IAE PARIS alumni

D.N.D Agency
Digital & Network Defense

APPLICATION PRATIQUE DE LA PROTECTION ET DE LA SÉCURITÉ DES DONNÉES DANS LE SECTEUR DE LA SILVER ECONOMIE

La Silver Economie

Ensemble des activités économiques, industrielles et de service à la personne qui bénéficient aux séniors et leur permettent d'améliorer leur qualité, voire leur espérance de vie et de faciliter les cas de maintien à domicile.

SCÉNARIO IN - IN

SCÉNARIO IN - OUT

SCÉNARIO IN – OUT - IN

Scenario IN ➡ IN

Données traitées dans l'espace privé, via des dispositifs restant **sous la maîtrise unique de la personne concernée**, de ses représentants légaux ou de ses proches n'intervenant pas à titre professionnel.

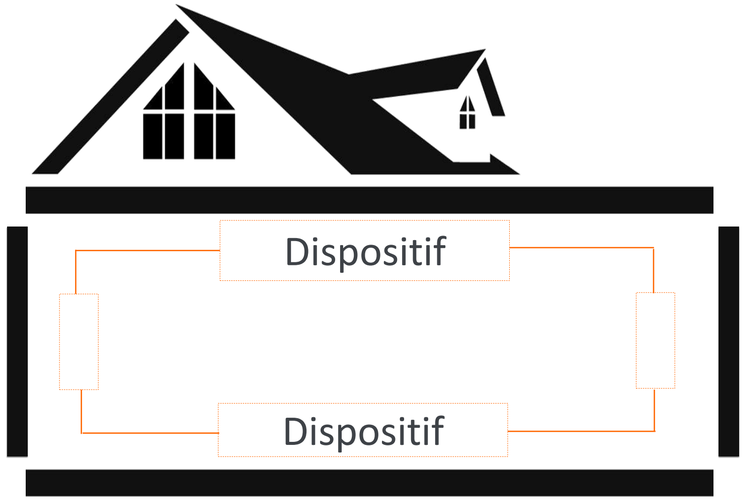
- Exemple type -

Concerne les cas où :

- Un ou plusieurs produits ou logiciels collectent des données et communiquent éventuellement entre eux **sans que les données sortent de l'espace privé** ;
- Les données sortent de l'espace privé **sans être transmises, collectées ni réutilisées par d'autres tiers** que les représentants légaux ou les proches de la personne concernée.

Précision - Dans ce cas d'espèce, les données :

- **Restent confinées** sur des réseaux de communication locaux sécurisés sous la maîtrise unique de l'utilisateur.
- **Circulent sur des réseaux de télécommunications** sans être stockées.



Points de considération principaux du RGPD dans la Silver Economie

- Scénario IN & IN -

Consentement

Ne doit pas être subordonné à la souscription d'un autre produit ou service. Les modalités de recueil du consentement doivent prendre en compte :

- **L'Etat des personnes** concernées ;
- La **sensibilité des données** collectées ;
- Le **contexte de mise en œuvre** du traitement et d'**utilisation** du service ;

Hébergement

L'hébergement des données se trouvant au domicile même de la personne:

- **Pas de réglementation particulière** dans le cas d'un scénario IN & IN.
- Exception « **Domestique** ».

Durée de conservation

A définir dès la conception des dispositifs, pour chaque finalité.

Les fournisseurs doivent permettre aux personnes concernées de :

- **Définir et de modifier** elles-mêmes, à tout moment, la durée de conservation des données ;
- **D'accéder et d'effacer** aisément les données enregistrées.

Mesures de sécurité

Adaptées au niveau de sensibilité des données
& aux capacités de contrôle des appareils

Chiffrement

Un chiffrement des échanges de données entre les différents appareils avec des algorithmes à l'état de l'art.

