Gilles Kempgens
Conseiller en sécurité SPP IS

POD Maatschappelijke Integratie
SPP Intégration Sociale

SESSION DE SECURITE 2017 I

PROGRAMME

1. LE RGPD: BREF RAPPEL
2. COMMENT SE METTRE EN ORDRE EN 6 ETAPES ?
3. LE WI FI ET L'IBPT

POD Maatschappelijke Integratie
SPP Intégration Sociale

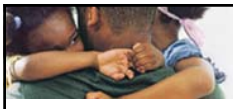
.be

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 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

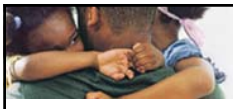
RGPD

LE REGISTRE DES TRAITEMENTS

POD Maatschappelijke Integratie
SPP Intégration Sociale

5

.be



RGPD

ETAPE 1

POD Maatschappelijke Integratie
SPP Intégration Sociale

6

.be

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.

POD Maatschappelijke Integratie
SPP Intégration Sociale

7

.be

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 institutions ;
- **concevoir** des campagnes de sensibilisation ;
- **maintenir** la conformité au RGPD de façon permanente.

POD Maatschappelijke Integratie
SPP Intégration Sociale

8

.be

RGPD

ETAPE 2

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

RGPD: ETAPE 2

Faire un registre des traitements de données

- Faire l'inventaire des données à caractère personnel que le CPAS conserve et noter leur origine.
- Indiquer les personnes avec lesquelles elles sont partagées.
- Enregistrez les traitements du CPAS: social, comptable, ressources humaines, logistique, distribution de repas, logiciel de patrimoine, etc.

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

RGPD: ETAPE 2

Faire un registre des traitements de données

- Eventuellement organiser un audit d'information à cet effet.

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

POD Maatschappelijke Integratie
SPP Intégration Sociale

11

.be

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.

POD Maatschappelijke Integratie
SPP Intégration Sociale

12

.be

RGPD: ETAPE 2

Par traitement, on comprend:

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."

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

RGPD: ETAPE 2

Il faut donc faire l'inventaire des traitements.

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

RGPD: ETAPE 2

IL FAUT FAIRE L'INVENTAIRE DES DONNEES PERSONNELLES (NOTION TRES ELARGIE AUJOURD'HUI).

EXEMPLES

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

POD Maatschappelijke Integratie
SPP Intégration Sociale

15

.be

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;
- remédiation de dette;
- enquête de satisfaction;
- suivi des visites du site internet;
- suivi de la page FaceBook;
- surveillance des locaux, etc.

POD Maatschappelijke Integratie
SPP Intégration Sociale

16

.be

RGPD: ETAPE 2

Il faut déterminer qui traite les données:

- sous-traitants;
- fournisseurs;
- intégrateurs;
- autres;

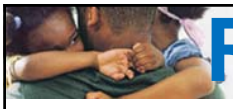
pour actualiser les clauses de confidentialité

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

POD Maatschappelijke Integratie
SPP Intégration Sociale

17

.be



RGPD: ETAPE 2

En résumé et concrètement.

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

Qui ?

- Inscrire dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et celui du DPD.
- Identifier les responsables des services opérationnels traitant les données au sein de votre organisme.
- Etablir la liste des sous-traitants.

POD Maatschappelijke Integratie
SPP Intégration Sociale

18

.be

RGPD: ETAPE 2

Exemple

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

CPAS X, Directeur général: M. Lambert

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 ?

- Identifier les catégories de données traitées: RN, composition familiale, adresse, …
- Identifier 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 ? Chez quel fournisseur ? Chez quel intégrateur ?

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

Durée de conservation?

Attention: le RGPD demande de ne pas conserver des données plus longtemps que nécessaire.

Exemples:

- les images de caméras doivent être effacées après un mois sauf incident (attention à la nouvelle loi en arrivance);
- les données relatives au paiement des salaires et aux horaires travaillés: 5 ans;
- les données médicales: 10 ans sauf législation spécifique aux CPAS par exemple.

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 réception;
- 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.

POD Maatschappelijke Integratie
SPP Intégration Sociale

25

.be

RGPD

ETAPE 3

POD Maatschappelijke Integratie
SPP Intégration Sociale

26

.be

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 de bénéficiaires potentiels, de visiteurs.

POD Maatschappelijke Integratie
SPP Intégration Sociale

27

.be

RGPD: ETAPE 3

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

POD Maatschappelijke Integratie
SPP Intégration Sociale

28

.be

RGPD: ETAPE 3

Modèles de registre disponibles:

- Le registre de traitement du SPP IS en préparation qui sera mis à disposition début avril. Ce modèle est inspiré de celui de la BCSS.
- Modèle de la Commission très complet mais complexe.
- Modèle de la CNIL.
- Etc

POD Maatschappelijke Integratie
SPP Intégration Sociale

29

.be

REGISTRE DES TRAITEMENTS

Processus: enquête sociale => RMI / DIS & equivalent RIS

Nom du processus: un processus (dans le contexte du RGPD) est un groupe de traitements où des données à caractère personnel sont traitées.

