Webinaire - Questionnaire MNM de la BCSS

2021-09-06

Agenda

- Présentation
- Désignation et Déclaration du DPO
- Questionnaire – Taux de réponses

1e partie

- Questionnaire – Pratique
- Questions / Réponses : Disclaimer
- Questions / Réponses

2e partie

Désignation DPO
Base Légale

- Loi du 15 janvier 1990 – art 4 § 5

§ 5. Toute autorité publique, personne physique et organisme public ou privé qui a accès aux données d'identification des registres Banque-Carrefour ou en obtient la communication, conformément au § 4, ***désigne, parmi ses membres du personnel ou non, [un délégué à la protection des données, ...***

Déclaration DPO
Base Légale

- Loi du 15 janvier 1990 – art 24

Toute institution de sécurité sociale désigne, au sein de son personnel ou non,un délégué à la protection des données et ***communique son identité à la Banque-carrefour***.

- AR 12 août 1993 – art 4

Après leur désignation, l'identité du délégué à la protection des données et de ses adjoints éventuels dans les institutions qui appartiennent à un réseau secondaire ***est communiquée à l'institution gérant le réseau secondaire concerné.***

Déclaration DPO

1. Déclaration à la BCSS
   - Formulaire à security@ksz-bcss.fgov.be

2. Déclaration au SPP IS
   - dpo@mi-is.be

3. Déclaration à l'APD

Désignation et Déclaration DPO

"Comment d'autres institutions (même structure/taille CPAS) s'en sortent avec les enjeux de la sécurité"

- Le partage d'un DPO entre plusieurs CPAS
- Faire appel à une société externe (outsourcing)

Déclaration DPO

Déclaration à la BCSS est obligatoire

- **± 60** CPAS: pas de DPO déclaré/connu (WL + BXL)

→ Violation de la loi

→ Manque de communication

→ Gestionnaire local: condition en concertation avec SPP IS

- Formation DPO BCSS
  - Site-web BCSS
  - Infos pratique: joelle.ankaer@smals.be
  - Infos contenu: security@ksz-bcss.fgov.be

Questionnaire – Taux de Réponses

- **282 (-60) = 222** de CPAS interrogés
- **± 50 %** de réponses (WL + BXL)

- Non-compliant?

→ Flux de données peuvent être arrêtés

→→ Affecte le citoyen directement

→ En cas d'investigation de l'APD

→→ Complications

Questionnaire – Taux de Réponses

"Peut-on avoir un retour sur les réponses données?"

- Majorité de "oui" dans les réponses : vous savez que vous êtes sur la bonne voie

- SPP IS
  - est l'institution de gestion
  - contrôle la sécurité
  - a accès aux listes/réponses

Questionnaire – Pratique

- Invitation en début d'année par mail: via SPP IS ou BCSS
- Deadline : 2 mois après réception du questionnaire
- Base légale: AR 12 août 1993 – art 14

Le groupe de travail sur la sécurité de l'information est plus particulièrement chargé de :

1° la préparation des normes minimales concernant la sécurité physique et logique de l'information;

*2° la préparation d'**une liste de contrôle permettant l'évaluation du respect des normes minimales** concernant la sécurité physique et logique de l'information;*

Questionnaire – Pratique

- **Est-il prévu que le SPP IS fournisse un document explicatif pour mieux comprendre les questions du questionnaire ?**

demander au SPP IS

- **Un questionnaire simplifié du SPP IS sera encore à l'ordre du jour pour 2021-2022 ?**

SPP IS peut simplifier, mais questionnaire MNM reste inchangé

- **Est-il toujours prévu qu'un membre de notre réseau secondaire assiste au groupe policy pour donner son avis sur la proposition de questionnaire à remplir pour l'année 2022 ?**

SPP IS invite 1 ou 2 membres du réseau secondaire à chaque réunion trimestrielle

Feedback 1e Partie ?

Questions / Réponses : Disclaimer

- Interprétation et compréhension du questionnaire "MNM"
- Nous ne pouvons répondre à votre place pour des cas particuliers ; responsabilité et travail de chaque responsable de traitement avec le support de leur DPO
- 1 slide par Question ==> slide(s) réponse ==> feedback éventuel entre chaque sujet

Question 1

- 5.3.1.2a : *Existe-t-il un service chargé de la sécurité de l'information placé sous l'autorité fonctionnelle directe du responsable de la gestion journalière de l'organisation ?*

- **si le CPAS n'a pas de service formel chargé de la sécurité mais a un DPO qui organise régulièrement des réunions de suivi avec la direction générale et les chefs de service, est-ce suffisant pour répondre « oui » ?**

Réponse 1

- Oui, si le DPO est bien en charge de la sécurité
- En pratique il faut s'assurer que le suivi soit fait et que les normes soient respectées
- La structure, la gouvernance et l'implémentation varient en fonction de chaque organisation ; un « service de sécurité » peut tout à fait être assuré par 1 seule personne, si cette configuration est adaptée au contexte.

