PACK DE CONFORMITÉ

SILVER ÉCONOMIE ET DONNÉES PERSONNELLES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

SILVER ÉCONOMIE ET DONNÉES PERSONNELLES

SOMMAIRE

INTRODUCTION 02

- Périmètre du « pack » 02
- La loi « Informatique et Libertés » et le règlement général sur la protection des données sont-ils applicables à ces trois scénarios ? 04
- Les obligations en termes de sécurité sont-elles les mêmes pour les trois scénarios ? 05
- Définition des notions et des principes clés à respecter au regard de la loi « Informatique et Libertés » et du règlement général sur la protection des données 06

SCÉNARIO 1 IN → IN

LES DONNÉES SONT 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 11

- Périmètre 11
- Exemples de finalités : 11

SCÉNARIO 2 IN → OUT

LES DONNÉES SONT TRAITÉES DANS L'ESPACE PRIVÉ ET TRANSMISES À L'EXTÉRIEUR 15

- Périmètre 15
- Exemples de finalités : 15

SCÉNARIO 3 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 SITUÉS DANS L'ESPACE PRIVÉ 24

- Périmètre 24
- Exemples de finalités 24

SILVER ÉCONOMIE ET DONNÉES PERSONNELLES

1. PÉRIMÈTRE DU « PACK »

Dans le cadre d'un partenariat entre la CNIL et la Fédération des Industries Électriques, Électroniques et de Communication (FIEEC), un groupe de travail a été créé pour identifier les principes devant encadrer la collecte et le traitement de données personnelles par les produits et services de la « silver économie ».

La FIEEC regroupe 22 syndicats professionnels dans les secteurs de l'industrie électrique, électronique, numérique et des biens de consommation durables. Ces syndicats réunissent plus de 3 000 entreprises, emploient 400 000 salariés et réalisent 100 milliards d'euros de chiffre d'affaires dont 46 % à l'export.

La FIEEC a pour missions de promouvoir les électro-industries auprès des décideurs économiques, politiques et institutionnels ainsi qu'auprès des acteurs de la société civile, de proposer des réformes, anticiper et participer aux évolutions réglementaires, accompagner les entreprises et clarifier l'application des règles techniques.

Elle accompagne les entreprises dans le développement de leur activité en les sensibilisant sur la règlementation existante et à venir et promeut les bonnes pratiques mises en place par ces dernières.

La « silver économie » est une filière qui regroupe l'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.

Les travaux menés dans ce domaine portent, plus précisément, sur le traitement des données collectées et traitées via des produits et applications destinés à :

- apporter plus de confort et de sécurité aux seniors « actifs » et/ou « fragilisés » et/ou « dépendants » en raison de leur âge, de leur état de santé ou d'un handicap en vue de prévenir leur perte d'autonomie ou de les accompagner dans l'entrée en dépendance ;
- intervenir auprès de la personne concernée en cas de besoin.

L'objectif du groupe de travail est d'aboutir à la publication d'un référentiel sectoriel (ou « pack » de conformité) qui a pour objet d'accompagner l'innovation des industriels en intégrant la protection des données personnelles le plus en amont possible de la conception des produits et services et d'assurer la transparence et la maîtrise par les personnes concernées de leurs données, tout en prenant en compte les réalités du secteur.

Ce « pack » de conformité a vocation à être porté au niveau européen pour permettre aux acteurs de se positionner sur un marché européen voire mondial. C'est en ce sens, qu'il pourrait constituer une ligne directrice européenne en application du règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE (ci-après « RGPD »).

La Commission précise sur ce point que ces lignes directrices sont représentatives de la compréhension, à un moment donné, de technologies et d'usages devant faire l'objet d'un bilan régulier. Elle souhaite donc souligner le caractère évolutif du présent « pack ».

Trois scénarios ont été identifiés à partir de produits et services de la « silver économie » proposés par les professionnels du secteur ou en cours de développement et d'un examen de leurs conditions de mise en œuvre.

Ces hypothèses de travail ont permis d'identifier, pour chaque scénario, le cadre et les conditions dans lesquelles les traitements peuvent être mis en œuvre, à l'appui d'exemples de finalités, de catégories de données traitées, de durées de conservation adéquates, de destinataires, de modalités d'information et d'exercice des droits des personnes et de mesures de sécurité adaptées aux risques.

SCÉNARIO 1 « IN → IN » :

les données sont traitées dans l'espace privé, via des dispositifs restant sous la maîtrise unique de la personne concernée et pour son usage personnel.