Exemple: consultation des données Registre national et de la composition de ménage

POD Maatschappelijke Integratie
SPP Intégration Sociale

30

.be

REGISTRE DES TRAITEMENTS

Finalités de l'activité du traitement

Exemples: accorder de l'aide aux bénéficiaires, vérifier les conditions d'octroi.

Nom des activités de traitement

Information nécessaires dans les contrats entre le sous-traitant et le responsable du traitement lorsque ce traitement est exécuté par une autre partie (article 28.3 RGPD) - voir registre "sous-traitant"

REGISTRE DES TRAITEMENTS

Finalités de l'activité du traitement: loi organique

Catégorie de données fonctionnelles:

données d'identification personnelles disponibles à la demande

Catégorie(s) d'intéressés : données pouvant être considérées de façon générale comme une augmentation du risque potentiel concernant les droits et libertés des personnes (cf Art. 9)

REGISTRE DES TRAITEMENTS

Sous-traitant : information enregistrée dans un onglet consacré aux sous-traitants

Identification du contrat de traitement de données avec le sous-traitant: indiquer les informations relatives au contrat

Catégorie(s) de destinataires (*) : informations à fournir à l'intéressé lorsque celui-ci souhaite exercer son droit d'accès (article 15 RGPD)

RGPD

ETAPE 4

RGPD: ETAPE 4

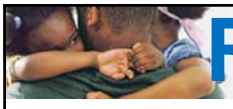
GERER LES RISQUES
DONC FAIRE UNE AIPD

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

POD Maatschappelijke Integratie
SPP Intégration Sociale

35

.be



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.

POD Maatschappelijke Integratie
SPP Intégration Sociale

36

.be

RGPD: ETAPE 4

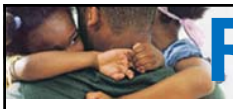
Une AIPD doit contenir les éléments suivants:

- *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 de l'article 35 du RGPD (traitement – risque – analyse d'impact);*

POD Maatschappelijke Integratie
SPP Intégration Sociale

37

.be



RGPD: ETAPE 4

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.

- *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». Article 35, §7, d*

POD Maatschappelijke Integratie
SPP Intégration Sociale

38

.be

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 effectue/fait effectuer et valider 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.

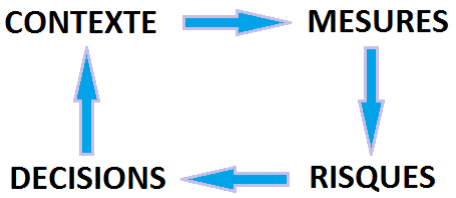
Le(s) sous-traitant(s) : fournit les informations nécessaires à l'élaboration du PIA.

Les métiers: le DPD 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

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

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.

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

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 ?

↓

VALIDATION +
EVENTUELLEMENT PLAN D'ACTION

→

NON ?

OBJECTIFS A ATTEINDRE ET NOUVELLE AIPD

RGPD: ETAPE 4

LES RISQUES

Il existe d'autres methodes efficaces dont:

https://www.cnil.fr/fr/rgpd-un-logiciel-pour-realiser-son-analyse-dimpact-sur-la-protection-des-donnees-pia

Celle-ci a le mérite d'être simple.

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

RGPD: ETAPE 4

LA Commission de la vie privée a aussi créé une analyse de risque ainsi que la BCSS.

Les outils sont disponibles sur leurs sites.

A noter que toutes les methodes sérieuses sont autorisées pourvu qu'elles respectent les prérequis du RGPD (art. 35, § 7).

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

RGPD: ETAPE 4

QUI PARTICIPE A L'AIPD ?

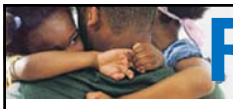
Toutes les personnes concernées:

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

POD Maatschappelijke Integratie
SPP Intégration Sociale

51

.be



RGPD: ETAPE 4

Il ne reste plus que le rapport de l'AIPD à mettre en forme. Ce rapport doit répondre à des exigences détaillées dans le RGPD.

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

POD Maatschappelijke Integratie
SPP Intégration Sociale

52

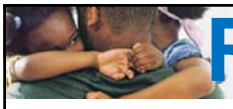
.be

RGPD

ETAPE 5

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be



RGPD: ETAPE 5

ORGANISER

1. S'organiser pour compléter le registre de traitement des données et l'Analyse d'Impact.
2. Impliquer toutes les personnes concernées.
3. Coordonner les actions sous l'égide du DPD.
4. Documenter et faire les rapports.
5. Mettre à jour régulièrement.

POD Maatschappelijke Integratie
SPP Intégration Sociale

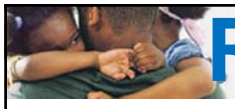
.be

RGPD

ETAPE 6

POD Maatschappelijke Integratie
SPP 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 aux 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.).

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

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.

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

MERCI

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be