SESSION DE SECURITE 2017 II

Gilles Kempgens

Conseiller en sécurité SPP IS

POD SPP | Maatschappelijke Integratie Intégration Sociale

PROGRAMME

1. INTRODUCTION – SUJETS A ABORDER
2. LEXIQUE
3. LE RGPD
4. LE DPD ET LE CONSEILLER EN SECURITE
5. LE WI FI ET L'IBPT

RGPD

LEXIQUE:

- DPD : Délégué à la Protection des Données
- RGPD: Règlement Général pour la Protection des Données
- AIPD: Analyse d'Impact préalable à la Protection des Données
- Autorité de la Protection des Données (ex Commission de la Vie Privée)
- DCP : Données à Caractère Personnel
- CPAS: ???

ACTUALITE 25/01/2018

L'Europe risque de ne pas être prête à temps pour garantir la protection des données

ELODIE LAMER

RGPD

QU’EST-CE QUE LE RGPD ?

LE REGLEMENT GENERAL DE LA PROTECTION DES DONNEES

BUT: DONNER AUX CITOYENS PLUS DE CONTROLE SUR LEURS DONNEES PERSONNELLES ET L’USAGE QUI EN EST FAIT

RGPD

LE RGPD EST UN CADRE JURIDIQUE POUR TOUS LES PAYS DE L'UE.

IL A POUR BUT DE SIMPLIFIER LES FORMALITES POUR LES ENTREPRISES PRIVEES **ET** PUBLIQUES

POD SPP Maatschappelijke Integratie Intégration Sociale

RGPD

BUT

Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures.

POD Maatschappelijke Integratie
SPP Intégration Sociale

RGPD

BUT

Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants).

POD Maatschappelijke Integratie
SPP Intégration Sociale

RGPD

BUT

Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et les sanctions renforcées.

POD SPP Maatschappelijke Integratie Intégration Sociale

RGPD

1 Des données à emporter !

Je peux récupérer les données que j'ai communiquées à une plate-forme et les transmettre à une autre (réseau social, fournisseur d'accès à internet, site de streaming, etc.)

Ceci concerne aussi les administrations.

Exemple: transfert de SPF à SPF, à une commune, etc

RGPD

A partir du 25 mai 2018, toute personne pourra venir au CPAS demander toutes les données qui la concernent, l'utilisation qui en est faite et la correction de celles-ci.

RGPD

3 Protection des mineurs

Les services en ligne doivent obtenir le consentement des parents des mineurs de moins de 16 ans avant leur inscription.

RGPD

4 Guichet unique

En cas de problème, je m'adresse à l'autorité de protection des données de mon pays, quel que soit le lieu d'implantation de l'entreprise qui traite mes données.

En Belgique, ce sera la nouvelle Commission de la vie privée qui devient **l'Autorité de la Protection des Données.**

RGPD

Jusqu'à 20.000.000 € d'amende ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires, l'amende la plus lourde étant choisie.

RGPD

6 Consécration du droit à l'oubli

Je peux demander à ce qu'un lien soit déréférencé d'un moteur de recherche ou qu'une information soit supprimée s'ils portent atteinte à ma vie privée.

Exemple: vous êtes victime d'une fausse accusation. La justice le constate et vous demandez à Google d'effacer tout ce qui a trait à cette fausse accusation.

RGPD

ATTENTION !!!

Le droit à l’oubli n’est pas toujours applicable dans les CPAS.

Exemple: étudiante, RTBF, archives du royaume, logiciel social, etc…

RGPD

Quels sont les acteurs impliqués ?

Les entreprises privées.

Les ASBL.

Les administrations.

Les sous-traitants (CIVADIS).

Toutes les entreprises privées ou publiques à partir du moment ou des données à caractères personnelles sont collectées.

RGPD

Comment cela s’organise-t-il ?

Il faut un registre des traitements de données plus communément appelé “Registre des traitements”.

Il faut un DPD, Délégué à la Protection des Données.

Il faut effectuer une Analyse d’Impact relative à la Protection des Données (AIPD).

Il faut protéger les données sur base de l’AIPD.

Il faut documenter vos données.

RGPD

Le registre des données

L’article 30 du RGPD impose la mise en place d’un registre tant par les responsables de traitement que par les sous-traitants.

RGPD

Le registre des données

Les CPAS sont-ils dans ce cas de figure ?

Les données qu'ils peuvent être amenés à traiter peuvent-elles comporter un risque pour les droits et libertés des personnes concernées ?

