conformité au référentiel de certification. L'hébergeur choisit un organisme certificateur qui devra être accrédité par le COFRAC[4] (ou équivalent au niveau européen).
L'organisme procède à un audit en deux étapes pour évaluer la conformité de l'hébergeur aux exigences du référentiel de certification. Il vérifie notamment l'équivalence des éventuelles certifications ISO 27001 ou ISO 20000 déjà obtenues par l'hébergeur.

- Étape 1 : audit documentaire. L'organisme certificateur réalise une revue documentaire du système d'information du candidat afin de déterminer la conformité documentaire du système par rapport aux exigences du référentiel de certification.
- Étape 2 : audit sur site. Les preuves d'audit sont recueillies dans les conditions définies dans le référentiel d'accréditation.

L'hébergeur dispose de trois mois après la fin de l'audit sur site pour corriger les éventuelles non-conformités et faire auditer ses corrections. Passé ce délai et sans action de l'hébergeur, toute la procédure d'audit sur site sera de nouveau réalisée.

Source : esante.gouv.fr

Annexe 4 : Certification hébergement données de santé : un nouveau modèle pour les infogéreurs.

En 2018, le processus d'agrément des hébergeurs de données de santé va évoluer vers une certification basée sur les normes ISO. Ce passage d'un agrément basé sur un dossier déclaratif, à une certification basée sur un audit sur site, va bouleverser la manière de travailler d'un certain nombre d'hébergeurs agréés de données de santé. Une partie d'entre eux vont voir leur métier modifier au-delà de ce changement de procédure.

Une certification et un audit pour répondre aux limites de l'agrément

Le modèle actuel d'agrément est en fin de vie. Pour encore quelques mois, sur les bases d'une déclaration, l'hébergeur candidat exprime toute sa bonne foi dans un énorme dossier remis à l'ASIP Santé[5]. Le candidat ne fait l'objet d'aucun audit de la part des autorités.
L'exercice consiste donc à être cohérent et crédible face aux règles énoncées par le Ministère de la santé. Et pour certains, parfois ne pas réaliser complétement ce qui a été écrit… Nous comprenons très vite les limites d'un tel système, notamment en termes de sécurité numérique.

[4] COFRAC : Comité français d'accréditation chargé de délivrer les autorisations aux organismes intervenant dans l'évaluation de la conformité en France

[5] ASIP Santé : Agence des Systèmes d'Information Partagé en santé créée en 2009 (remplacée en 2019 par l'ANS Agence du Numérique en Santé) chargée d'accompagner la transformation numérique du système de santé français (réguler l'e-santé en fixant un cadre et des bonnes pratiques, notamment en termes de sécurité et d'interopérabilité, accompagner le déploiement des outils et projets numériques en santé).

Le modèle de certification désormais proposé par la DSSIS (Délégation à la Stratégie des Systèmes d'Information de Santé) et l'ASIP Santé cherche à accroître la confiance envers les hébergeurs, en instaurant un audit sur site réalisé par un tiers indépendant. Et ceci aux frais de l'hébergeur.
De ce fait, le ticket d'entrée de la certification sera bien plus élevé que ne l'était celui de l'agrément, avec pour conséquence une redistribution des cartes chez les actuels hébergeurs déjà agréés. […]

Source : claranet.fr - 30/01/2018

Annexe 5 : Hébergeur de Données de Santé (HDS), pourquoi tout le monde s'y met ?

C'est une totale effervescence. Pas une semaine sans qu'un hébergeur, un acteur du cloud public, n'annonce en fanfare son certificat « Hébergeur de Données de Santé ».

Le gain pour ces acteurs ? La possibilité désormais de stocker et de gérer des données à caractère personnel relatives à la santé d'une personne physique. De quoi garantir en principe un strict respect de la vie privée et le secret médical pour les patients, et les hôpitaux qui souhaitent passer par un prestataire pour le stockage et le traitement des données.