Dans ce cas d'usage :

- un ou plusieurs produits ou logiciels collectent des données au sein de l'espace privé et peuvent communiquer entre eux sans que les données n'en sortent ;
- les caractéristiques des produits ou logiciels peuvent impliquer que les données sortent de l'espace privé sans qu'elles ne soient transmises, collectées ni réutilisées par d'autres tiers que les représentants légaux ou les proches de la personne concernée.

FOCUS

L'espace privé correspond notamment au domicile de la personne concernée ou à tout autre logement dans lequel elle réside, par exemple, une chambre dans un établissement d'hébergement ou de soin.

SCÉNARIO 2 : « IN → OUT » :

les données sont traitées dans l'espace privé et transmises à l'extérieur.

Dans ce cas d'usage les données :

- sortent de l'espace privé pour être transmises à des tiers autres que les représentants légaux ou les proches de la personne concernée (fournisseur de service, établissement d'hébergement ou de soin, personnel médical, intervenants professionnels (services d'urgence ou de soins à domicile, etc.), sous-traitant, prestataire, partenaire commercial, etc.) ;
- sont traitées par des tiers pour permettre une intervention auprès de la personne concernée ou lui proposer un service n'impliquant pas un pilotage à distance ou une interaction avec des équipements présents dans l'espace privé.

SCÉNARIO 3 : « 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 situés dans l'espace privé.

Dans ce cas d'usage les données :

- sortent de l'espace privé pour être transmises à des tiers autres que les représentants légaux ou les proches de la personne concernée (fournisseur de service, établissement d'hébergement ou de soin, personnel médical, intervenants professionnels (services d'urgence, ou de soins à domicile, etc.), sous-traitant, prestataire, partenaire commercial, etc.) ;

- sont traitées par des tiers pour permettre une intervention auprès de la personne concernée ou lui proposer un service impliquant un pilotage à distance ou une interaction avec un équipement situé dans l'espace privé.

FOCUS

La Commission souligne que selon les fonctionnalités des dispositifs en question, leurs conditions de mise en œuvre et l'utilisation qui en est faite, ces derniers peuvent relever d'un ou plusieurs de ces scénarios, auquel cas les préconisations des différents scénarios concernés trouveraient à s'appliquer.

Elle précise que la présente fiche introductive expose les principes relatifs à la protection des données personnelles découlant de la loi « Informatique et Libertés », d'une part, et les nouveautés découlant du RGPD devant être prises en compte dès la conception des produits ou services, d'autre part.

2. LA LOI « INFORMATIQUE ET LIBERTÉS » ET LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES SONT-ILS APPLICABLES À CES TROIS SCÉNARIOS ?

La loi « Informatique et Libertés » du 6 janvier 1978 modifiée et le RGPD s'appliquent lorsqu'il est procédé à un traitement de données personnelles.

Constitue un **traitement de données personnelles** toute opération (collecte, enregistrement, conservation, modification, extraction, consultation, utilisation, communication, interconnexion, destruction, etc.) portant sur toute information permettant d'identifier directement ou indirectement une personne physique. L'ensemble des éléments permettant de relier les données à la personne doit être pris en compte pour déterminer si une personne est identifiée ou identifiable.

Les obligations découlant de ces textes sont applicables à l'ensemble des produits et services de la « silver économie » proposés par les responsables des traitements (fournisseurs, établissement d'hébergement ou de soin, etc.) et leurs sous-traitants (prestataire, partenaire commercial, etc.), dont le fonctionnement suppose le traitement de données personnelles.

Les fiches pratiques des scénarios 2 (« IN → OUT ») et 3 (« IN → OUT → IN ») présentent ces obligations (notamment : identification d'une base légale, recueil éventuel du consentement, minimisation des données, définition d'une durée de conservation limitée, information conforme et respect des droits des personnes, mesures de sécurité adaptées aux risques, réalisation des formalités préalables adéquates voire d'une étude d'impact sur la vie privée, etc.).

La loi « Informatique et Libertés » et le RGPD ne sont en revanche pas applicables aux particuliers qui installent de tels dispositifs au sein de leur espace privé pour un usage personnel, ni à leurs représentants légaux ou proches n'intervenant pas à titre professionnel, dans la mesure où ils bénéficient d'une exception « domestique ».

C'est pourquoi, la fiche pratique 1 (« IN → IN ») formule des recommandations visant à s'assurer que les traitements sont effectivement destinés à l'exercice d'activités exclusivement personnelles, c'est-à-dire réalisés à l'initiative et sous la maîtrise entière de la personne concernée ou avec l'aide ou l'assistance d'un représentant légal, d'un proche ou d'un aidant familial. Ces préconisations visent également à garantir que les personnes concernées aient une complète maîtrise sur l'utilisation faite de leurs données.

