5. RÈGLEMENT GÉNÉRAL DE LA PROTECTION DES DONNÉES (RGPD)

CNR 073/17 – madame Legiest/ madame Audrey Van Schaeren

ORDRE DES MEDECINS
CONSEIL NATIONAL

ORDE DER ARTSEN
NATIONALE RAAD

DÉLÉGUÉ À LA PROTECTION DES DONNÉES

ORDRE DES MEDECINS
CONSEIL NATIONAL

ORDE DER ARTSEN
NATIONALE RAAD

1. QUI EST LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES?

Audrey Van Scharen

- DPD Conseil national
- Jurist
- privacy@ordomedic.be
- 0478/70.31.58

QU’EST-CE QUE LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)?

ORDRE DES MEDECINS
CONSEIL NATIONAL

ORDE DER ARTSEN
NATIONALE RAAD

2. QU'EST-CE QUE LE RGPD?

2.1. Quid des données à caractère personnel?

- Toute information se rapportant à une personne physique susceptible d'être identifiée, directement ou indirectement.
- Par exemple: un identifiant, un nom, une photo, un numéro de sécurité sociale, un matricule interne, une plaque d'immatriculation, une adresse postale, un numéro de téléphone, des données de localisation, un identifiant en ligne (adresse IP par exemple), un enregistrement vocal, …
- Catégorie particulière: données de santé
- Identifiables par tous les moyens actuels et futurs
- Pas les personnes décédées (mais bien les informations génétiques de ces personnes) ou données anonymes (attention: c'est différent des données à caractère personnel pseudonymisées qui sont toujours des données à caractère personnel)

2. QU’EST-CE QUE LE RGPD?

2.2. Quid du traitement?

- 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 des données à caractère personnel.

2. QU'EST-CE QUE LE RGPD?

2.3. Qui traite les données à caractère personnel?

Responsable du traitement: détermine l'objectif et les moyens pour le traitement des données à caractère personnel

p. ex. informations à caractère personnel, dossiers disciplinaires, fichier des membres, etc.

Sous-traitant: traite les données à caractère personnel pour le responsable du traitement

p. ex. envoi d'informations au SPF, SD WORX, etc.

3. QUELLES SONT LES OBLIGATIONS REPRISES DANS LE RGPD?

ORDRE DES MEDECINS
CONSEIL NATIONAL

ORDE DER ARTSEN
NATIONALE RAAD

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.1. Aperçu

1. Obligation de justification
2. Respect des principes du RGPD
3. Délégué à la protection des données (DPD)
4. Sensibilisation
5. Registre des données
6. Base légale pour le traitement des données à caractère personnel
7. Communication
8. Droits de l’intéressé
9. Protection des données par projet et analyse d'impact relative à la protection des données
10. Contrats existants
11. Transfert de données à caractère personnel

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3. 1. Obligation de justification

- Savoir quelles données à caractère personnel l'on traite
- Sanctions
- Ce qu'il faut encore faire: plan de route
- Le responsable du traitement est responsable du respect des principes

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.2. Respect des principes du RGPD

- Légalité
- Limitation des finalités
- Minimisation des données
- Intégrité et confidentialité
- Transparence et information
- Proportionnalité
- Limitation de la conservation
- Obligation de justification
- Raison
- Exactitude

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.3. Délégué à la protection des données

= DPD

- Endosse la responsabilité du respect des mesures de protection des données, mais la responsabilité incombe au responsable pour le traitement
- Un médecin individuel doit-il désigner un DPD? Non, ce n'est pas nécessaire.
  - Par contre, c'est obligatoire en cas de traitement d'une quantité considérable de données de santé comme dans un hôpital ou à partir de 250 employés

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.4. Sensibilisation

- Sessions d’information (19/1 et 20/1)
- Informations pour les médecins
- Avis spécifiques

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.5. Registre des données

- Identifier minutieusement les données à caractère personnel que l'on détient, leur origine, et les personnes avec lesquelles elles sont partagées.

