Le RGPD : Quelles implications pour les CPAS ?
Fédération des CPAS – Namur – 27 mars 2018

RGPD : Quelles responsabilités pour les CPAS ?

Loïck Gérard
Assistant à la Faculté de droit de l'UNamur et chercheur Chaire Egov/CRIDS
loick.gerard@unamur.be

1. *Cadre actuel et futur*
2. *Qu'est-ce que le RGPD ?*
3. *Principes fondamentaux*
4. *Obligations du responsable de traitement*
5. *RGPD et sanctions*

1. Cadre actuel et futur – Actuellement: règles éparses

- Directive UE 95/46

Loi générale

- Loi « vie privée » (du 8/12/1992 sur la protection de la vie privée à l'égard des traitements de données à caractère personnel)

Lois sectorielles

- Loi « Banque-carrefour de la sécurité sociale » (15/01/1990)
- Loi « Registre national » (8/08/1983)
- Loi « eHealth » (21/08/2008)
- …

Décrets

- Décret RW/CF « Partage de données » (10/07/2013)
- Décret flamand « Echange électronique de données administrative » (18/08/2008)
- Ordonnance Bruxelloise « Intégrateur de données » (8 mai 2014)
- …

1. Cadre actuel et futur – Futur avec le RGPD

A partir du 25 mai 2018:

- ~~Directive UE 95/46~~

Loi générale

- ~~Loi « vie privée » du 8/12/1992~~

Lois sectorielles

RGPD permet leur maintien

Loi-cadre

En cours d'analyse par le Conseil d'Etat

Loi du 3 décembre 2017 sur l'Autorité de protection des données

Remplace la Commission vie privée → ! Supprime les comités sectoriels

2. Qu'est-ce que le RGPD ?

- Reprise des grands concepts et principes de la Directive / Loi de 92 :
  - **Données à caractère personnel**
  - **Traitement de données**
  - **Responsable du traitement et sous-traitants**
  - **Licéité du traitement**
- Le RGPD est une évolution, pas une révolution
  - Pas de chamboulement au niveau des principes

2. Qu'est-ce que le RGPD ?

- Donnée à caractère personnel :
  - Identifie ou rend identifiable…
    - Moyens raisonnablement susceptibles d'être utilisés
    - Identification directe ou indirecte
    - Tenir compte des technologies disponibles et de leur évolution
  - …une personne physique (« personne concernée »)
  - Exemples :
    - Noms et prénoms
    - Une photographie
    - Un numéro de téléphone / adresse mail
    - Numéros d'identification (NIRN / NISS)
    - Adresse postale
    - Résultat d'un examen médicale (donnée sensible)
    - Préférences alimentaires et contre-indications
    - …

2. Qu'est-ce que le RGPD ?

- « Traitement » de données à caractère personnel :
  - Opération ou ensemble d'opérations appliquée à des données à caractère personnel :
    - Collecter les données
    - Enregistrer les données
    - Utiliser les données
    - Consulter les données
    - Communiquer les données
    - …
  - Peu importe que le traitement soit automatisé ou manuel
    - Si traitement manuel : données contenues dans un fichier = ensemble structuré + accès selon critères déterminés
  - Peu importe le support utilisé (numérique ou papier)

2. Qu'est-ce que le RGPD ?

- Responsable du traitement et sous-traitant
  - **Responsable du traitement**
    - Acteur principal du traitement
      - » Définit les finalités du traitement : quel est l'objectif poursuivi ?
      - » Définit les moyens du traitement : comment traite-t-on les données ?
    - **Principal débiteur des obligations** du RGPD (droits des personnes concernées, registre, analyse d'impact,…)
  - Sous-traitant
    - Traite des données pour le compte du responsable de traitement
    - Ne peut traiter les données que sur ordre du responsable du traitement
    - En mesure de répondre aux exigences du RGPD (garanties contractuelles)