3. LES OBLIGATIONS EN TERMES DE SÉCURITÉ SONT-ELLES LES MÊMES POUR LES TROIS SCÉNARIOS ?

Les mesures à prendre pour assurer la sécurité et la confidentialité des données sont très variables, d'une part, en fonction des équipements/dispositifs concernés et, d'autre part, du niveau de sensibilité et du circuit des données traitées.

Les risques que fait peser un traitement de données personnelles sur les droits et libertés des personnes concernées doivent être évalués. Pour ce faire, doivent notamment être identifiés :

- les sources de risques et leurs capacités (par exemple, un pirate informatique) ;
- les supports des données personnelles (par exemple, une base de données) ;
- les événements redoutés et leurs impacts pour les personnes concernées (par exemple, l'accès illégitime aux données pour leur exploitation) ;
- les menaces et leurs probabilité de survenance (par exemple, l'interception des communications par une attaque de type man in the middle).

Les risques doivent être caractérisés au regard de leur gravité (l'importance et l'impact des événements redoutés pour les personnes) et de leur vraisemblance (la probabilité de voir une menace se réaliser).

L'identification des facteurs de risques permet de concevoir des mesures adaptées visant à assurer la sécurité et la confidentialité des données. Il peut, par exemple, s'agir de mesures techniques (authentification, chiffrement, cloisonnement, sécurisation des équipements, etc.) ou de mesures organisationnelles (gestion des habilitations, encadrement de la maintenance, etc.).

Ce qui change avec le RGPD

Le RGPD prévoit que dans certains cas (en présence de risques élevés pour les personnes, appréciés sur la base de différents critères mentionnés à l'article 35 du RGPD), les responsables des traitements (fournisseurs de produits et services, etc.) ont l'obligation de formaliser l'analyse des risques et la définition des mesures correspondantes à travers une étude d'impact sur la vie privée (« EIVP » ou *privacy impact assessment* « PIA »).

La Commission recommande aux fournisseurs d'anticiper l'applicabilité du RGPD (à partir du 25 mai 2018) et de réaliser des EIVP dès la conception des produits et services. Elle met à disposition des professionnels des catalogues de bonnes pratiques destinées à les accompagner dans cette démarche (https://www.cnil.fr/fr/PIA-privacy-impact-assessment).

Les trois fiches pratiques du présent « pack » de conformité proposent des catalogues de risques et de mesures de sécurités adaptés aux spécificités de chaque scénario de traitement de données. Cette liste n'est pas exhaustive et est appelée à évoluer notamment en fonction des technologies utilisées.

4. DÉFINITION DES NOTIONS ET DES PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI « INFORMATIQUE ET LIBERTÉS » ET DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

PERSONNE CONCERNÉE :

toute personne physique à laquelle se rattachent directement ou indirectement les données qui sont collectées et traitées.

RESPONSABLE DE TRAITEMENT :

il s'agit, sauf désignation expresse par des dispositions législatives ou réglementaires, de la personne l'autorité publique, le service ou l'organisme qui détermine les finalités (ce à quoi sert le traitement) ou les moyens (permettant de répondre à cet objectif) d'un traitement de données personnelles.

Le responsable de traitement est tenu de respecter l'ensemble des obligations découlant de la loi « Informatique et Libertés » et du RGPD (notamment l'information et l'éventuel recueil du consentement de la personne concernée, la mise en place de mesures de sécurité adaptées et, le cas échéant, la réalisation des formalités préalables auprès de la CNIL).

Ce qui change avec le RGPD

Le RGPD prévoit que plusieurs organismes peuvent être conjointement identifiés comme responsables du traitement, lorsqu'ils déterminent ensemble les finalités et/ou les moyens d'un seul et même traitement.

Dans ce cas, ces derniers doivent définir leurs obligations respectives, s'agissant notamment des modalités d'information et d'exercice des droits des personnes (qui pourront les exercer auprès de chaque responsable).

SOUS-TRAITANT :

toute personne, organisme ou autorité à qui le responsable du traitement a confié la réalisation de tout ou partie du traitement. Il collecte et traite les données uniquement au nom et pour le compte du responsable du traitement et sur instruction de celui-ci.

***Par exemple**, lorsqu'un établissement d'hébergement ou de soin propose un dispositif permettant à ses résidents de générer une alerte en cas de chute et recourt à une société tierce pour équiper les résidents pour son compte, l'établissement est considéré comme responsable du traitement, tandis que la société tierce est considérée comme sous-traitant.*

En revanche, lorsqu'un particulier recourt directement à cette société pour être équipé, et si celle-ci traite ses informations pour son propre compte, c'est cette dernière qui doit être analysée comme responsable du traitement.