Registre des activités de traitement

- **Qui?**
  - Remplir le nom et les coordonnées du responsable du traitement (et éventuellement représentant légal) et du délégué à la protection des données si vous devez en désigner un.
  - Établir une liste des sous-traitants.
- **Quoi?**
  Identifier les catégories de données traitées et les catégories de personnes concernées. Identifier aussi les données dites sensibles comme les données de santé et les données judiciaires

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.5. Registre des données

- **Pourquoi**?
  Identifier les finalités pour lesquelles les données sont traitées. La description des finalités doit être aussi précise que possible.
- **Où?**
  - Mentionner les catégories de destinataires (aussi s'ils sont établis dans des pays tiers) auxquels les données sont transmises.
  - Mentionner les transferts à un pays tiers ou une organisation internationale et identifier le pays et, le cas échéant, les garanties appropriées existantes
- **Jusque quand?**
  Mentionner pour toute catégorie de données le délai de conservation.
- **Comment?**
  Donner une description générale des mesures techniques et organisationnelles de sécurisation intégrées qui garantissent un niveau de sécurité adapté aux risques

processus opérationnel/traitement	propriétaire du processus
dentification du processus opérationnel *nom, propriétaire du processus* *'dans la colonne ci-dessous, on reprend le nom du traitement en fonction de la lisibilité de la version électronique du registre)*	identifiez le ou les propriétaires (fonction) du processus opérationnel dont relève le traitement

description fonctionnelle du traitement	finalité du traitement
identification et information au sujet du traitement *numéro, , description fonctionnelle, , finalité, fondement du traitement, type de traitement et description fonctionnelle*	mentionnez la finalité du traitement l'onglet "listes" reprend une liste indicative avec quelques finalités standard (liste indicative de types de finalités). Attention : cette liste ne couvre cependant pas toutes les situations. L'Autorité de protection des données peut par exemple estimer que pour un traitement déterminé, des informations plus précises sont requises.

données utilisées et personnes concernées	**catégorie de données fonctionnelle**	**catégorie(s) de personnes concernées**	**catégorie de personnes concernées vulnérables***	**délai de conservation**	**couplage de données**	**source authentique**
détails sur les données traitées et sur les personnes concernées dont les données sont traitées *catégorie fonctionnelle, catégorie sensible de traitement de données, catégorie de personne concernée, niveau de classification, délai de conservation, source authentique*	mentionnez la ou les catégories de données fonctionnelles l'onglet "listes" reprend une liste indicative avec quelques finalités standard (liste indicative de types de finalités) Attention : cette liste ne couvre cependant pas toutes les situations. L'Autorité de protection des données peut par exemple estimer que pour un traitement déterminé, des informations plus précises sont requises.	mentionnez la ou les catégories de personnes concernées	indiquez si les personnes concernées font partie d'une catégorie fragile oui --> s'il s'agit de personnes concernées qui se trouvent dans une situation où il y a un déséquilibre dans la relation entre la position d'une personne concernée et un responsable du traitement, comme par exemple des enfants, des travailleurs, des patients, ... non --> s'il ne s'agit pas d'une catégorie de personnes concernées telle que mentionnée ci-dessus	indiquez le délai de conservation des données traitées	indiquez si des données provenant d'ensembles de données différents sont couplées.	mentionnez la source de données si celle-ci n'est pas la personne concernée elle-même.

sous-traitant	n° du contrat de traitement de données
identification du sous-traitant (externe à l'organisation) impliqué dans le traitement *nom, n° du contrat de traitement de données*	complétez le numéro/titre du ou des contrats de traitement de données.