2. Qu'est-ce que le RGPD ?

- Responsable du traitement et sous-traitant
  - Relation contractuelle imposée et mentions obligatoires :
    - Ainsi, le sous-traitant doit notamment :
      - » Traiter les données uniquement s'il en reçoit l'ordre du responsable
      - » Prendre les mesures permettant de garantir la sécurité des données
      - » Obtenir l'autorisation du responsable pour recourir aux services d'un sous-traitant « secondaire »
      - » Assister le responsable du traitement sur les questions de sécurité du traitement et d'exercice des droits des personnes concernées

2. Qu'est-ce que le RGPD ?

- Quand suis-je autorisé à traiter des données ? *Licéité* du traitement
  - **Consentement de la personne concernée**
  - Nécessaire à l'exécution d'un contrat
  - **Nécessaire au respect d'une obligation légale**
  - Intérêt vital de la personne concernée
  - **Nécessaire à l'exécution d'une mission d'intérêt public / relevant de l'exercice de l'autorité publique**
  - ~~Intérêt légitime du responsable du traitement~~

2. Qu'est-ce que le RGPD et qui doit l'appliquer ?

- Quand suis-je autorisé à traiter des données ? *Licéité* du traitement
  - Consentement
    - Caractéristiques : libre / spécifique / éclairé / univoque
    - Ne se présume pas (« acte positif clair »)
    - Peut être retiré à tout moment
    - Le responsable du traitement doit être en mesure de prouver l'existence du consentement
    - Renforcement du critère de liberté du consentement pour les autorités publiques

3. Principes fondamentaux

- Comment dois-je traiter des données ?
  - Loyauté et transparence
    - Fourniture d'informations aux personnes concernées
    - D'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples
    - Obligation (droit) d'information

3. Principes fondamentaux

- Comment dois-je traiter des données ?
  - Limitation des finalités
    - Finalités déterminées, explicites et légitimes
    - Pas de traitement ultérieur incompatible
      - » Evaluation de la compatibilité : critère de l'attente raisonnable

3. Principes fondamentaux

- Comment dois-je traiter des données ?
  - Minimisation des données
    - Données adéquates, pertinentes et limitées à ce qui est nécessaire
    - Dans la mesure du possible : coder les données
      - » ATTENTION : pseudonymiser n'est pas anonymiser !

3. Principes fondamentaux

- Comment dois-je traiter des données ?
  - Exactitude
    - Données exactes et mises à jour
  - Limitation de la conservation
    - Pas de conservation pendant une durée excédant celle nécessaire aux finalités

3. Principes fondamentaux

- Comment dois-je traiter des données ?
  - Intégrité et confidentialité
    - Sécurité des traitements et du système informatique
  - Responsabilité ou « *accountability* »
    - Changement de paradigme >< Directive
      - » Pouvoir « rendre des comptes » >< Déclaration préalable

4. Obligations du responsable de traitement

- Respecter les droits des personnes concernées
- « *Accountability* »
- « *Privacy by default and by design* »
- Désignation d'un DPO
- Tenue d'un registre de traitements
- Analyse d'impact
- Sécurité
- Notification des violations de données

4. Obligations du responsable de traitement

Droit des personnes concernées

- Droit à l'information (cfr « Loyauté et transparence »)
- Droit d'accès
- Droit de rectification
- Droit à l'effacement (« Droit à l'oubli »)
- Droit à la limitation du traitement
- Droit à la portabilité des données
- Droit d'opposition
- Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé

4. Obligations du responsable de traitement

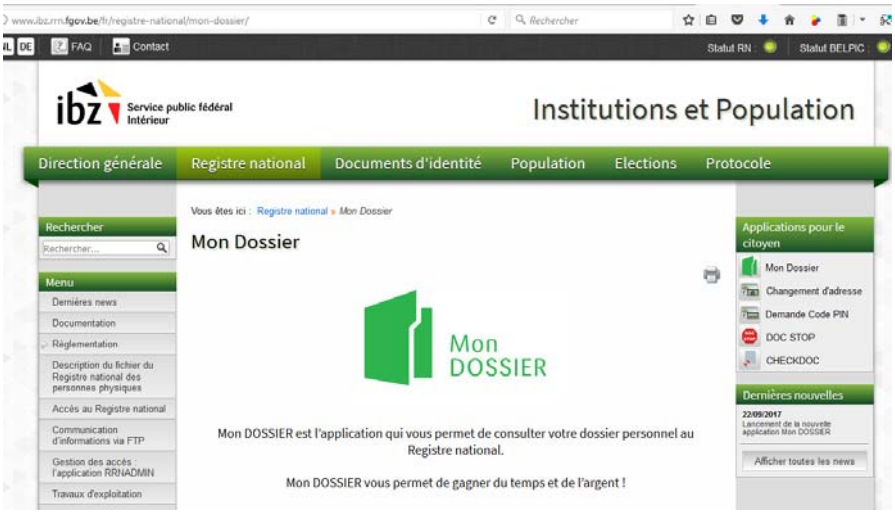
– Droit à l'information (cfr « Loyauté et transparence »)

	Données collectées auprès de la personne	**Données non collectées auprès de la personne**
Quand?	Au moment où les données sont collectées	- Délai raisonnable après la collecte (max 1 mois) - Si données utilisées pour communiquer avec la personne ou communiquées à un autre destinataire : avant la première communication
Quelles infos?	Informations obligatoires Informations complémentaires « nécessaires pour garantir un traitement équitable et transparent »	
Exception ?	Si la personne dispose déjà des informations	Si la personne dispose déjà des informations Si la communication s'avère impossible/ nécessiterait des efforts disproportionnés Si l'obtention/communication est prévue (loi)

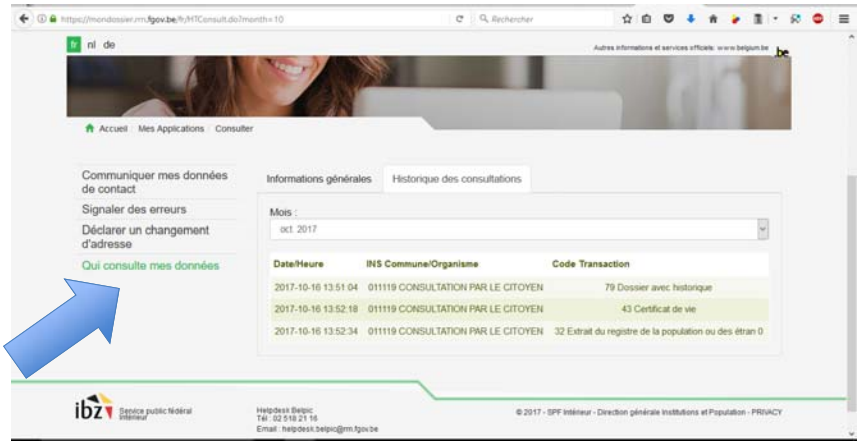
4. Obligations du responsable de traitement

– Droit d'accès

- Droit du citoyen de connaître ce que l'administration détient sur lui, pour quelle raison, ce qu'elle en fait, etc.
- Droit d'obtenir :
  - La confirmation que des données sont (ou non) traitées
  - Si oui, l'accès aux données + communication d'informations
  - Une copie des données faisant l'objet du traitement (Nouveauté RGPD)



http://www.ibz.rrn.fgov.be/fr/registre-national/mon-dossier/



Lettre type droit d'accès direct

(responsable du traitement)
Nom
Adresse

Mon prénom et mon nom
Mon adresse

Concerne : droit d'accès à mes données à caractère personnel

lieu et date

Madame, Monsieur,

Veuillez trouver ci-joint une demande d'accès aux données à caractère personnel que vous possédez éventuellement me concernant.
Conformément à l'article 10 de la Loi vie privée[1] vous êtes tenu de m'informer si vous avez ou non traité des données à caractère personnel me concernant. Si c'est le cas, veuillez également me communiquer les informations suivantes (veuillez cocher les informations que vous désirez recevoir):

- ☐ la nature des données me concernant que vous traitez ;
- ☐ la finalité pour laquelle vous utilisez ces données ;
- ☐ l'origine de ces données (où et comment vous les avez obtenues) ;
- ☐ les catégories de personnes auxquelles ces données seront communiquées: à qui vous les avez communiquées ou à qui vous pourriez (éventuellement) les communiquer ultérieurement ;
- ☐ les données exactes me concernant que vous traitez.