Avec la loi « Informatique et Libertés », seule pèse sur le sous-traitant l'obligation d'assurer la sécurité et la confidentialité des données collectées.

Ce qui change avec le RGPD

Le RGPD renforce les obligations du sous-traitant qui devra également :

- prêter concours au responsable du traitement dans le respect de ses obligations découlant du RGPD (notamment pour la gestion des droits des personnes) en déployant des mesures techniques et organisationnelles appropriées ;
- supprimer ou renvoyer les données qu'il détient au responsable du traitement au terme de la prestation de service ;
- mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de leurs obligations découlant du RGPD ;
- permettre la réalisation d'audits par le responsable du traitement ou un autre auditeur que celui-ci a mandaté ;
- informer immédiatement le responsable du traitement s'il estime qu'une instruction donnée par ce dernier constitue une violation du RGPD ou d'autres dispositions du droit de l'Union européenne ou du droit national relatives à la protection des données ;
- tenir à jour un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement.

DESTINATAIRES :

toutes personnes ou organismes habilités à recevoir communication de ces données autres que la personne concernée, le responsable du traitement, le sous-traitant, les personnes qui sont chargées de traiter les données dans le cadre de leurs fonctions et les autorités légalement habilitées.

DONNÉES DE SANTÉ :

outes informations relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette dernière.

Précision : La sensibilité de cette catégorie de données personnelles justifie que la loi « Informatique et Libertés » et le RGPD entourent leur utilisation de garanties particulières.

Un traitement portant sur de telles données n'est ainsi possible qu'à condition de s'appuyer sur une base légale spécifique (consentement, sauvegarde de la vie humaine, suivi médical, prévention, diagnostic, administration de soins ou de traitements ou gestion de services de santé mis en œuvre par des professionnels de santé, etc.).

Enfin, dans le cas où un responsable du traitement aurait recours à un tiers pour héberger pour son compte des données de santé recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, il doit s'assurer que ce dernier a été certifié ou agréé à cet effet, conformément aux dispositions de l'article L. 1111-8 du code de la santé publique modifié par l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement des données à caractère personnel.

Sur ce point, la Commission souligne que si un particulier recoure à un prestataire à cette fin, il devra s'assurer que celui-ci est certifié ou agréé afin de s'assurer que ses données sont hébergées dans des conditions de sécurité adaptées.

CONSENTEMENT :

toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données personnelles la concernant soient traitées.

Il s'agit de l'une des bases juridiques permettant au responsable du traitement de justifier la mise en œuvre d'un traitement de données personnelles (avec, par exemple, le respect d'une obligation légale, la sauvegarde de la vie de la personne concernée, l'exécution d'un contrat ou l'intérêt légitime du responsable de traitement).

Le consentement recueilli doit être spécifique, c'est-à-dire distingué clairement des autres questions posées à la personne concernée, et formulé en des termes clairs et simples afin qu'elle puisse s'engager en pleine connaissance de cause. De plus, il ne doit pas être subordonné à la souscription d'un autre produit ou service.

Précision : Les responsables des traitements doivent par ailleurs veiller à ce que les personnes concernées aient la capacité de consentir. En cas d'incapacité décidée par l'autorité judiciaire, le consentement de leurs représentants légaux pourra être recueilli (les proches dans le cadre d'une habilitation familiale ou les mandataires judiciaires à la protection des majeurs dans le cadre de leur fonction).

Il est donc nécessaire d'adapter les modalités de recueil du consentement en prenant en compte notamment l'état des personnes concernées, la sensibilité des données collectées et le contexte de mise en œuvre du traitement et d'utilisation du service (remplissage d'un formulaire ou d'une case à cocher non pré-cochée, etc.). En tout état de cause, la seule acceptation de conditions générales n'est pas une modalité suffisante.

Ce qui change avec le RGPD

La personne concernée doit pouvoir retirer son consentement aussi facilement qu'elle l'a donné. Ce retrait doit conduire à l'arrêt du traitement et à la suppression des données s'il s'agissait de la base légale sur laquelle il s'appuyait.

Enfin, le RGPD prévoit que le responsable de traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données personnelles la concernant, par tout moyen adapté (lorsqu'il s'agit de la base légale du traitement). La Commission recommande aux responsables des traitements d'anticiper cette nouvelle obligation.