échange de données	catégorie(s) de destinataires	pays tiers/organisation internationale	nature de la transmission vers un pays tiers/u	documents garanties appropriées
informations au sujet d'un éventuel échange de données avec des tierces parties. catégorie(s) de données, *catégorie(s) de destinataires, pays tiers/organisation internationale, documents garanties appropriées*	le cas échéant, indiquez quelle est ou quelles sont la ou les catégories de destinataires. l'onglet 'listes' reprend une liste indicative ('catégorie(s) de destinataires') de quelques finalités standard. Attention : cette liste ne couvre cependant pas toutes les situations. L'Autorité de protection des données peut par exemple estimer que pour un traitement déterminé, des informations plus précises sont requises.	le cas échéant, mentionnez les pays tiers/les organisations internationales concerné(e)s par le transfert de données à caractère personnel. définition de "pays tiers" : tous les pays en dehors de l'Union européenne (UE) et de l'Espace Économique Européen (EEE) définition d'une "organisation internationale" une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.	le cas échéant, mentionnez la nature du transfert vers les pays tiers/les organisations internationales. L'onglet 'listes' reprend un aperçu des différentes possibilités.	s'il y a un transfert de données à caractère personnel vers un pays tiers/une organisation internationale + un transfert sur la base de la condition de l'article 49.2 du RGPD, mentionnez les documents qui précisent les garanties appropriées prises ainsi que l'endroit où on peut les trouver.

technologie	description
description de la technologie, des applications et du logiciel employés pour le traitement.	mentionnez la manière dont ce traitement est effectué. quelle technologie (par exemple basée sur le cloud, block chain, ...), application ou logiciel sont utilisés à cet effet ?

risque & mesures de sécurité	risque	description des mesures de sécurité	documentation
informations quant au risque et mesures de sécurité du traitement de données *risque, description des mesures de sécurité, documentation des mesures de sécurité, AIPD (DPIA)*	indiquez le risque inhérent pour les droits et libertés fondamentaux des personnes concernées.	indiquez en des termes généraux les mesures de sécurité techniques et organisationnelles prises spécifiquement pour le traitement. les mesures de sécurité techniques et organisationnelles au niveau business ne doivent en soi pas être mentionnées. Mentionnez alors "mesures standard"	renvoi vers les documents reprenant la description la description des "mesures standard" et les mesures de sécurité prises spécifiquement pour le traitement.

droits des personnes concernées	information des personnes concernées	procédure d'exercice des droits	remarque
renvoi vers les documents qui déterminent les procédures de respect des droits des personnes concernées.	indiquez la manière dont les personnes concernées sont informées de l'enregistrement de leurs données.	indiquez le document qui décrit cette procédure. indiquez le cas échéant quelles sont les mesures particulières pour l'exercice des droits des personnes concernées dans le cadre de du présent traitement.	indiquez d'éventuel[le]s remarques/points d'attention concernant l'activité de traitement.

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.6. Base légale

- Accord de l'intéressé: p. ex. lettre d'information
- Convention: p. ex. personnel, patient
- Obligation légale: p. ex. transfert des données pour remboursement, dossiers disciplinaires
- Intérêt vital de la personne concernée ou d'une autre personne: p. ex. urgences
- Mission d'intérêt public ou tâche dans le cadre de l'exercice de l'autorité publique qui est confiée au responsable du traitement: p. ex. stage information au SPF
- Intérêt légitime du responsable du traitement: p. ex. questionnaire de qualité, e-mail pour déménagement, etc.

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.6. Traitement des catégories particulières de données à caractère personnel: données de santé art. 9 RGPD

- En principe, interdit sauf si:
  - Consentement donné
  - Nécessaire pour le droit du travail ainsi que le droit à la protection sociale et à la sécurité sociale
  - Intérêts vitaux de la personne concernée
  - Données à caractère personnel rendues publiques par la personne concernée
  - Nécessaire pour l'institution, exercice ou fondement d'une action en justice ou lorsque les tribunaux agissent dans le cadre de leur compétence de droit
  - Nécessaire pour un intérêt public important

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.6. Traitement des catégories particulières de données à caractère personnel: données de santé art. 9 RGPD

- Nécessaire aux fins de la médecine préventive ou du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la dispense de soins de santé ou de services sociaux ou traitements, ou de la gestion des systèmes et des services de soins de santé ou de systèmes et services sociaux, sur la base du droit de l'UE ou du droit national, ou en vertu d'un contrat conclu en tant que professionnel de la santé
- Nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, comme la protection contre des dangers transfrontaliers graves pour la santé ou la garantie de normes élevées concernant la qualité et la sécurité des soins de santé et des médicaments ou des ressources médicales, sur la base du droit de l'UE ou du droit national qui reprennent des mesures adaptées et spécifiques en vue de la protection des droits et libertés de l'intéressé, notamment le secret professionnel
- Archivage dans l'intérêt général, recherches scientifiques ou historiques, ou à des fins statistiques

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.6. Traitement des catégories particulières de données à caractère personnel: données de santé art. 9 RGPD

- Traitement par ou sous la responsabilité d'un professionnel de la santé soumis à une obligation de **secret professionnel** conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou par une autre personne également soumise à une **obligation de secret** conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents

Registre!