Protection

Mise en place des mesures de protection des clés de chiffrement permettant d'en garantir la confidentialité ;

Authentification des dispositifs

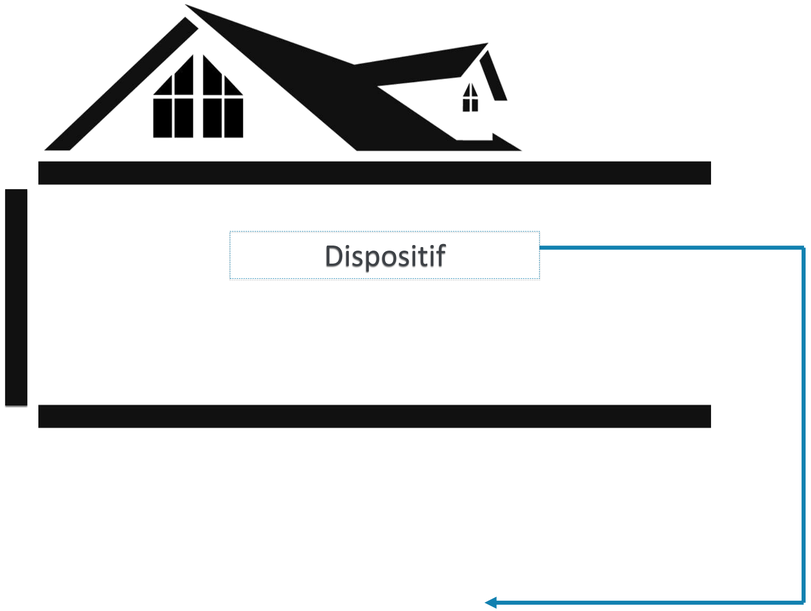
Mécanismes d'authentification des appareils entre eux (reconnaissance IP ou MAC), pour transmission d'ordre entre les dispositifs eux-mêmes.

Authentification personnelle

Mécanismes d'authentification de la personne préalablement à l'accès à des données personnelles, ou à la transmission d'ordres au dispositif lui-même.

Concerne les cas où les données :

- Sortent de l’espace privé pour être transmises à des tiers autres que les représentants légaux ;
- Sont traitées par des tiers pour permettre une intervention auprès de la personne concernée ;
- Sont traitées par des tiers pour proposer un service n’impliquant pas un pilotage à distance.



Scénario
IN ➡ OUT

Données traitées dans l’espace Privé et **transmises à l’extérieur**.

- Exemple type -

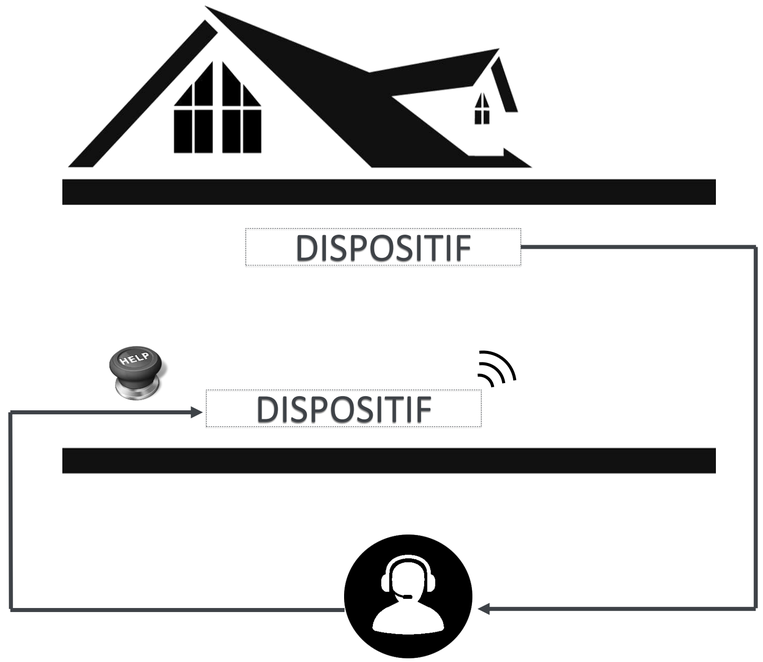
Scénario
IN ➡ OUT ➡ IN

Les données sont traitées dans l’espace privé et transmises à l’extérieur Pour permettre en retour une action Automatique sur les équipements situe dans l’espace prive.

- Exemple type -

Concerne les cas où les données :

- Sortent de l’espace privé pour être transmises à des tiers autres que les représentants légaux ;
- Sont traitées par des tiers pour permettre une intervention auprès de la personne concernée ;
- Sont traitées par des tiers pour proposer un service impliquant un pilotage à distance ou une interaction avec un équipement situé dans l’espace privé.