Que dit l'article 9 ?

RGPD

Article 9 du RGPD

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

Les traitements des données à caractère personnel qui révèlent:

- l'origine raciale ou ethnique;
- les opinions politiques;
- les convictions religieuses ou philosophiques;
- l'appartenance syndicale;
- le traitement des données génétiques,

RGPD

- des données biométriques aux fins d'identifier une personne physique de manière unique;
- des données concernant la santé;
- des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

sont interdits.

RGPD

Ces restrictions ne s'appliquent pas si:

- la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques …..;
- le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, **de la sécurité sociale et de la protection sociale ….**
- suite p. 38 du RGPD.

RGPD

LES **CPAS** SONT DONC **CONCERNES**.

ILS TRAITENT DES DONNEES A CARACTERE PERSONNEL.

ILS PEUVENT AVOIR DES DONNEES A CARACTERE MEDICAL (paiement des actes médicaux sur base de réquisitoire et de médicaments).

ILS ONT L'AUTORISATION LEGALE DE TRAITER CES DONNEES.

CERTAINES DONNEES CONSERVEES AU CPAS PEUVENT COMPORTER UN RISQUE POUR LES DROITS ET LIBERTES DE LEURS BENEFICIAIRES.

RGPD

COMMENT SE METTRE EN ORDRE AVEC LE RGPD EN 6 ETAPES ?

RGPD

ETAPE 1

RGPD: ETAPE 1

1. **Désigner un guide, un pilote appelé DPD, Délégué à la Protection des Données.**

Son profil:

- **informer et conseiller** le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- **contrôler le respect du RGPD** en conformité avec le droit national en matière de protection des données ;
- **conseiller le CPAS** sur la réalisation d'études d'impact sur la protection des données et en vérifier l'exécution ;
- **coopérer avec l'Autorité de la Protection des Données** et d'être le point de contact de celle-ci.

RGPD: ETAPE 1

Le DPD devra également:

- **s'informer** sur le contenu des nouvelles obligations (nouvelles techniques, nouvelles règlementations, nouveaux logiciels, nouvelles règles européennes..) ;
- **sensibiliser** les décideurs sur l'impact de ces nouvelles règles ;
- **réaliser l'inventaire** des traitements de données du CPAS et de ses Chapitres XII et autres ASBL ;
- **concevoir** des campagnes de sensibilisation ;
- **maintenir** la conformité au RGPD de façon permanente.

RGPD

ETAPE 2

RGPD: ETAPE 2

2. Faire un registre des traitements de données

- Faites l'inventaire des données à caractère personnel que le CPAS conserve et noter quelle est leur origine.
- Indiquer les personnes avec lesquelles vous les avez partagées.
- Enregistrez les traitements du CPAS: social, comptable, ressources humaines, logistique, distribution de repas, logiciel de patrimoine, etc.
- Eventuellement organiser un audit d'information à cet effet.

Ce registre doit être tenu de façon informatique et être clair et compréhensible.

RGPD: ETAPE 2

L'article 4 du RGDP définit un **traitement** comme

" toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que:

la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;"

RGPD: ETAPE 2

QUESTIONS:

1. Un CARDEX est-il un traitement ?
2. Un repertoire est-il un traitement ?
3. Une DB est-elle un traitement ?
4. Un registre des inscriptions est-il un traitement ?
5. Un tableau Excel avec la liste du personnel est-il un traitement ?
6. Les archives sont-elles un traitement ?

RGPD: ETAPE 2

Il faut donc faire l'inventaire des traitements.

RGPD: ETAPE 2

IL FAUT FAIRE L'INVENTAIRE DES DONNEES PERSONNELLES (NOTION CONNUE PAR TOUS LES CONSEILLERS EN SECURITE).

QUESTION: quelle donnée ci-dessous n'est pas une donnée personnelle ?

- Une plaque d'immatriculation.
- Un prénom.
- Un numéro d'abonnement.
- Un surnom.
- Un alias.
- Une adresse IP.

RGPD: ETAPE 2

Il faut ensuite décrire l'objectif principal de chaque application informatique de données personnelles. Exemples de finalité : gestion des recrutements, gestion des bénéficiaires, enquête de satisfaction, surveillance des locaux, etc.

Il faut déterminer qui traite les données, sous-traitants et fournisseurs compris pour actualiser les clauses de confidentialité.