« Cet agrément va permettre à tout l'écosystème médical, notamment les professionnels de la santé, les assureurs, les mutuelles et les start-up de biotechnologie, de bénéficier d'une réelle alternative technique et économique, en reposant sur nos infrastructures avec un très haut niveau de sécurité » assure Arnaud de Bermingham, le dirigeant de Scaleway, un des derniers acteurs à se féliciter de l'obtention de la fameuse certification.

Quelques semaines plus tôt, c'est Microsoft France qui mentionnait les bénéfices de l'obtention de cette certification : "La certification accordée à Microsoft s'applique à l'ensemble de ses services cloud proposés depuis la France. "Nous avons la possibilité désormais de nous reposer sur des certifications qui existaient déjà" confirme Bernard Ourghanlian, directeur technique et sécurité de Microsoft France. Cette certification garantit que l'hébergeur est conforme à des normes telles que ISO 27001, ISO 500001.

En clair, côté métier, le personnel médical pourra utiliser les outils bureautiques et de production en mode SaaS de Microsoft, alors que jusqu'à présent seules les données administratives des patients, et non les données de santé, pouvaient transiter par les serveurs de Microsoft. De quoi ouvrir la voie aussi à l'éditeur pour pousser ses services sur Azure de santé prédictive, de télémédecine, ou encore de suivi thérapeutique.

Vers une refonte des infrastructures IT de santé.
"Cela assure la mise en place d'une gamme d'outils qui permet de faire évoluer et de sécuriser leur pratique. Avant, il faut reconnaître que les praticiens prenaient souvent des outils grand public trouvés à droite et à gauche" explique Philippe Leca, directeur ressources numériques et SI au groupement hospitalier Lille Flandres métropole. Avec la certification HDS, "cela va changer" dit-il.
"Cela permet de l'interopérabilité entre les différents écosystèmes (certifiés) pour travailler entre différents établissements" remarque de son côté Guillaume Deraedt, DPO du centre hospitalier de Lille, qui dit avoir "fait en sorte de travailler sur un socle interopérable pour les données de santé".

Changement réglementaire.
Reste le fond de l'affaire. Pourquoi les Azure, OVH ou autres Amazon se précipitent désormais sur le HDS ? "L'engouement pour la certification HDS vient du fait qu'elle repose sur des couches ISO internationales. Et il faut être attentif sur le fait que l'hébergeur soit certifié sur toutes les couches" explique Guillaume Deraedt.

Avant la mise en place de la certification HDS existait en France (et uniquement en France) depuis 2006 un agrément. "L'agrément exigeait des conditions qui relevaient à mon sens d'une forme de

protectionnisme" poursuit-il. "Cette certification remplace l'agrément aujourd'hui délivré par le ministère de la Santé" mentionne le ministère à ce sujet.

Pas étonnant donc que les acteurs du cloud aient poussé en faveur d'un changement réglementaire. Car avec le respect des normes ISO comme socle à la certification, il leur est désormais beaucoup plus simple d'obtenir le droit d'héberger des données de santé.
Car attaquer le secteur de la santé est à présent une nécessité commerciale pour les géants du cloud qui s'ébattent sur le marché français. […]

En effet, le passage de l'agrément à la certification HDS a mis plus d'une institution hospitalière française en difficulté. Depuis 2018, le statut d'hébergeur de données de santé n'est plus encadré par le seul agrément HDS – qui imposait de répondre à un cahier des charges, sans tiers certificateur – mais bien à une certification, incroyablement plus compliquée à obtenir. Si les hôpitaux avaient pu obtenir leur agrément pour assurer eux-mêmes l'hébergement des données médicales, le passage à la certification, qui repose sur la norme ISO 27001, demeure une épreuve de force. Ils seront donc nombreux à recourir à des prestataires certifiés HDS.

Source : d'après zdnet.fr- 6/02/2019

Annexe 6 : Entre cloud et installation en propre, l'offre pour l'hébergement de données de santé se diversifie.