Question 2

- Questions 56 à 87, majoritairement BLD APPDEV
- Si on indique au niveau du contexte qu'il n'y a pas de développement interne des systèmes d'information ICT (applications) certaines réponses se mettent en N/A, mais pas toutes
- **Ces questions concernent-elles réellement les CPAS qui ne font pas de développement interne ?**

Réponse 2

- Oui, il faut répondre à toutes les questions
  - Attention, "N/A" est une réponse en soi ! :-) L'institution indique via "N/A" que la question ne s'applique pas dans son contexte ; l'auto-switch est un aide / une suggestion

- Le responsable du traitement reste l'ultime responsable

- Généralement contraintes via contrats pour le développement

- Par exemple Question 70 : "*Les accès font-ils l'objet d'un logging ?*" doit faire partie des requirements d'un software outsourcé

Question 3

- 5.5.4b : L'organisation exerce-t-elle en permanence un contrôle sur l'e-mail, la communication en ligne et l'utilisation d'internet dans le cadre des objectifs suivants : (……)

- **On parle bien d'un « contrôle permanent » ? Pourriez-vous préciser cette notion ? Est-ce bien légal ?**

Réponse 3

- On parle de contrôles dans le sens ISO27k et mitigation de risques
- Ceci pourrait être l'application de la *SSL Inspection*
- Les contrôles ne sont pas toujours techniques
  - Accords avec les collaborateurs
  - Informations aux end-users
  - Acceptable use policy
  - Règlement de travail

Question 4

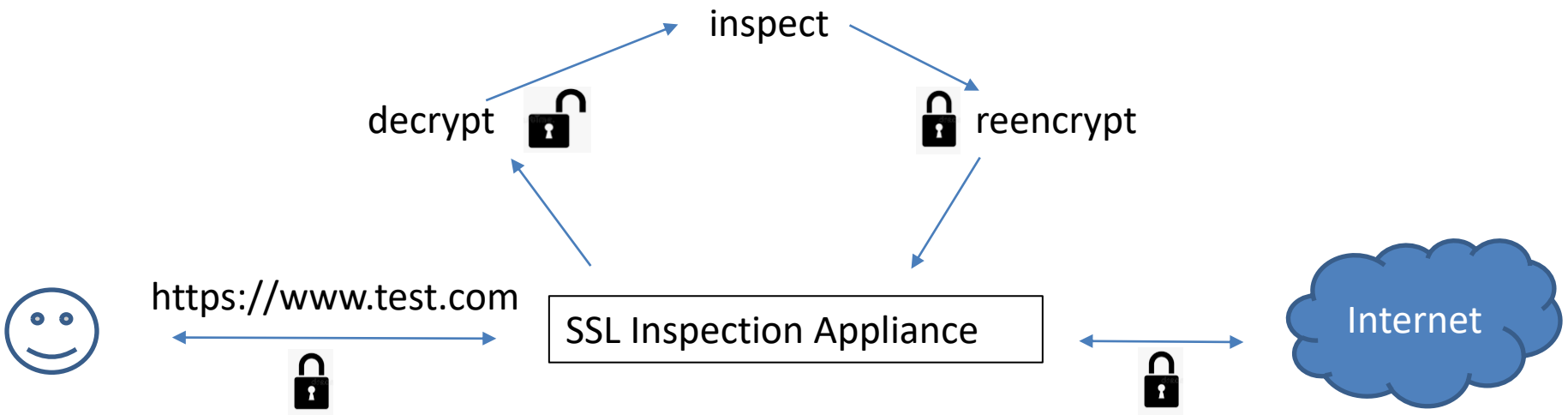
- 5.7.1e : Les données chiffrées de tiers qui entrent dans le réseau de l'organisation sont-elles d'abord déchiffrées et scannées pour détecter la présence de virus et autres malware ?