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.7. Communication

- **Déclaration vie privée et disclaimers**
- Des modifications sont-elles nécessaires aux déclarations en matière de vie privée existantes?
- Fournir certaines informations à la personne concernée:
  - L'identité du sous-traitant et façon dont celui-ci utilisera les données
  - La base légale pour le traitement des données
  - Les délais pendant lesquels l'on conservera les informations
  - L'échange éventuel de données hors de l'Union européenne
  - La possibilité pour la personne concernée d'introduire une plainte auprès de l'APD si elle pense que ses données à caractère personnel ont mal été traitées

Bulletin du Conseil national (BCN)

Archive BCN

Ordre des médecins

Conseil national
Place de Jamblinne de Meux 34-35
B-1030 BRUXELLES
Tel.: 02.743.04.00
Fax: 02 735 35 63

Contact

ORDRE DES MEDECINS
HAINAUT

Accueil
Contact
Conseils
Plan
Ordre national
Documents

Bienvenue sur le site de l'Ordre des Médecins du Haina

info.hainaut@ordomedic.be

Médecins en difficulté
Cliquez sur l'image pour la télécharger

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.8. Droits de la personne concernée

- Information et accès aux données à caractère personnel
- Rectification et suppression des données
- Objection à l'encontre de pratiques de marketing direct
- Objection à l'encontre de prises de décision automatisées et de profilage
- Portabilité des données

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.9. Protection des données par projet et analyse d'impact relative à la protection des données

- Privacy by design et Privacy impact assessment (PIA) = lié aux autres processus organisationnels comme la gestion des risques et la gestion de projet
- Quand est-ce nécessaire? Situations à haut risque, p. ex. quand une nouvelle technologie est mise en place ou une opération de profilage peut entraîner des effets considérables pour les personnes concernées
- En cas de « risque élevé », il faut solliciter l'avis de l'APD concernant la conformité aux lois du traitement à la lumière du RGPD

Registre: Back-up

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.10. Fuites de données

- Procédures adéquates pour détecter, rapporter et examiner les fuites de données personnelles
- L'obligation de signalement :
  - Toutes les fuites de données ne doivent pas être signalées à l'APD – uniquement celles pour lesquelles il apparaît que la personne concernée peut souffrir d'une quelconque forme de dommages, p. ex. à la suite d'un vol d'identité ou la violation de l'obligation de réserve
  - Le non-respect de l'obligation de mention peut donner lieu à une amende, en plus de celle pour la fuite de données

Notifier à: privacy@ordomedic.be

Registre: 'incidents'

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.11. Contrats existants

- Contrats existants avec les sous-traitants: p. ex. Etac, Isabel, BOB, SD Worx,…
  - Importance des mesures de sécurité adaptables aux banques de données

3. QUELLES SONT LES OBLIGATIONS DU RGPD?

3.12. Transfert de données à caractère personnel

- P. ex. : étudiants qui font des examens dans une pratique, collaboration entre pratiques, envoi des résultats au patient, pratiques de marketing, etc.
  - Existe-t-il une base légale pour les transférer (loi, contrat, etc.)?
  - Faut-il conclure un contrat de traitement?
  - L'envoi des données de santé doit se faire de façon sécurisée, un e-mail n'est donc pas une bonne option!

CONCLUSION

ORDRE DES MEDECINS
CONSEIL NATIONAL

ORDE DER ARTSEN
NATIONALE RAAD

CONCLUSION

Que devons-nous faire maintenant?

- Tout le monde doit créer un registre des activités de traitement
  - Respecter les principes et en informer les collaborateurs
  - Vérifier les contrats?
  - Questions?