« Privacy by Design » dans le développement d'un Dispositif Médical

Frederic Varnieu

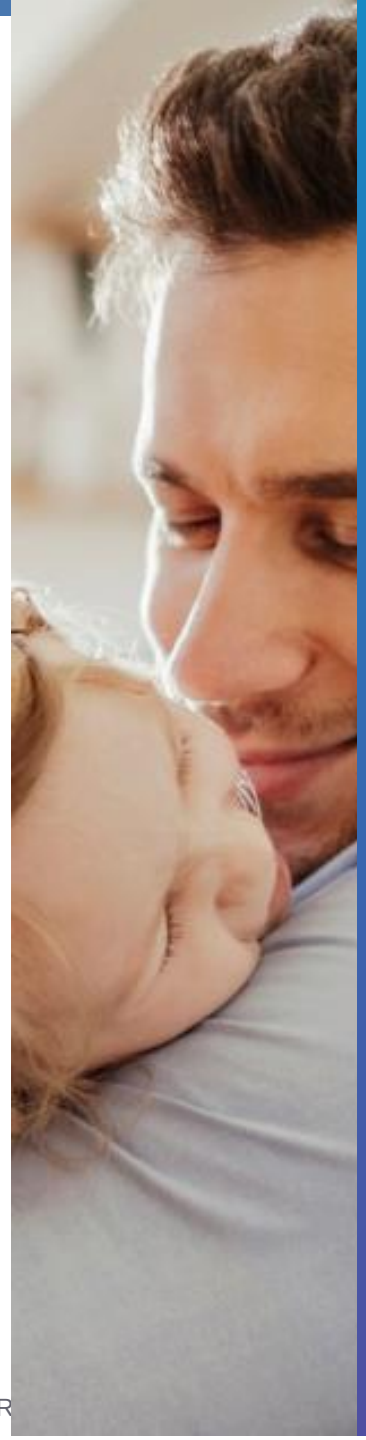
journée Cyber & santé : "cybersécurité des dispositifs médicaux et des objets connectés en Santé »

19 Novembre 2020

Sommaire

- Présentation
- Contexte réglementaire : RGPD
- « Privacy by Design & by default »
- Lignes directrices et outils

ResMed



>7,500 employés

Présent dans plus de 140 pays
Siège à San Diego, Californie, USA

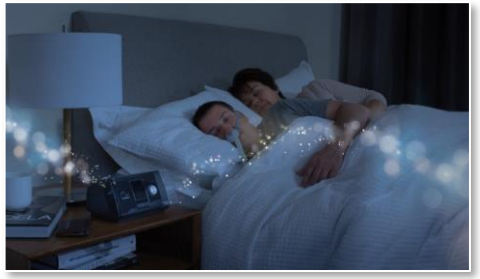
>30 ans d'expérience en médecine du sommeil

Leadership en innovation : +6000 brevets ou designs

ResMed (NYSE : RMD, ASX : RMD) développe des solutions innovantes pour soigner les patients en dehors de l'hôpital.

Nos **dispositifs médicaux connectés** au cloud transforment les soins des patients souffrant **d'apnée du sommeil,** ou **d'insuffisance respiratoire chronique** telle que la BPCO.

Solutions de santé connectée



Troubles Respiratoires du Sommeil

Insuffisance Respiratoire

ResMed

Présentation

Frederic Varnieu

Directeur Privacy Europe (ResMed)

ResMed

Contexte réglementaire : RGPD

ResMed

RGPD

Le sigle RGPD signifie « Règlement Général sur la Protection des Données ». Il encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Le règlement, s'il reste fidèle aux principes fondateurs de la protection des données en Europe, modifie profondément les obligations pesant sur les organismes, qui traitent des données.

Ce nouveau cadre repose sur une logique de **RESPONSABILISATION** des organismes qui traitent des données.