- **Et en pratique ? Pourriez-vous donner un exemple de solution technique ?**

Réponse 4

- C'est le principe classique de "*SSL Inspection*" (en + de AV sur PC)
- Les connexions passent par une quelconque appliance / proxy de type "web gateway" qui
  - Décrypte
  - Scan le contenu pour détecter des signatures malicieuses
  - Réencrypte
    - Le certificat de l'appliance est trusté au niveau des browsers des workstations
    - Attention niveau transparence / agreements avec les utilisateurs finaux !
- De nombreuses appliances fournissent ce type de service ; Smals fournit ce service à plusieurs institutions via BlueCoat
- Ne pas le faire n'est pas une non-compliance envers les MNM

Réponse 4 (2)


inspect
decrypt
reencrypt
https://www.test.com
SSL Inspection Appliance
Internet

Question 5

- 5.12.1f : Les adaptations de la prestation de service sont-elles gérées par des tiers ?
  Par adaptations, on entend notamment l'actualisation et l'amélioration des politiques, procédures et mesures relatives à la sécurité de l'information et à la vie privée existantes.

- **Pourriez-vous clarifier le contenu de cette question ?**

Réponse 5

- Coquille dans la traduction néerlandais vers français !
- Correct : "Les adaptations des prestations de services faites par des tiers sont-elles gérées ?"
- Quand le service que fournit un sous-traitant change (changement de plateforme, d'accords, de responsabilités, ajout d'un champ dans une DB qui en changerait la sensibilité, **ou tout simplement changement de sous-traitant**), est-ce que les politiques ou mesures existantes sont suffisantes / applicables ? Il faut valider les changements de sous-traitants ou des activités de sous-traitants
- Si le service fourni par un tiers change, il faut s'assurer que les mesures garantissent toujours la sécurité.

Question 6

- 5.12.2b : Lorsque l'organisation souhaite traiter des données sensibles, confidentielles ou professionnelles dans un cloud, satisfait-elle aux garanties contractuelles minimales et aux directives telles que décrites au point 2.2, 2.3 et 2.4 de la politique « Cloud computing » ?

- **Les solutions mails de Microsoft (simplement l'interface Outlook ou MS365) sont, selon moi, des solutions Cloud. Microsoft ne satisfait pas à toutes les directives de la BCSS. Quelle alternative réaliste ?**

Réponse 6

- Le client Outlook sur un poste de travail pour réception et envoi d'emails n'est pas une solution Cloud ; hors scope (OK)
- L'utilisation de serveurs mail ou autre peut être faite on-premise ou via un fournisseur local ; mais ce n'est pas la mission de la BCSS de fournir des providers
- Les MNM sont (au moins) d'application pour les données sociales à caractère personnel ; O365 pas OK pour DSCP ; pour d'autres données il faut faire l'analyse au niveau de l'institution
  - Les MNM n'interdisent pas l'utilisation de O365 pour ce qui n'est pas données sociales à caractère personnel (contrats fournisseurs, schéma réseau, …)
- L'interdiction concerne l'export de DSCP vers un fournisseur sous tutelle d'un pays hors EU

Question 7

- 5.6.4 : L'organisation dispose-t-elle des autorisations nécessaires du comité de sécurité de l'information compétent pour l'accès aux données (sociales) à caractère personnel gérées par une autre organisation ?

- **N'est-ce pas le SPP IS qui se charge de toutes les autorisations ?**

Réponse 7

- Oui, c'est bien le SPP-IS
- Chaque donnée que vous recevez de la BCSS via le SPP-IS est cadrée par une délibération
- Les traitement liés à ces données doivent respecter les MNM et les finalités décrites dans la délibération (à garantir par les CPAS ; le SPP-IS n'exerce pas de contrôle)
- Le CPAS ne peut pas utiliser ces données pour d'autres finalités sans base légale valable

Question 8

- 5.3.2.1h : La possibilité de bloquer directement l'accès aux informations de l'organisation (données ou applications présentes sur l'appareil mobile) et d'effacer des données existe-t-elle ?