En élevant fortement le niveau d'exigence, le passage de l'agrément au certificat HDS rebat les cartes du marché de l'hébergement de données de santé. Aux côtés des traditionnels infogéreurs, les géants du cloud public montrent leurs muscles. […] Il ne se passe pas une semaine sans qu'un acteur annonce avoir obtenu le certificat d'hébergeur de données de santé (HDS). Quinze mois après la publication au journal officiel du décret qui entérine le passage de l'agrément au certificat, une vingtaine de prestataires ont déjà décroché le précieux sésame [51 hébergeurs certifiés HDS début octobre 2019 et 97 en novembre 2020]. On retrouve principalement les acteurs traditionnels de l'infogérance (Claranet, Tessi, Cheops) face – c'est la grande nouveauté – à des fournisseurs de cloud français (OVH, Orange) ou américains (Amazon Web services, Microsoft Azure).

La centaine de prestataires agréés HDS ne sont toutefois pas hors course. Leur agrément reste valide jusqu'à son échéance, soit trois ans maximum. […] Pour autant, la marche à franchir risque d'être haute pour un certain nombre de "petits" prestataires. […]

Source : mindhealth.fr – 18 juin 2019

Annexe 7 : RSE. « Le bien-être des salariés, une priorité » pour une majorité de décideurs.

La responsabilité sociétale des entreprises (RSE), « une activité bénéfique pour l'activité, » qui doit être prise en compte « pour le bien-être des salariés et par les salariés ».
La prise en compte de la RSE dans les entreprises évolue.
Ainsi, les chefs d'entreprises et cadres mettent en avant une dimension « sociale » de la RSE. « La prise en compte du bien-être des salariés dans l'entreprise arrive ainsi en tête des citations (51%) parmi les enjeux prioritaires de la RSE ». Ce volet de la RSE est suivi de l'éthique dans les affaires, la transparence et la lutte contre la corruption (44 %), la prise en compte de l'empreinte écologique de l'entreprise (37 %) mais aussi celle de la santé des salariés (37 % également). […] La RSE, une problématique « par et pour les salariés, même s'ils ne sont ni les seuls acteurs, ni les seuls bénéficiaires de cette action dans l'entreprise », explique l'étude.
Enfin la RSE n'est pas vue comme une contrainte par une majorité de décideurs (55 %) [ni un frein au changement], mais comme « une opportunité économique », et « une source d'avantage concurrentiel ». […]

Enfin, au vu de l'impact important que la RSE engage pour l'entreprise, une majorité de décideurs souhaite « aller plus loin dans l'intégration complète de la RSE à la stratégie et aux opérations commerciales », et 54 % d'entre eux émettent la volonté d'aller plus loin que les obligations réglementaires.

Source : ouest-france.fr – 12 février 2018

Annexe 8 : Intervention du directeur des ressources humaines de la société OUEST PROG lors de la réunion du comité de pilotage.

Depuis sa création en 2001, notre société a acquis un véritable savoir-faire dans le domaine de l'hébergement de données. Nos clients nous font confiance. Nous leur assurons la disponibilité, la sauvegarde et une haute sécurisation de leurs données dans nos deux centres d'hébergement de données localisés en France. La société connaît une croissance régulière bien supérieure à la moyenne du secteur (croissance annuelle du chiffre d'affaires de 8%), notre politique RSE est certainement à l'origine de ces performances.

Nous nous attachons en effet à fournir des conditions de travail optimales, de réelles perspectives d'évolution et de formation (1 salarié sur 2 a bénéficié d'une formation l'année dernière). Nous fidélisons ainsi tout naturellement nos collaborateurs (1% seulement de turn-over).
La politique salariale menée au sein de la société se veut être équitable et attractive par une distribution de primes en fonction des résultats de l'entreprise. De plus 80% des salariés sont actionnaires de l'entreprise.