Ce qui change avec le RGPD

Droit à la portabilité : le droit à la portabilité renforce la maîtrise des personnes concernées sur leurs données personnelles. Il crée également de nouvelles opportunités de développement et d'innovation en facilitant le partage de données personnelles, de manière sécurisée et sous le contrôle de la personne concernée.
Plus concrètement, le droit à la portabilité offre aux personnes concernées la possibilité de récupérer les données personnelles les concernant traitées par un organisme, dans un format structuré, couramment utilisé et lisible par machine, pour leur usage personnel afin, notamment, de les stocker sur un appareil ou un cloud privé.
Ce droit permet également aux personnes concernées de transmettre elles-mêmes leurs données d'un système d'information à un autre, **par exemple**, en vue de leur réutilisation par un autre responsable de traitement.
Lorsque cela est techniquement possible, les personnes concernées peuvent demander à ce que l'organisme qui détient les données les concernant transfère directement ces données à un autre responsable de traitement.
Le droit à la portabilité ne s'applique qu'aux données personnelles fournies activement et consciemment par la personne concernée au responsable de traitement (**par exemple**, une adresse électronique pour créer un compte en ligne via un formulaire dédié) et aux données générées par l'activité de cette dernière lorsqu'elle utilise un produit ou un service (**par exemple**, les données brutes générées par un pilulier connecté lors de la prise de médicaments).
À l'inverse, les données personnelles qui sont dérivées, calculées ou inférées à partir des données fournies par la personne concernée, telles que le profil d'un utilisateur créé grâce à l'analyse des données d'usage produites par dispositif sont exclues du droit à la portabilité, dans la mesure où elles ne sont pas fournies par la personne concernée, mais créées par l'organisme.
Par ailleurs, le droit à la portabilité ne s'applique que si les données sont traitées de manière automatisée (les fichiers papiers ne sont donc pas concernés).
Enfin, ce droit ne s'applique qu'aux traitements fondés sur le consentement ou nécessaires à l'exécution d'un contrat auquel elle est partie (**par exemple**, les données générées par un dispositif équipé de capteurs en cas de chute de la personne au sein du domicile, transmises à un service de téléassistance afin de permettre une intervention d'urgence, conformément au contrat de prestation de service).
Il en résulte que les données personnelles traitées sur la seule base de l'intérêt légitime du responsable de traitement ne peuvent faire l'objet d'une demande de portabilité (par exemple, les données traitées à des fins d'optimisation de modèles ou d'amélioration de produits ou logiciels).

Droit à la limitation du traitement : ce droit permet aux personnes concernées de limiter les opérations susceptibles d'affecter les données les concernant via leur cantonnement informatique temporaire. Ce cantonnement a pour but d'empêcher l'accès, la modification ou l'effacement des données sélectionnées, principalement, pendant l'examen d'une demande d'exercice d'un droit par la personne concernée ou à des fins probatoires (en particulier, en cas de contestation quant à la licéité d'un traitement, l'exactitude ou la nécessité des données ou la primauté des motifs légitimes du responsable de traitement sur ceux de la personne concernée).

Ainsi « gelées », les données personnelles ne peuvent (à l'exception de leur conservation), être traitées qu'avec le consentement de la personne concernée, pour la constatation, l'exercice ou la défense de droits en justice, pour la protection des droits d'une autre personne physique ou morale ou pour des motifs importants d'intérêt public.

ANONYMISATION :

opération irréversible conduisant à rompre tout lien d'identification entre les données et la personne concernée. Les mécanismes d'anonymisation doivent être conformes à l'avis du G29 du 10 avril 2014 sur les mécanismes d'anonymisation (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf).

Les données anonymes ne sont pas soumises à la loi informatique et libertés » ni au RGPD. Elles peuvent donc être librement utilisées et transmises et conservées sans limitation de durée.

Tel n'est en revanche pas le cas des données **pseudonymisées**, qui restent des données à caractère personnel. La pseudonymisation est une technique qui consiste à remplacer des données personnelles directement identifiantes par un pseudonyme non signifiant. Cela peut par exemple être réalisé par le calcul d'une empreinte obtenue par l'utilisation d'un algorithme de hachage à clé secrète. Le recours à la pseudonymisation des données permet d'améliorer la protection de la confidentialité des informations à caractère personnel en réduisant les risques de mésusage.

SCÉNARIO N°1
IN → IN

LES DONNÉES SONT 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

PÉRIMÈTRE

Ce scénario couvre les cas dans lesquels :

- 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. Dans ce cas d'usage, les données :
  - restent confinées sur des réseaux de communication locaux sécurisés sous la maîtrise unique de l'utilisateur (Wi-Fi, cloud privé ou autre réseau local) ;
  - circulent sur des réseaux de télécommunications ouverts au public (notamment ADSL, fibre optique, GSM, 4G, 3G, EDGE ou GPRS) sans être stockées sur un serveur centralisé ni réutilisées à d'autres fins que la gestion du trafic par les opérateurs de communication électronique .