Il faut identifier les origines et les destinations des données de chaque flux (A036 par exemple).

RGPD: ETAPE 2

En résumé et concrètement.

Pour chaque traitement de données, il faut se poser les questions suivantes:

Qui ?

- Inscrivez dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du DPD ;
- Identifiez les responsables des services opérationnels traitant les données au sein de votre organisme ;
- Etablissez la liste des sous-traitants.

RGPD: ETAPE 2

Exemple

Nom et coordonnées du responsable du traitement et son représentant légal:

CPAS d'Outsiplou, Directeur général: M. Dupont

Responsables de service traitant les données:

- Mme Dusollier, cheffe du service social;
- M. Duval: responsable du personnel;
- M. Charlet: responsable informatique.

Liste des sous-traitants: CIVADIS, Secrétariat social, firme informatique pour un soft comptable ou autre.

RGPD: ETAPE 2

Quoi ? Quel type de traitement ?

- Identifiez les catégories de données traitées: RN, composition familiale, adresse, …
- Identifiez les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple, les données relatives à la santé, les données financières).

RGPD: ETAPE 2

Pourquoi ?

Indiquer la ou les finalités pour lesquelles les données sont collectées ou traitées (exemple : ouverture d'un DIS, gestion RH, prime de première installation, minerval, etc…).

Où ?

Préciser où les données sont hébergées. Dans quel(s) pays ?

RGPD: ETAPE 2

Durée de conservation?

- Indiquer, pour chaque catégorie de données, combien de temps le CPAS les conserve.
- 1 an, 5 ans, 10 ans, 30 ans, 100 ans ?

RGPD: ETAPE 2

Comment les données sont-elles sécurisées?

- Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées ?

Ceci vaut pour les données digitales et les données sur papier.

RGPD: ETAPE 2

Exemples de mesure de sécurité d'accès:

- contrôle d'accès à la reception;
- enregistrement des identités des visiteurs;
- logging d'accès au réseau;
- logging d'accès au logiciel social;
- logging d'accès au logiciel du personnel;
- registre des accès aux archives;
- etc.

RGPD: ETAPE 2

EXEMPLE DE REPERTOIRE DES TRAITEMENTS SIMPLIFIE BASE SUR LE DOCUMENT DE L'AUTORITE DE LA COMMISSION DES DONNEES

(CF FICHIER EXCEL)

RGPD: ETAPE 2

RGPD

ETAPE 3

RGPD: ETAPE 3

Prioritiser les actions.

- S’assurez-vous que **seules les données strictement nécessaires** à la poursuite des objectifs sont collectées et traitées.

  Exemple: pas de récolte de données dans le but de faire des cadeaux.

RGPD: ETAPE 3

- Identifiez **la base juridique** sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale)
- Révisez vos **mentions d'information** afin qu'elles soient conformes aux exigences du règlement (articles 12, 13 et 14 du règlement).

RGPD: ETAPE 3

- Vérifiez que vos **sous-traitants** connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence, en matière de sécurité, **de clauses contractuelles rappelant les obligations du sous-traitant** (un document est en cours de rédaction au SPP IS) de confidentialité et de protection des données personnelles traitées.

RGPD: ETAPE 3

- Prévoir les modalités d'exercice des **droits des personnes** concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...).
- En ce qui concerne le droit à la portabilité, ce sera la responsabilité de CIVADIS.
- Vérifier les **mesures de sécurité** mises en place.

RGPD

ETAPE 4

RGPD: ETAPE 4

GERER LES RISQUES DONC FAIRE UNE AIPD

(Analyse d'Impact préalable relative à la Protection des Ponnées)

RGPD: ETAPE 4

QU'EST-CE QU'UNE AIPD OU UNE ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES ?

Une AIPD est un outil d'évaluation d'impact sur la vie privée.

Elle permet de construire des traitements de données respectueux de la vie privée et de démontrer la conformité des traitements au RGPD.

RGPD: ETAPE 4

Une AIPD doit contenir les éléments suivants:

- *une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;*
- *une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;*
- ***une évaluation des risques** pour les droits et libertés des personnes concernées conformément au paragraphe 1;*

https://www.privacycommission.be/node/20717

RGPD: ETAPE 4

- *les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées».*

Afin de mieux garantir le respect du présent règlement lorsque les opérations de traitement sont susceptibles d'engendrer **un risque élevé pour les droits et libertés des personnes physiques**, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque.