- **Est-ce que le fait de bloquer l'accès Windows sur le réseau et les codes d'accès sur les applications sont suffisants?**

- **Serait-il possible de nous donner un exemple concret permettant de supprimer les données sur un appareil mobile en cas de son vol?**

Réponse 8

- Non, ces mesures ne sont pas suffisantes. Il faut prévoir la mise en place d'un système de "Mobile Device Management" ("MDM")
  - Des solutions de MDM existent sur le marché
  - Concrètement, un employeur dispose d'un certain contrôle à distance sur un device managé
  - En cas de perte ou de vol, une suppression à distance des données peut être effectuée

Question 9

- (Question d'ordre général liée aux applications et aux logs)
- **Les "privacy logs" sont-ils utilisés uniquement en cas de développement des logiciels en interne ?**

Réponse 9

- Non, les privacy logs doivent être prévus pour tout système qui traite des données sociales à caractère personnel
- Il faut au minimum pouvoir y trouver :
  - Quelle opération a eu lieu (par exemple CRUD, ou Transfer to)
  - Quand l'activité a eu lieu (par exemple un timestamp)
  - Qui a réalisé l'activité (quel employé ou quelle organisation)
  - Sur quel système l'activité a eu lieu (identifiant unique d'application)
  - Au sujet de qui l'activité a eu lieu (NISS du Data Subject)
  - Quel est le résultat de l'activité (OK ou KO)
- Il est recommandé d'y trouver également :
  - La finalité du traitement (pourrait être déduite de l'identifiant de l'app)
  - La date de fin de vie du log (liée à la période de rétention du log)
  - Un numéro de transaction unique (lien entre plusieurs systèmes)

Question 10

- (Question d'ordre général liée à la détection d'intrusion)

- **Serait-il possible de nous donner un exemple sur une mesure qui permet de détecter des tentatives non autorisées de diffusion, de déchiffrement, d'accès ou de remplacement de clés ou de données chiffrés ?**

Réponse 10

- L'utilisation de logs sécurisés ("non-tamperable")
- L'utilisation d'un IDS et / ou d'un IPS
- L'utilisation d'un honeypot
- La détection de fausses données diffusées dans la nature

Question 11

- (Question d'ordre général liée à l'audit)

- **Quelle est la périodicité recommandée pour faire un audit de conformité de la situation relative à la sécurité de l'information et à la vie privée pour un CPAS ?**

Réponse 11

- Cette périodicité peut dépendre de nombreux facteurs ; pas de réponse fixe ou juridiquement valable. En général une entreprise effectue ce type d'audit tous les ans (par exemple pour une certification ISO27001)

- En ce qui concerne les MNM, un audit fait en interne (par exemple avec l'aide du DPO) peut suffire

Question 12

- (Question d'ordre général liée à l'outsourcing de logiciels)

- **Dans la partie ICT, la distinction entre ce qui concerne le développement de programmes en interne et l'achat / location de programmes à des tiers n'est pas toujours facile à faire. J'hésite ainsi souvent si je dois mettre "non applicable" (notre CPAS ne développe pas d'application en interne) ou considérer que ce point doit avoir fait l'objet d'une formalisation entre nous et nos fournisseurs (mais certains de ces points concernent du développement et non la mise en œuvre, donc la réponse ne paraît pas toujours évidente).**

Réponse 12

- Question dure à cerner, il faudrait être + spécifique par rapport à une ou plusieurs questions des MNM (donner leur numéro)

- De manière générale, qu'un service soit développé en interne ou outsourcé, il devra de toutes manières répondre aux exigences décrites dans les MNM

- La formalisation avec un fournisseur sera toujours bénéfique

Question 13

- 5.2.2a : L'organisation dispose-t-elle d'un processus d'évaluation des risques (utilisé dans le cadre des projets et des processus) qui tient compte de la sécurité de l'information et de la vie privée ?

- **Est-ce qu'on peut se limiter à généraliser les risques au niveau de l'institution ou doivent-ils être détaillés par service et/ou entités (homes/cpas)? Existe-il un canevas de base (hormis l'annexe C) ? Existe-t-il un tableau des risques générique, où les valeurs sont identiques à tous les CPAS (en parallèle avec les normes minimales)?**

Réponse 13

- La réponse à la première question peut varier en fonction du contexte. Vous pourriez disposer d'un registre des risques dans lequel des risques sont liés à la globalité de vos activités, et d'autres liés à une entité spécifique
- Il existe énormément de recommandations dans la littérature, et c'est à chaque institution de piocher dans ce qui correspond à son organisation ; voir notamment les principes de ISO 31000 (gestion des risques)
- Tableau générique : oui mais pas spécifiques aux CPAS (à notre connaissance)
  - Certains standards comportent des grilles qui peuvent vous servir d'inspiration ; COBIT, IRAM2, MONARCH, ...

Question 14

- 5.6.1b : L'organisation a-t-elle stimulé ses collaborateurs à lire et à appliquer les règlements relatifs à l'utilisation des systèmes d'information des portails ?