Relèvent donc de ce scénario, les traitements de données personnelles mis en œuvre :

- à l'initiative et sous la maîtrise entière de la personne concernée ;
- à l'initiative et sous la maîtrise entière de la personne concernée ou avec l'aide ou l'assistance d'un particulier chargé de la représenter juridiquement dans le cadre d'une habilitation familiale (hypothèse des mandataires familiaux désignés par l'autorité judiciaire dans l'entourage d'une personne) ou d'une personne de son entourage n'intervenant pas dans le cadre d'une activité professionnelle ou commerciale (proches ou aidants familiaux).

FOCUS

En revanche, ce scénario exclut les traitements mis en œuvre par les professionnels intervenant en tant que représentants légaux des personnes concernées, tels que les mandataires judiciaires à la protection des majeurs dans le cadre de leur fonction.

EXEMPLES DE FINALITÉS :

- **1 Amélioration du confort :** la personne souhaite adapter ou équiper son logement afin d'améliorer son confort de vie et faciliter les cas de maintien à domicile. Elle utilise à cette fin un ou plusieurs dispositifs de « domotique » qui traitent des données relatives aux habitudes de vie ou au logement afin de répondre à ce besoin. Ces données ne sortent pas du logement.

Le fait que les données passent sur les réseaux gérés par des opérateurs de communications électroniques ne pose pas de difficultés dans la mesure où ces opérateurs ont des obligations renforcées quant à ce qu'ils peuvent faire avec ces données de trafic. Ceci n'est cependant valable que si l'opérateur en question agit bien en tant que fournisseur du service de communication électronique. À l'inverse, si l'opérateur souhaite fournir un autre service, les recommandations applicables sont celles des scénarios 2 (« IN → OUT ») ou 3 (« IN → OUT → IN »).

Exemple : *système de gestion des éclairages ou des volets roulants que l'utilisateur peut commander et piloter via un smartphone. Ce dispositif enregistre les heures de lever et de coucher paramétrées par les usagers pour permettre une action automatique sur ces équipements.*

- **2 Prévention et renforcement de la sécurité des personnes concernées et de l'espace privé :** la personne utilise des dispositifs émettant des signaux dans le logement pour informer ou alerter les occupants en cas de danger ou d'accident.

Exemple : *système permettant de détecter, au moyen de capteurs, la position des personnes qui se lèvent pendant la nuit afin d'éclairer les parcours potentiellement accidentogènes et leur permettre de se déplacer en toute sécurité. Le dispositif peut enregistrer les heures et la fréquence des levées pour anticiper les besoins de déplacements.*

Exemple : *dispositifs équipés de sondes et de thermostats permettant de détecter la présence de l'occupant et de l'alerter en cas de variation inhabituelle de la température du logement (canicule, grand froid). Le système régule automatiquement la température pour atteindre celle choisie par l'utilisateur. À cette fin, le dispositif peut notamment détecter la présence des usagers, les caractéristiques du logement (isolation thermique, etc.) et les conditions météorologiques extérieures.*

QUELLES OBLIGATIONS AU REGARD DE LA LOI « INFORMATIQUE ET LIBERTÉS » ET DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) ?

La loi « Informatique et Libertés » et le RGPD sont applicables à l'ensemble des produits et services proposés par les responsables des traitements (fournisseurs, établissement d'hébergement ou de soin, etc.) et leurs sous-traitants (prestataire, partenaire commercial, etc.), dont le fonctionnement suppose le traitement de données personnelles.

Ces textes ne sont en revanche pas applicables aux particuliers qui installent de tels dispositifs au sein de leur espace privé pour un usage personnel (exception « domestique ») ni à leurs représentants légaux ou proches n'intervenant pas à titre professionnel.

FOCUS

Les recommandations suivantes visent ainsi à fixer le cadre et les conditions dans lesquelles les dispositifs relevant du scénario « IN → IN » peuvent bénéficier de l'exception « domestique ».

Pour chacune de ces finalités, la personne concernée pourra toutefois bénéficier de services complémentaires nécessitant que les données sortent de l'espace privé afin d'être traitées par des tiers autres que ses représentants légaux ou ses proches n'intervenant pas à titre professionnel.

Selon les fonctionnalités des dispositifs en question et leurs conditions de mise en œuvre, ces derniers pourraient ainsi relever d'un autre scénario (« IN → OUT » et/ou « IN → OUT → IN »).