RGPD: ETAPE 4

Il convient de tenir compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le présent règlement.

En résumé, quels sont les risques existants liés aux données traitées, conservées, stockées, reçues et envoyées de et à l'extérieur du CPAS ?

RGPD: ETAPE 4

Qui participe à l'élaboration de l'analyse d'impact ?

Le responsable de traitement : il valide l'AIPD et s'engage à mettre en œuvre le plan d'action défini dans l'AIPD.

Le DPD: il élabore le plan d'action et se charge de vérifier son exécution.

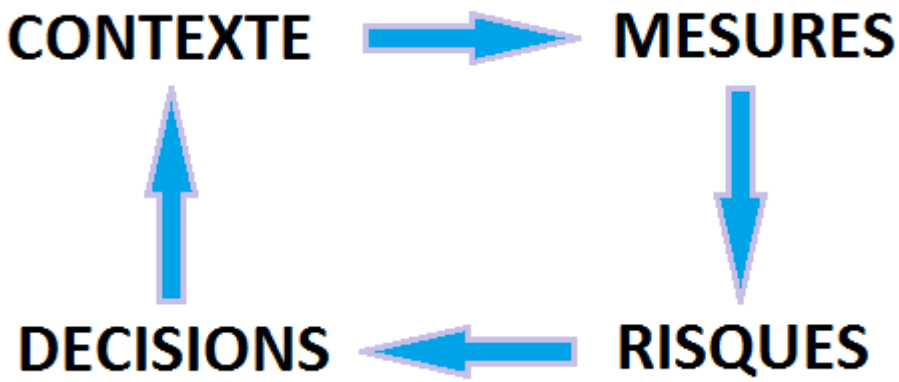
Le(s) sous-traitant(s) : fournit les informations nécessaires à l'élaboration du PIA.

Les métiers: le CS et le concepteur-développeur (: aident à la réalisation du PIA en fournissant les éléments adéquats.

Les personnes concernées : donnent leurs avis sur le traitement. Directeur, chef de service, autre.

RGPD: ETAPE 4

APPROCHE SIMPLIFIEE D'UNE METHODOLOGIE D'AIPD



RGPD: ETAPE 4

LE CONTEXTE

- Le CPAS est-il seul dans le bâtiment ?
- Est-il associé à une autre institution ?
- Des personnes étrangères au CPAS travaillent-elles dans le CPAS ?
- Qui gère l'informatique ? Le CPAS, une ou plusieurs firmes de soft ? L'informatique du CPAS travaille-t-elle dans un cloud ? Qui s'occupe des développements informatiques ? Qui a accès à distance à l'informatique (software et hardware) ?
- Quelles sont les mesures de protection (physiques, juridiques: clause de confidentialité, …) ?

RGPD: ETAPE 4

LES MESURES

- Quelles sont les mesures de sécurité existantes ?
- Les mesures de sécurité existantes sont-elles suffisantes ?
- Quelles sont les mesures de sécurité manquantes ou insuffisantes pour répondre aux exigences du RGPD ?
- Quelles sont les mesures de sécurité prévues ou à adopter pour réduire le risque à un niveau acceptable et proportionnel à l'importance des données ?

RGPD: ETAPE 4

LES RISQUES

Après avoir fait l’inventaire des risques, les évaluer en function des données traiteés, de leur impact possible sur la vie privée et voir s’ils sont correctement traités.

RGPD: ETAPE 4

Petite proposition d'évaluation des risques.

NATURE DES CONSEQUENCES							
					CAUSES HUMAINES		
Gravité	Perte financière en M €	Ordre public	Juridique judiciaire	Image de l'autorité	Divulgation de données non sensibles	Divulgation de données sensibles	Intégrité physique
	F	O	J	I	H1	H2	H3
1	0,1 - 1	Perturbation locale et momentanée	Sanctions internes	Plaintes occasionnelles	1 - 10 personnes	-	Traumatisme passager
2	1 - 10	Menace pour l'ordre public	Action en justice	Critiques dans les médias nationaux	11 - 100 personnes	1 - 10 personnes	Invalidité légère
3	10 - 100	Difficulté à maintenir l'ordre public	Condamnation de l'autorité	Critiques graves dans les médias nationaux	101 - 1000 personnes	11 - 100 personnes	Invalidité importante
4	> 100	Ordre public gravement en péril	Condamnation internationale de l'autorité	Critiques graves dans les médias internationaux	> 1000 personnes	> 100 personnes	Invalidité sévère - perte de vies humaines