Points de considération principaux du RGPD dans la Silver Economie

- Scénario IN & OUT -
- Scénario IN & OUT & IN -

Consentement

Ne doit pas être subordonné à la souscription d'un autre produit ou service. Les modalités de recueil du consentement doivent prendre en compte :

- **L'Etat des personnes** concernées ;
- La **sensibilité des données** collectées ;
- Le **contexte de mise en œuvre** du traitement et d'**utilisation** du service ;

Collecte & traitement des données

Le principe de minimisation s'applique:

- **Seules les données strictement nécessaires** à la réalisation de l'objectif poursuivi peuvent être collectées ;
- Dans le cas d'un contrat de prestation de service, seules les données indispensables à la fourniture du service en question peuvent être traitées ;
- Une collecte « à la carte » en cas de traitements multiples ;

Sous-traitant

Si le responsable des traitements confie l'hébergement des données à un prestataire tiers:

- **Certification ou agrément nécessaire**
  - Selon les conditions prévues par l'article L. 1111-8 du code de la santé publique - modifié par l'ordonnance n° 2017-27 du 12 janvier 2017

Points de considération principaux du RGPD dans la Silver Economie

- Scénario IN & OUT -
- Scénario IN & OUT & IN -

Dispositif, Sous-traitant & Responsabilité

En fonction de la situation la responsabilité d'un sous-traitant peut changer :

- Lorsqu'un particulier recourt directement à une société pour être équipé, et si celle-ci traite ses informations pour son propre compte, ladite société devient responsable du traitement.
- Si un établissement propose un dispositif traitant des données et recourt à une société tiers pour équiper les résidents pour son compte, l'établissement est responsable du traitement. Et ladite société reste sous-traitante.

Durée de conservation

A définir dès la conception des dispositifs, pour chaque finalité.

Les fournisseurs doivent permettre aux personnes concernées de :

- **Définir et de modifier** elles-mêmes, à tout moment, la durée de conservation des données ;
- **D'accéder et d'effacer** aisément les données enregistrées.

Mesures de sécurité

Adaptées au niveau de sensibilité des données
& aux capacités de contrôle et d'action des appareils

Chiffrement

Chiffrement des données en base ou dans les dispositifs.

Transfert des données à l'extérieur via VPN et chiffrement 256 bit.

Hébergement

Hébergement des données chez un prestataire tiers certifié ou agréé à cet effet.
Hébergement en local sécurisé tant au niveau hardware que software.

Pseudonymisation & Anonymisation

Mécanismes d'authentification des appareils entre eux (reconnaissance IP ou MAC), pour transmission d'ordre entre les dispositifs eux-mêmes.

Opérations de hachage des données associées à des clés secrètes qui seront ensuite supprimées.

Authentification & Sûreté

Mise en place de mécanismes d'authentification des dispositifs entre eux, et d'authentification de la personne préalablement à l'accès aux données personnelles, ou à la transmission d'ordres au dispositif lui-même;

Permettre à la personne de couper le pilotage distant depuis l'intérieur du logement ;

Mesures de sécurité

Adaptées au niveau de sensibilité des données
& aux capacités de contrôle et d'action des appareils

Sécuriser l'environnement local

Mise en place de matériel informatique afin de sécuriser l'écosystème:

- Serveur en RAID 5
- Back Up sauvegarde en cas de mauvaise manipulation
- Onduleur
- Connexion de secours
- …

Synchronisation en externe

Une seconde sauvegarde des données doit être effectuée en externe:

- Hébergeur Certifié HAS cas échéant
- Canal SSL crypté (256 bit min).
- Synchronisation planifiée

Authentification

Authentification des accès aux données locales pour les personnes habilitées:

- Processus d'authentification du personnel
- Plateforme sécurisée
- Envoi crypté & limité

Formation

Information et sensibilisation :

- Formation régulière du personnel utilisateur
- Veille constante
- Communication en interne

RGPD & Sécurité de la donnée vont de pair

La plupart des dispositifs de la Silver Economie sont des Objets Connectés

Le développement se fait de manière rapide sans prendre en compte certains principes:

- **Sécurisation des données sortantes**;
- **Sécurisation des données entrantes** ;
- Type de données traitées ;

En raison d'une **méconnaissance de la sécurité** informatique d'un point de vue technique ;

Or tous les dispositifs médicaux et IoT impliquent la conformité & la sécurité :

Performance & sécurité sont imposées par les règlements :

- 2017 - 745 (applicable aux dm) ;
- 2017 - 746 (applicable aux dm in-vitro)

A prendre en compte donc dès la conception de chacun des nouveaux dispositifs et dès leurs lancement sur le marché.


IAE
PARIS
alumni


D.N.D Agency
Digital & Network Defense