Exemple : *l'utilisation d'un robot de « compagnie » par la personne concernée afin d'augmenter son autonomie pour les tâches quotidiennes dans l'espace privé ne nécessitant pas que des données soient traitées par un fournisseur de service s'inscrira dans le scénario »IN → IN ».*

En revanche, dans le cas où ce même robot proposerait des fonctionnalités complémentaires nécessitant que des données sortent de l'espace privé et soient transmises à un tiers, cette utilisation s'inscrirait dans le scénario « IN → OUT », voire « IN → OUT → IN » (par exemple, identifier une situation critique telle qu'une chute et alerter des services d'urgence afin d'intervenir auprès de la personne concernée).

DONNÉES COLLECTÉES :

Seules les données strictement nécessaires à la réalisation de l'objectif poursuivi peuvent être collectées (principe de minimisation de la collecte).

DURÉES DE CONSERVATION :

Les données ne doivent être conservées dans les dispositifs que le temps nécessaire pour atteindre l'objectif poursuivi. La durée de conservation doit être définie dès la conception des dispositifs, pour chaque finalité.

FOCUS

Sous réserve des contraintes techniques propres aux dispositifs, la Commission recommande aux fournisseurs de dispositifs de permettre aux personnes concernées de définir et de modifier elles-mêmes, à tout moment, la durée de conservation des données. Cette capacité serait de nature à renforcer la maîtrise des usagers sur le fonctionnement des dispositifs en leur permettant de décider et de contrôler les usages faits des données les concernant.

Pour renforcer cette maîtrise, elle recommande en outre que les personnes concernées soient en mesure de désactiver à tout moment tout ou partie des fonctionnalités des dispositifs, d'une part, et en mesure d'accéder aux données traitées et d'effacer aisément les données enregistrées, d'autre part (notamment en cas de déménagement ou lorsqu'une opération de maintenance impliquant qu'un tiers accède aux données est nécessaire).

Cette suppression peut, **par exemple**, être réalisée au moyen :

- d'une interface d'administration prévue dans le dispositif lui-même (bouton d'arrêt, débranchement, etc.) ;
- ou via une application dédiée accessible depuis un smartphone ou tout autre terminal, facilement utilisable et compréhensible.

Précision : La Commission souligne la nécessité pour les fournisseurs de prévoir des solutions adaptées à l'état des personnes ciblées, dès la conception des dispositifs, afin que ces dernières puissent en avoir une maîtrise effective.

En tout état de cause, lorsqu'un responsable du traitement ou un sous-traitant récupère un dispositif qui n'a pas vocation à être réinstallé dans l'espace privé de la personne concernée, ces derniers doivent supprimer les données contenues dans ce dispositif (pour les produits reconditionnables ou loués), voire détruire le dispositif (pour les produits en fin de vie).

DESTINATAIRES :

Dans la mesure où, dans le présent scénario (« IN → IN »), il n'y a pas de communication de données hors de l'espace privé, seule la personne concernée, ses représentants légaux et ses proches n'intervenant pas à titre professionnel peuvent avoir accès aux données.

INFORMATION ET DROITS DES PERSONNES :

Précision : Afin que les personnes concernées, aient une parfaite connaissance des modalités de traitement de leurs données, la Commission recommande que ces dernières soient a minima informées de la présence des dispositifs (notamment au sein d'espace privés dans des établissements d'hébergement ou de soin), des modalités d'accès et de suppression des données et des moyens permettant à tout moment d'en désactiver aisément tout ou partie des fonctionnalités.

À cette fin, les fonctionnalités des systèmes doivent être explicitées par tout moyen adapté (notice remise lors de l'acquisition du dispositif, ou accessible directement depuis le dispositif, etc.).

FORMALITÉS PRÉALABLES :

Dans la mesure où les traitements sont mis en œuvre par les personnes concernées pour leur usage personnel, il n'y a pas de formalité préalable à effectuer auprès de la CNIL.

MESURES DE SÉCURITÉ :

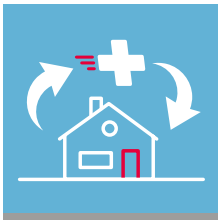
De façon générale, le fournisseur de dispositifs collectant et traitant des données personnelles doit mettre en place des mesures de sécurité afin de garantir la confidentialité, l'authenticité et l'intégrité des données traitées par les appareils qu'il fournit à la personne. Ces mesures doivent être adaptées au niveau de sensibilité des données et aux capacités de contrôle des appareils. Elles doivent no-

tamment inclure, lorsqu'elles sont pertinentes au regard de la nature des dispositifs considérés :

- un chiffrement des échanges de données entre les différents appareils avec des algorithmes à l'état de l'art ;
- des mesures de protection des clés de chiffrement permettant d'en garantir la confidentialité ;
- des mécanismes d'authentification des appareils entre eux ;
- des mécanismes d'authentification de la personne préalablement à l'accès à des données personnelles, le choix d'utiliser ce mécanisme pouvant être laissé aux usagers.