- **Dans la politique on parle uniquement de la fonction (minimum) du gestionnaire et co-gestionnaire, mais on ne lit nulle part les règles à appliquer par les "utilisateurs" repris sur le portail, peu importe leurs fonctions ou accès (match-it, digiflow, rapport unique, etc) ou encore la distinction entre ceux qui ont les accès à la partie sociale et les autres à la partie rémunération. Quid quand certains des utilisateurs sont des agents communaux faisant partie d'un service RH fusionné (CPAS-Commune), quid des règles à prévoir pour l'utilisation des informations du portail?**

Réponse 14

- De la sensibilisation doit être effectuée envers les collaborateurs en ce qui concerne l'application des principes de sécurité et du respect de la vie privée

Question 15

- 5.5.1b : L'organisation dispose-t-elle de procédures appropriées et de registres en vue de la labellisation (étiquetage) des traitements de l'ensemble des collectes de données, supports de données et systèmes d'information en cours de gestion, et ce conformément au schéma de classification interne ?

- **Dans quel type de données peut-on classifier les données du personnel, si celles-ci sont traitées par différents services dans un même bâtiment, dont certains services sont fusionné (RH, ICT) et d'autres non (stationnement, mobilité).**
- **Doit-on tenir compte de cette classification, dans les 2 cas, même si ce ne sont pas des agents CPAS qui traitent les données du personnel ?**

Réponse 15

- Il est possible que la classification soit de type "Confidentiel"
  - La classification est faite par le responsable de traitement avec le DPO / l'équipe de sécurité en conseil

- Oui en principe il faut toujours tenir compte de la classification des données

Question 16

- 5.15.2a : L'organisation dresse-t-elle régulièrement la carte des risques relatifs à la conformité au Règlement européen et exécute-t-elle les actions devenues nécessaires suite à un risque résiduel majeur de non-conformité ?

- **Règlement européen = RGPD? Peut-on l'inclure dans l'évaluation des risques ?**

Réponse 16

- Le terme "règlement européen" fait bien référence notamment au RGPD. Il faut toutefois prendre en considération d'autres règlements applicables au niveau de l'EU.
  - Voir par exemple la décision récente de la Cour de Justice Européenne concernant le cas "Schrems II"

- Oui vous pouvez inclure cette notion dans l'évaluation des risques de votre institution
  - Un DPIA est une analyse de risque

Question 17

- 5.9.5 : La gestion des logs est-elle prévue dès le début, dans le design lors du développement ou lors de la détermination des critères d'achat de systèmes ou d'applications, afin de réaliser un « security/privacy by design » ?

- **Terminologie "log "= login PC, log logiciel sociaux, log BCSS? Fichier ini/ ini-user? y a t'il d'autres log à tenir en compte?**

Réponse 17

- Il existe toute une série de logs qui doivent être pris en fonction des cas, avec au minimum les Privacy Logs et les Security Logs
  - Les Privacy Logs permettent de reconstruire une chaîne de traitements et de répondre à une série de questions (voir slides précédents)
  - Les Security Logs sont pris dans le but de détecter et / ou analyser les événements et les incidents de sécurité
  - Il n'y a pas de liste exhaustive concernant les Security Logs, ceci dépend des systèmes d'information que vous utilisez et des protections mises en place. Par exemple si vous utilisez un IDS, des logs supplémentaires seront créés par ce système.

Question 18

- 5.10.1a : L'organisation dispose-t-elle, pour l'ensemble des réseaux sans fil qu'elle a sous sa gestion et à tous les endroits, d'un processus permettant d'obtenir un aperçu de l'ensemble des réseaux sans fil existants et autorisés, des protocoles de sécurité utilisés par ces réseaux, et de l'ensemble des mesures de sécurité qui y sont associées ?