RGPD

Cette notion de responsabilisation (*accountability*) se traduit par l'affirmation de deux principes :

- Une adaptation profonde des outils, des méthodes et, au-delà, de la culture en matière de protection des données des entreprises. Il s'agit d'un **enjeu majeur en termes de confiance** des personnes et, par conséquent, de compétitivité pour les entreprises.
- La prise en compte de la protection des données **dès la conception** du service ou du produit et **par défaut** (*privacy by design and by default*) – *Article 25 RGPD*

ResMed

RGPD

RGPD Article 25.1 Protection des données dès la conception
Responsable de traitement doit mettre en œuvre des *mesures techniques et organisationnelles* durant la conception du traitement jusqu'au moment de la mise en œuvre de celui-ci en fonction des risques (probabilité et gravité)

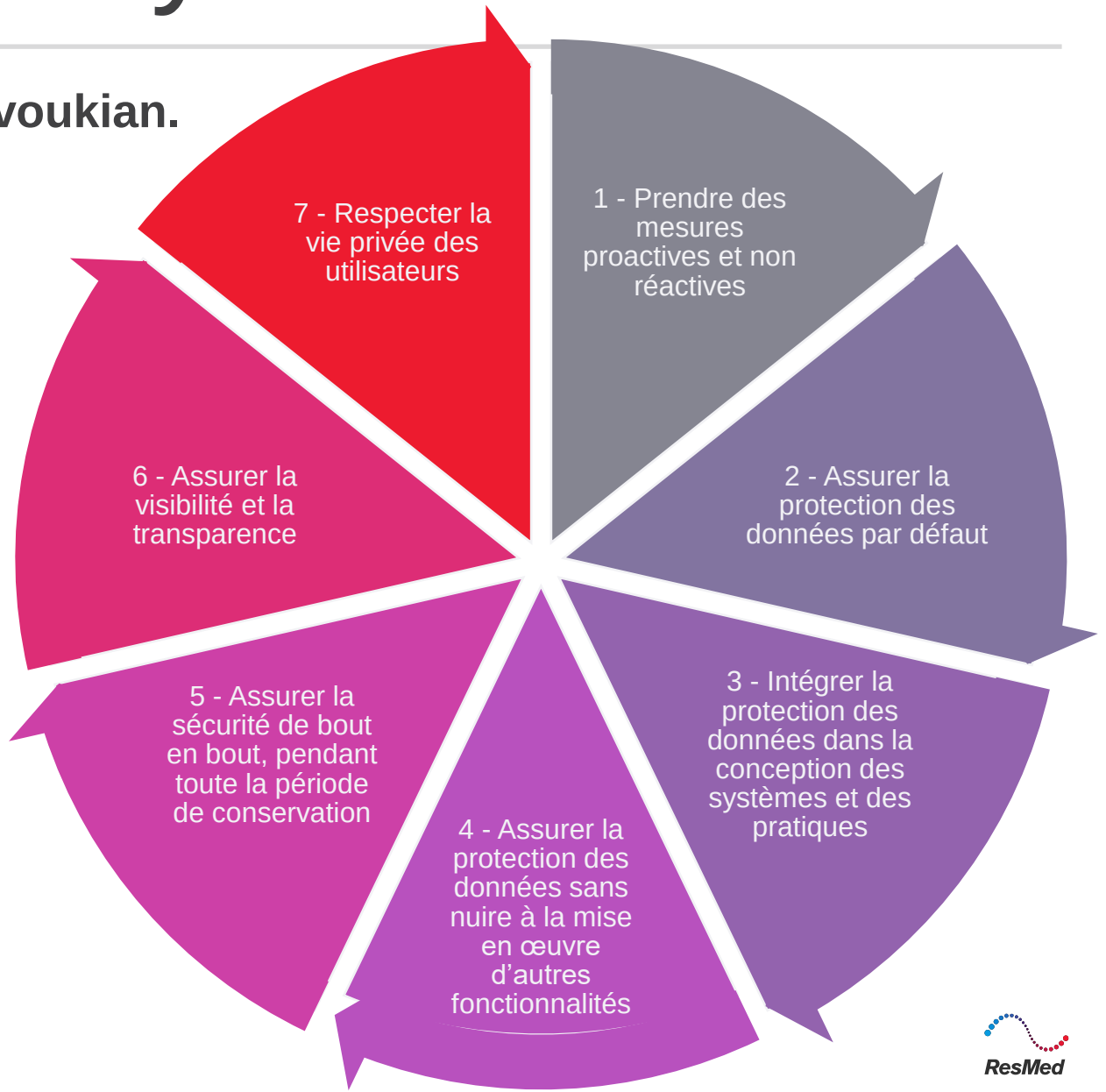
RGPD Article 25.2 Protection des données par défaut
Le responsable du traitement met en œuvre les *mesures techniques et organisationnelles* appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