En tant que directeur des ressources humaines, je crois dans le talent de chacun des collaborateurs qui travaille au sein de OUEST PROG : 95% des embauches sont en CDI, et j'attache une grande importance à reconnaître la valeur de chaque collaborateur tant d'un point de vue de ses compétences professionnelles que de ses qualités humaines. Notre culture d'entreprise, basée sur la transparence et la confiance, véhicule des valeurs primordiales qui permettent de fédérer et maintenir la cohésion, et ce, afin d'assurer la réussite de l'entreprise. Cette réussite ne peut se faire sans l'engagement réel de tous, surtout lorsque l'on sait qu'un salarié impliqué a des performances 50% supérieures à celles d'un autre.
Chaque cadre de la société fait en sorte que les salariés sachent qu'ils sont partie prenante dans la réussite des projets de l'entreprise. C'est pourquoi il nous faudra bien faire comprendre ce nouveau virage stratégique et faire en sorte que chaque salarié puisse identifier précisément son rôle dans la réalisation de celui-ci.

Enfin, cette réussite reposera sur le capital humain de la société. L'addition de toutes les connaissances techniques, les expériences acquises, les savoir-faire relationnels avec la clientèle, de tous les salariés de OUEST PROG transmis de génération en génération, constitue ce capital humain essentiel à la réussite actuelle et future de notre entreprise.
C'est ce qui fera, je n'en doute pas, la différence avec nos concurrents.

Source : Les auteurs

Annexe 9 : Sanction à l'encontre de la société SERGIC.

La société SERGIC est spécialisée dans la promotion immobilière, l'achat, la vente, la location et la gestion immobilière. Pour les besoins de son activité, elle édite le site web www.sergic.com. Ce dernier permet notamment aux candidats à la location de télécharger les pièces justificatives nécessaires à la constitution de leur dossier.

En août 2018, la CNIL a reçu une plainte d'un utilisateur du site indiquant avoir pu accéder, depuis son espace personnel sur le site, à des documents enregistrés par d'autres utilisateurs en modifiant légèrement l'URL affichée dans le navigateur. Un contrôle en ligne réalisé le 7 septembre 2018 a permis de constater que des documents transmis par les candidats à la location étaient librement accessibles, sans authentification préalable. Parmi ces documents, figuraient des copies de cartes

d'identité, de cartes Vitale, d'avis d'imposition, d'attestations délivrées par la caisse d'allocations familiales, de jugements de divorce, de relevés de compte ou encore d'identité bancaire.

Le jour même de son contrôle, la CNIL a alerté la société de l'existence de ce défaut de sécurité et de la violation de données personnelles consécutive. Quelques jours plus tard, un contrôle sur place a été réalisé dans les locaux de la société. À cette occasion, il est apparu que la société avait connaissance de la vulnérabilité depuis le mois de mars 2018 et que, si elle avait entamé des développements informatiques pour les corriger, ce n'est que le 17 septembre 2018 que la correction totale est devenue effective.

Sur la base des investigations menées, la formation restreinte – organe de la CNIL chargé de prononcer les sanctions - a constaté des manquements au règlement général sur la protection des données (RGPD).

Tout d'abord, la formation restreinte de la CNIL a considéré que la société SERGIC a manqué à son obligation de préserver la sécurité des données personnelles des utilisateurs de son site, prévue par l'article 32 du RGPD. La société n'avait pas mis en place de procédure d'authentification des utilisateurs du site permettant de s'assurer que les personnes accédant aux documents étaient bien celles à l'origine de leur téléchargement, alors qu'il s'agissait d'une mesure élémentaire à prévoir. Ce manquement était aggravé d'une part, par la nature des données rendues accessibles, et d'autre part, par le manque particulier de diligence de la société dans sa correction : la vulnérabilité n'a été définitivement corrigée qu'au bout de 6 mois et aucune mesure d'urgence visant à limiter l'impact de la vulnérabilité n'a été prise dans l'attente.

