service public fédéral
SANTE PUBLIQUE,
SECURITE DE LA CHAINE ALIMENTAIRE
ET ENVIRONNEMENT

Direction générale Soins de santé
Service Soins aigus et chroniques

AUX GESTIONNAIRES D'HÔPITAUX

NOS RÉF. NNA_ GDPR_20170502

DATE 5 MAI 2017

CONTACT ehealthcare@health.belgium.be

OBJET : Exécution du General Data Protection Regulation (GDPR)

Madame, Monsieur,

Le Règlement général européen sur la protection des données *("European General Data Protection Regulation"*, en abrégé "GDPR") est entré en vigueur le 24 mai 2016. Une période de transition de deux ans a été prévue, en vertu de laquelle les organisations ont le temps jusqu'au 25 mai 2018 pour se conformer aux nouvelles exigences du règlement GDPR. Contrairement à une directive, aucune transposition dans la législation belge n'est requise.

Le Règlement introduit de nouvelles règles en matière de gestion et de protection des données à caractère personnel. Sans entrer dans des détails exhaustifs, il en résulte de manière générale que le "responsable du traitement" est responsable de la conformité aux principes du GDPR et qu'il doit également être en mesure de démontrer cette conformité. Cette obligation de justification s'accompagne d'une nouvelle approche fondée sur le risque. Le responsable du traitement doit prendre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au Règlement. À cet égard, il doit tenir compte "de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie *("privacy by design")*". Il est donc préférable d'évaluer dès maintenant les situations où il sera nécessaire de réaliser ce genre d'analyses de risques.

Le responsable du traitement doit prendre les mesures de politique interne nécessaires et mettre en œuvre certains concepts dans le fonctionnement de l'hôpital, comme par exemple le *"privacy impact assessment"*. Le nouveau système prévoit en effet en principe une évaluation préalable de l'impact sur la protection des données pour certains traitements considérés comme plus délicats et met l'accent sur les mesures pouvant être prises pour diminuer ces risques.

Le GDPR crée également un nouveau système pour la notification d'infractions. Il faut dès lors mettre en place des procédures adéquates pour détecter, rapporter et investiguer les fuites de données à caractère personnel.

Le GDPR renforce enfin considérablement la position du délégué la protection des données, qui doit être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel. Cette fonction peut être exercée par le conseiller en sécurité que vous avez désigné.

Afin de vous informer correctement sur le GDPR, la plate-forme eHealth a rassemblé à travers la page web ci-dessous les informations correctes à ce sujet. Cette page renvoie à diverses sources authentiques, parmi lesquelles un plan par étapes pour la mise en œuvre du GDPR, préparé par la Commission de protection de la vie privée.

https://www.ehealth.fgov.be/fr/services-de-base/general-data-protection-regulation

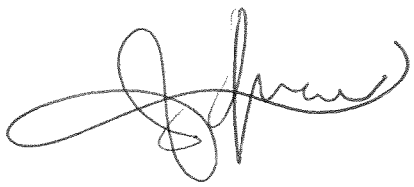
Cette page sera actualisée chaque fois que cela s'avérera nécessaire et, le cas échéant, vous serez informé(e) des évolutions nouvelles via le bulletin d'information de la plate-forme eHealth.

Il est extrêmement important de prendre dès maintenant des mesures préparatoires pour assurer le passage harmonieux à la nouvelle réglementation.

Pour le 25 mai 2018, chaque établissement doit avoir mis au point les procédures et canaux de communication qui démontrent la conformité au nouveau Règlement : Comment sont traitées des données personnelles, en fonction du type d'information en cause (données sur les patients, les employés, les visiteurs et d'autres tiers), ou des traitements et transferts d'informations vers des tiers par patient ou résident) ?

Il est important d'identifier les différents traitements, ainsi que les risques de sécurité possibles. Chaque institution doit prendre des mesures techniques appropriées pour garantir la vie privée des personnes au regard de la sensibilité des données qu'elle traite. Si un appel est fait à un processeur externe (sous-traitant), les droits et obligations devraient être inclus dans un accord écrit.

Veuillez agréer l'expression de mes salutations distinguées,



Pedro Facon
Directeur général
Direction générale Soins de Santé