Privacy by Design & by default

Privacy by Design & by default

Principes fondamentaux développés par Ann Cavoukian.

1. Prévoir, repérer et prévenir les incidents d'atteinte à la protection des données avant qu'ils ne se produisent; autrement dit, agir avant et non après de tels incidents. => Procédures sur la protection des données, Formation des utilisateurs, des chefs de projet et de produit
2. Faire en sorte que les données personnelles soient protégées de manière automatique avec un paramétrage par défaut. Si l'utilisateur ne fait rien, il est protégé.
3. Faire en sorte que les systèmes soient paramétrables par exemple en ayant un espace dédié aux utilisateurs pour qu'ils puissent eux-mêmes accéder ou modifier leurs données. Adapter les procédures existantes pour qu'elles incluent les bonnes pratiques de la protection des données.
4. Assurer une fonctionnalité complète, par exemple ne pas opposer la sécurité à la protection des données ou à la qualité.
5. Gérer le cycle de vie de la donnée, de la collecte à la destruction.
6. Dire ce que l'on fait, faire ce que l'on dit et être capable de le démontrer
7. Toujours prévaloir les intérêts de confidentialité de l'utilisateur final.



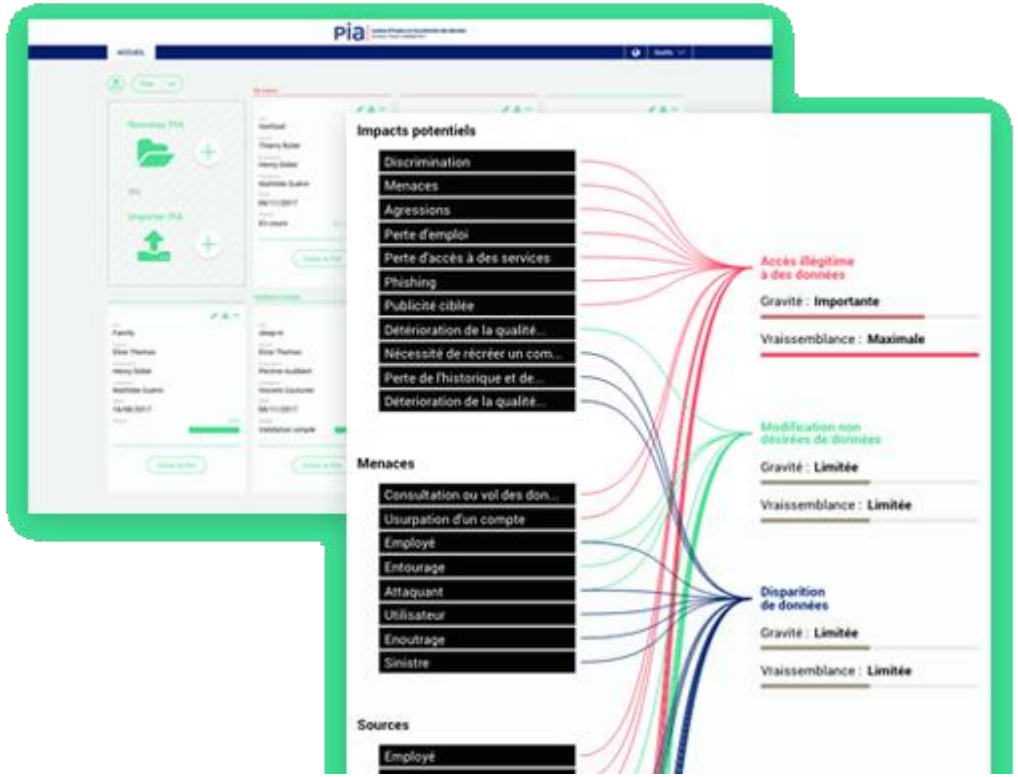
Lignes directrices et outils

ResMed

Lignes directrices et outils

- CNIL : Outil de Privacy Impact Assessment