Ensuite, la formation restreinte a constaté que la société conservait sans limitation de durée en base active l'ensemble des documents transmis par les candidats n'ayant pas accédé à location au-delà de la durée nécessaire à l'attribution de logements. […]

La formation restreinte a prononcé une amende de 400 000 euros, et décidé de rendre publique sa sanction. La formation restreinte a notamment tenu compte de la gravité du manquement, du manque de diligence[6] de la société dans la correction de la vulnérabilité et du fait que les documents accessibles révélaient des aspects très intimes de la vie des personnes.

Source : CNIL - 06 juin 2019

Annexe 10 : RGPD – Extrait du guide du sous-traitant publié par la CNIL.

Applicable à partir du 25 mai 2018 à l'ensemble de l'Union européenne, le règlement européen sur la protection des données renforce les droits des résidents européens sur leurs données et responsabilise l'ensemble des acteurs traitant des données (responsables de traitement et sous-traitants) qu'ils soient ou non établis au sein de l'Union européenne. Ce guide a pour objectif d'accompagner les sous-traitants, dans la mise en œuvre de ces nouvelles obligations.

[…]

Quel est votre rôle en tant que sous-traitant en cas de violation de données ?

Une violation de données est une faille de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à ces données.

En tant que sous-traitant, vous devez notifier à votre client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Sur la base de cette notification, votre client, en tant que responsable de traitement, devra quant à lui notifier cette violation de données à l'autorité de contrôle compétente [la CNIL] dans les conditions de l'article 33 du règlement européen [dans les meilleurs délais et si possible dans un délai de 72 heures] et communiquer à la personne concernée une telle violation dans les conditions de l'article 34 du règlement européen.

[6] Diligence : Rapidité dans l'exécution d'une chose

Sous réserve de l'accord de votre client et à condition que cela soit prévu explicitement par le contrat vous liant avec votre client, il est possible pour ce dernier de vous donner instruction d'effectuer pour son compte cette notification à l'autorité et, le cas échéant aux personnes concernées.
[…]
Quels sont les risques en cas de non-respect de vos obligations en tant que sous-traitant ?
Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement européen peut obtenir la réparation intégrale de son préjudice de la part du responsable de traitement ou du sous-traitant.
Vous pouvez donc être tenu pour responsable du dommage causé et faire l'objet de sanctions administratives importantes pouvant s'élever, selon la catégorie de l'infraction, jusqu'à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, jusqu'à 2% ou 4% du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu.

Source : CNIL – septembre 2017

Annexe 11 : Sanctions pour non-respect de la charte informatique.

Votre employeur peut vous infliger une sanction disciplinaire en cas de non-respect de la charte informatique de l'entreprise. Les sanctions applicables en cas de non-respect de la charte informatique sont ainsi indiquées dans la charte elle-même. Il peut s'agir d'un blâme, d'un avertissement, d'une mise à pied ou même d'un licenciement pour faute grave. Si, selon l'employeur, la présence au sein de l'entreprise du salarié fautif représente un danger, celui-ci peut être licencié sans préavis. Pour éviter les abus, la loi fixe un certain nombre de sanctions interdites en cas de violation de la charte informatique notamment les amendes ou encore les sanctions discriminatoires.

Pour qu'elle soit opposable aux salariés de l'entreprise, la charte informatique doit respecter certaines règles.

L'employeur peut annexer la charte informatique au contrat de travail mais le plus souvent elle figure en annexe du règlement intérieur de l'entreprise.

Dans ce dernier cas, certaines formalités doivent être respectées aussi bien lors de l'instauration de la charte qu'en cas de modification ultérieure des clauses qu'elle comporte : elle doit être soumise à l'avis des représentants du personnel, être déposée au greffe du conseil de prud'hommes et être transmise à l'inspection du travail. Enfin, les salariés doivent en prendre connaissance par voie d'affichage dans l'entreprise ou par la remise d'un exemplaire à chaque salarié.

Si l'ensemble de cette procédure n'est pas respecté, la charte informatique n'a pas de valeur contraignante pour les salariés.

Source : d'après journaldunet.fr – 15 juillet 2019