RGPD: ETAPE 4

Petite proposition de classification simplifiée du niveau de risque

NATURE DES CONSEQUENCES							
					CAUSES HUMAINES		
Gravité	Perte financière en M €	Ordre public	Juridique judiciaire	Image de l'autorité	Divulgation de données non sensibles	Divulgation de données sensibles	Intégrité physique
	F	O	J	I	H1	H2	H3
1	1	1	1	1	1		1
2	2	2	2	2	2	1	2
3	3	3	3	3	3	2	3
4	4	4	4	4	4	3	4

Le niveau maximum de risque sera donc de 4 + 4 + 4 + 4 + 4 + 3 + 4 = 23 Si on atteint 15, on sera à 65% du risqué.

RGPD: ETAPE 4

Cette méthodologie ne prend pas en compte d'autres paramètres tels que:

- perte de temps ou temps d'indisponibilité;
- perte d'actifs (une DB par exemple);
- perte de confidentialité (cf Spectre et Meltdown);
- perte de preuve;
- etc.

Il existe de nombreuses méthodologies de gestion du risque ainsi que des listes de risques (ISO 27005).

RGPD: ETAPE 4

DECISIONS

A LA FIN DE L'AIPD, IL FAUT FAIRE UN BILAN / RISQUE.

RISQUE ACCEPTABLE → OUI ?

↓

PLAN D'ACTION ET VALIDATION

→ NON ?

↓

OBJECTIFS A ATTEINDRE ET NOUVELLE AIPD

RGPD: ETAPE 4

QUI PARTICIPE A L'AIPD ?

Toutes les personnes concernées:

- le Secrétaire – Directeur Général;
- le Directeur – Gestionnaire financier;
- les chefs de service concernés;
- les personnes concernées: le CS, le CISO, le DPD, le responsable informatique, le conseiller en prévention;
- certains sous-traitants: logiciels, clouds, …

RGPD: ETAPE 4

Il ne reste plus que le rapport de l'AIPD à mettre en forme. Ce rapport doit contenir les élements suivants:

Introduction

- Présentation du(des) traitement(s) considéré(s)

Résultats de l'AIPD

- - Description du contexte
- - Liste des mesures de nature juridique
- - Liste des mesures destinées à traiter les risques
- - Cartographie des risques

RGPD: ETAPE 4

Conclusion

- Décision argumentée de validation de l'AIPD

Annexes

- - Description détaillée du contexte
- - Présentation détaillée des mesures
- - Description détaillée des risques
- - Plan d'action

ATTENTION: à chaque changement de traitement, il faut mettre l'AIPD à jour. Il s'agit donc d'un processus dynamique.

RGPD: ETAPE 4

IL EXISTE UN OUTIL RELATIVEMENT CONVIVIAL:

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

RGPD

ETAPE 5

RGPD: ETAPE 5

ORGANISER

1.S’organiser pour prendre en compte la sécurité des données dès le départ: par défaut et lors de la conception.

Cela implique la minimisation de la collecte de données au regard de la finalité, les cookies, la durée de conservation, les mentions d’information, le recueil du consentement (si nécessaire), la sécurité et la confidentialité des données, s’assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données.

RGPD: ETAPE 5

2. Sensibiliser et organiser la remontée d’information en organisant un système de communication auprès de vos collaborateurs.
3. Traiter les réclamations et les demandes des personnes concernées quant à l’exercice de leurs droits (droits d’accès, de rectification, d’opposition, droit à la portabilité, retrait du consentement) en définissant qui fait quoi (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen).

RGPD: ETAPE 5

4. anticiper les violations de données en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

Attention, en cas de violation de données, vous êtes tenus d'en informer l'Autorité de la Protection des Données (ex Commission de la Vie Privée).

Ne pas respecter cette règle peut mener à des sanctions.

Article 33, §1 RGPD: en cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

RGPD: ETAPE 5

Qu’est-ce qu’une violation de données à caractère personnel?

3 conditions :

- mise en œuvre d’un traitement de données personnelles;
- ces données ont fait l’objet d'une violation (destruction, perte, altération, divulgation ou un accès non autorisé à des données personnelles, de manière accidentelle ou illicite);
- La violation est intervenue dans le cadre de votre activité de fourniture de services de communications électroniques(par exemple, lors de communications d’informations d’un bénéficiaire).