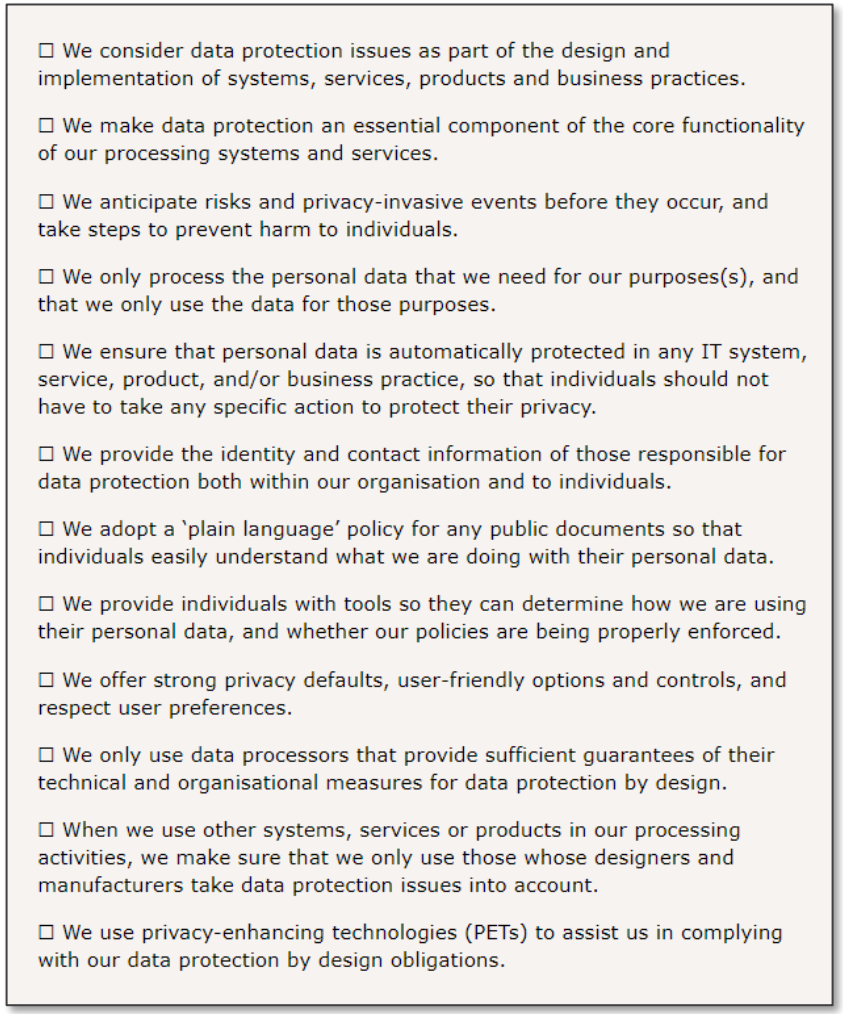
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil



Lignes directrices et outils

- ICO : Guide et Checklist

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/



☐ We consider data protection issues as part of the design and implementation of systems, services, products and business practices.

☐ We make data protection an essential component of the core functionality of our processing systems and services.

☐ We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.

☐ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.

☐ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.

☐ We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.

☐ We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.

☐ We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.

☐ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

☐ We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

☐ When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.

☐ We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

ResMed

Lignes directrices et outils

- European Data Protection Board (EDPB) : Lignes Directrices

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_fr

- AEPD : Guide Lignes Directrices sur le protection des données par défaut

https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

ResMed