https://www.privacycommission.be/fr

4. Obligations du responsable de traitement

- Droit de rectification
  - Rectification de données inexactes + compléter des données incomplètes
- Droit à l'effacement (« Droit à l'oubli ») (« Nouveauté » RGPD)
  - Données plus nécessaires par rapport aux finalités / ont fait l'objet d'un traitement illicite / retrait de consentement
    - Exception: Traitement nécessaire pour respect obligation légale / exécution mission d'intérêt public

4. Obligations du responsable de traitement

- Comment communiquer ?
  - De façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simple
- À quel prix ?
  - Principe : Aucun paiement ne peut être exigé
- Quel délai pour réagir ?
  - Dans les « meilleurs délais » – Maximum 1 mois à compter de la réception de la demande

4. Obligations du responsable de traitement

- « *Accountability* »
  - Le responsable de traitement doit pouvoir « rendre des comptes » pour démontrer qu'il respecte le RGPD
- « *Privacy by default and by design* »
  - Assurer la protection des données dès la conception du service et de son architecture IT
  - Par défaut, assurer une protection maximale

4. Obligations du responsable de traitement

- Désignation d'un DPO (Data protection officer = Délégué à la protection des données)
  - **Obligatoire** pour les organismes publics
  - Cfr présentations ultérieures

4. Obligations du responsable de traitement

- Tenue d'un registre de traitements
  - Cfr présentations ultérieures
- Analyse d'impact
  - Cfr présentations ultérieures

4. Obligations du responsable de traitement

- Sécurité
  - Mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (Proportionnalité)
- Notification des violations de données
  - Violation: Destruction, perte, vol, hacking,…
  - Notification:
    - À l'autorité de contrôle
    - Aux personnes concernées si risque élevé pour leurs droits

5. RGPD et sanctions

- Un des changements majeurs : renforcement des sanctions
- But poursuivi : effectivité du RGPD
- L'Autorité de contrôle se voit octroyer plus de pouvoirs
  - Cfr présentation ultérieure
- Les amendes administratives ne sont pas les seules sanctions

5. RGPD et sanctions

- Qui peut me sanctionner ?
  - La CPVP
    - Suite à une plainte d'un particulier / d'un organisme de défense de la vie privée
    - Pouvoirs d'enquêtes (ordonner transmission de documents, audit, obtenir l'accès aux locaux et aux données,…)
    - Mesures correctrices
      - » Rappel à l'ordre
      - » Ordonner l'exécution d'une obligation (ex : respecter droits des personnes concernées)
      - » Limitation / interdiction de traitement
      - » Amendes administratives
    - Possibilité de recours judiciaire contre ces sanctions

5. RGPD et sanctions

- Qui peut me sanctionner ?
  - La CPVP : amendes administratives
    - Proportionnées et dissuasives
    - Plafonnées à 10 ou 20 millions d'€ selon les cas
      - » 10 M : relations avec sous-traitant / tenue du registre / analyse d'impact / désignation du DPO / …
      - » 20 M : licéité du traitement / droit des personnes concernées / non-respect injonction CPVP
    - Applicables aux pouvoirs publics ?

5. RGPD et sanctions

- Qui peut me sanctionner ?
  - Le juge
    - Suite à une plainte d'un particulier / d'un organisme de défense de la vie privée
    - Mêmes « mesures correctrices » que CPVP
    - Réparation du préjudice matériel et moral subi
      - » Responsabilité solidaire responsable traitement – sous-traitant
      - » Exonération si preuve « que le fait qui a provoqué le dommage » n'est pas imputable

Le RGPD : Quelles implications pour les CPAS ?
Fédération des CPAS – Namur – 27 mars 2018

Merci pour votre attention !

Loïck Gérard
loick.gerard@unamur.be

crids CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ
NADI Namur Digital Institute
CHAIRE eGOV UNAMUR
UNIVERSITÉ DE NAMUR