RGPD: ETAPE 5

La notification doit être transmise à l'Autorité de la Protection des Données dans les 72h de la constatation de la violation.

- Si le CPAS ne peut fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, le CPAS doit joindre les motifs du retard.

Attention, l'Autorité de la Protection des Données en Belgique pourra ajouter d'autres exigences. Il faudra donc se tenir au courant.

RGPD: ETAPE 5

Que mettre dans la notification de la violation ?

L’article 33, §3 du RGPD donne toutes les informations à ce sujet.

RGPD

ETAPE 6

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

RGPD: ETAPE 6

DOCUMENTER

Documenter pour prouver la conformité.

1. Documenter les traitements de données à caractère personnel:
   a) le registre des traitements;
   b) l'AIDP (ou DPIA).
2. L'information des personnes:
   a) les mentions d'information;
   b) les modèles de consentement;
   c) les procédures créées pour l'exercice des droits (droit de modification, à l'oubli, etc.).

RGPD: ETAPE 6

3. Les contrats avec les definitions des rôles et des responsabilités des intervenants:
   a) les contrats avec les sous-traitants;
   b) les procédures internes en cas de violation de don nées;
   c) les preuves que les personnes concernées ont donné leur consentement lorsque cela s'avère nécessaire.

RGPD DIVERS

Et les sous-traitants ?

RGPD Article 37 §1

Désignation du délégué à la protection des données

1.Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

RGPD DIVERS

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 (les exceptions) et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

RGPD

LE DPD ET LE CS

MAIS QUI SERA LE DPD ?

UNE NOUVELLE PERSONNE ?

LE CONSEILLER EN SECURITE ?

UN EXPERT EXTERIEUR ?

UN FOURNISSEUR ?

LE DPD ET LE CS

SITUATION ACTUELLE

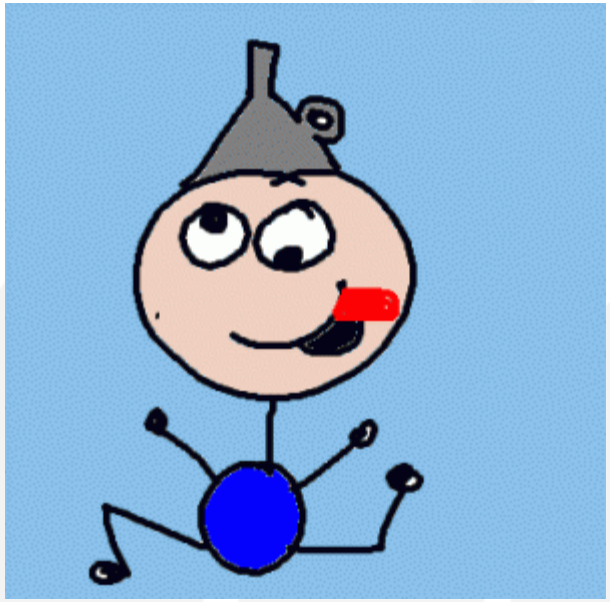
IL EXISTE UNE PROPOSITION D'AR PREVOYANT QUE LE CONSEILLER EN SECURITE ET LE DPD SOIENT LA MEME PERSONNE.

LE DPD ET LE CS

DANS LES NOUVELLES NORMES MINIMALES, ON CITE TANTOT LE CONSEILLER EN SECURITE, TANTOT LE DPD, TANTOT LE CISO.

LE DPD ET LE CS

ET IL EXISTE UNE PROPOSITION DE LOI SUR UN REGISTRE DES TRAITEMENTS STANDARDISE.



LE DPD ET LE CS

REPONSE: ON NE SAIT PAS ENCORE

MAIS

MAIS

MAIS

IL FAUDRA PENSER A TROUVER DES SOLUTIONS MUTALISEES EN WALLONIE.

LE DPD ET LE CS

WI FI ET IBPT

L'IBPT A DECRETE QUE METTRE UN WI FI A DISPOSITION NE FAIT PAS DU CPAS UN FOURNISSEUR DE SERVICE.

LES JURISTES DE L'UNAMUR ET DE L'ICHEC DECLARENT QUE LE FOURNISSEUR D'ACCES AU WI FI DOIT CONSERVER TOUTES LES TRACES DES ACCES SANS NECESSAIREMENT CIBLER L'IDENTITE DE L'UTILISATEUR

SESSION DE SECURITE 2017 I: FIN

QUESTIONS???

FIN