- **Hormis le WIFI (public/privé) quel type de réseau sans fil peut-on inclure dans cette norme? VPN?**

Réponse 18

- La BLD relative à cette question parle bien du WIFI (pas de la 4G par exemple) ; donc pas d'autre type à l'heure actuelle

- La notion de VPN est indépendante de la notion de réseau cablé VS WIFI ; il est possible d'être connecté à un VPN via cable ou via WIFI

Question 19

- Question d'ordre général au sujet de la cryptographie

- **Concernant la cryptographie : y a-t-il un standard qui a la préférence de la BCSS ?**

- **La cryptographie s'impose-t-elle pour toutes les communications (ce qui implique de chiffrer par exemple les e-mails) ?**

Réponse 19

- La BCSS n'a pas de préférence pour des standards ou algorithmes de cryptographie particuliers. Ceux-ci évoluent avec le temps.
  - Vous pouvez par exemple vous tourner vers ce que propose le NIST à ce sujet

- Il faut faire usage (ou non) de la crypto en fonction du degré de classification des données concernées
  - Un email contenant des DSCP devra être chiffré
  - Un email contenant la photo de votre chat ne devra pas être chiffré

- La crypto s'applique également pour protéger un site web (attaque MITM, ..), les flux entre institutions, certains stockages, ...

Question 20

- Question d'ordre général au sujet de la data classification

- **Concernant la classification des systèmes critiques : de quoi parlons-nous exactement ? Confidentiel-secret-top secret ? Il me semble que toutes les données des CPAS sont confidentielles ?**

Réponse 20

- La BCSS ne peut se prononcer sur la classification des données de chaque institution
  - Il est probable qu'une majorité de données traitées par un CPAS soit effectivement Confidentielles
  - Il est néanmoins possible que certaines informations soient tout simplement publiques (par exemple un guide informatif..)

Question 21

- 5.11.2d : A-t-on évité autant que possible la gestion des accès au niveau interne dans une application ?

- **« gestion des accès au niveau interne » : j'ai du mal à comprendre. Entend-on par là d'avoir un serveur dédié aux contrôles d'accès (Active Directory) ?**

Réponse 21

- Il est bon d'éviter d'avoir à faire une gestion de type "fine-grained" application par application depuis chaque application directement

- Effectivement une système de gestion central des droits d'accès est recommandé
  - Par ailleurs ceci simplifie la suppression de droits en cas de changement de fonction ou de départ d'un collaborateur

Question 22

- 5.8.3c2 : L'organisation réalise-t-elle une analyse des risques de la conformité au RGPD lorsqu'elle détruit des données à caractère personnel ? L'organisation valide-t-elle les risques des méthodes utilisées durant le cycle de vie complet des données: en usage, sous forme de backup et en transit ?

- **Pouvez-vous expliquer cette question ?**

Réponse 22

- Toute institution doit s'assurer que dans le cycle de vie complet de toute information, celle-ci soit protégée adéquatement en fonction de sa classification
  - Par exemple, lors de la destruction, est-il possible de reconstruire les données ?
    - Risque classique : utilisation d'un shredder qui permet de faire du puzzle et de tout reconstituer
  - Par exemple, lors de l'utilisation de backups, ces backups sont-ils protégés correctement ?
  - Par exemple, lors du stockage de données très sensibles, ce stockage est-il chiffré ?
  - Effacer un fichier et vider la corbeille ne supprime pas l'information du disque

Question 23

- 5.8.3e1 : L’organisation fixe-t-elle les mesures adéquates de suppression de données dans un contrat lorsqu’elle procède à la lecture des supports d'information ? (contexte : *mesures appropriées de suppression de données dans un contrat avec des tiers*)

- **Pouvez-vous expliquer cette question ?**

Réponse 23

- Toute institution doit s'assurer (en fonction de la classification des données..) que si un tiers accède (ou traite de manière générale) à des données, celui-ci prenne les mesures pour effacer ces données suite à une période de rétention adéquate ou à la fin du contrat
  - Si des données "passent" simplement par un fournisseur de services, il n'est pas sensé les stocker "par plaisir"
  - Si des données doivent être stockées par un fournisseur de services, il faut s'assurer qu'il ne les garde que pour une durée proportionnelle à la finalité des traitements
  - Des clauses adéquates doivent être définies dans les contrats appropriés
  - Il faut s'assurer que le sous-traitant est capable d'effacer les données

Question 24

- Question d'ordre général sur les médias et appareils mobiles
- **Quel est la différence entre médias et appareils mobiles ?**

Réponse 24

- Un **appareil** mobile est "intelligent" ; on parle là par exemple d'un smartphone ou d'une tablette, ou même d'un laptop

- Un **média** mobile n'est pas nécessairement "intelligent" ; donc ceci inclut les appareils mobiles, mais aussi des systèmes de stockage mobiles tels qu'une clé USB ou un disque dur externe

- Des mesures doivent être en place pour empêcher l'accès aux informations sensibles en cas de perte ou vol (remote wiping, encryption des données, ..)

Merci pour votre participation! :-)