Le fournisseur de dispositif doit également prendre toutes les précautions utiles pour en empêcher la prise de contrôle par toute personne non autorisée, en proposant notamment :

- des mécanismes d'authentification de la personne préalablement à la transmission d'ordre aux dispositifs, le choix d'utiliser ce mécanisme pouvant être laissé à l'utilisateur;
- des mécanismes d'authentification des appareils préalablement à la transmission d'ordre aux dispositifs.



SCÉNARIO N°2
IN → OUT

LES DONNÉES SONT TRAITÉES DANS L'ESPACE PRIVÉ ET TRANSMISES À L'EXTÉRIEUR

PÉRIMÈTRE

Ce scénario couvre les cas dans lesquels les données :

- sortent de l'espace privé pour être transmises à des tiers autres que les représentants légaux ou les proches n'intervenant pas à titre professionnel de la personne concernée (fournisseurs de service, personnel d'un établissement d'hébergement ou de soin, personnel médical, intervenants professionnels (professionnels du service ou du soin intervenant à domicile, services d'urgence, etc.), sous-traitant, prestataires, partenaires commerciaux, etc.) ;
- sont traitées par des tiers pour permettre une intervention auprès de la personne concernée ou lui proposer un service n'impliquant pas un pilotage à distance ou une interaction avec des équipements présents dans l'espace privé.

EXEMPLES DE FINALITÉS :

- **1 Prévention et renforcement de la sécurité des personnes concernées et de l'espace privé :** dispositifs permettant de localiser la personne concernée afin d'informer et d'alerter des tiers et leur permettre d'intervenir en cas d'urgence.

Exemple : *données actimétriques (permettant d'enregistrer des mouvements et d'analyser l'activité d'une personne) et de localisation générées par un bracelet, pouvant être proposés par certains établissements d'hébergement ou de soin à des résidents présentant un risque de fugue ou d'errance.*

Ces dispositifs peuvent également être proposés à des personnes maintenues à domicile. Le système permet de générer une alerte lorsque le porteur sort du du périmètre défini et de transmettre sa position à des tiers afin de permettre une intervention rapide.

FOCUS

La Commission souligne que ces traitements ne doivent pas être mis en œuvre à des fins de suivi des déplacements des résidents au sein d'établissements d'hébergement ou de soin ou maintenus à domicile, mais uniquement afin de localiser ces derniers en cas d'urgence.

Exemple : *détecteur de chute ou de malaise équipé d'un service de téléassistance permettant au porteur de déclencher une alerte en cas de problème (en actionnant, par exemple, un bouton d'appel sur un médaillon).*

Les alertes peuvent également être automatiquement générées par le dispositif identifiant, par exemple, des cas de chute à l'aide de capteurs sans fil installés dans l'espace privé. Les alertes sont interceptées et traitées par le responsable du traitement ou un prestataire (centre d'appel, etc.).

Le système peut également permettre de dialoguer à distance avec la personne concernée afin de mesurer la gravité de la situation (« levée de doute »). En l'absence de réponse ou en cas de confirmation d'une urgence, les services d'intervention, les proches ou les voisins peuvent être alertés.

Exemple : *« tissu connecté », sous-matelas équipé d'une technologie permettant de détecter les levers de la personne concernée et de prévenir le personnel médical (en cas d'hébergement en établissement) ou les services d'urgence (en cas de maintien à domicile) en cas d'absence prolongée.*

Le délai de déclenchement de l'alerte à partir de la détection des levers est personnalisable. Le dispositif est couplé à un système de téléalarme permettant d'alerter les tiers préalablement déterminés.

- **2 Renforcement de la prévention dans le domaine de la santé** : dispositifs médicaux (au sens de la directive 93/42/CEE) visant à assurer le suivi de l'état de santé des personnes concernées et à identifier les cas d'urgence. La Commission rappelle que les dispositifs médicaux autres que les dispositifs médicaux de diagnostic in vitro seront soumis aux dispositions du règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux.

Exemple : *balance ou pilulier connectés couplés à un système de télésurveillance. Les dispositifs permettent un suivi médical via une plateforme externe dédiée (« télémédecine »). Ils peuvent fournir aux professionnels (médecin, aidant professionnel, etc.) et aux proches des alertes en cas de non-prise de médicament ou de situation à risque nécessitant une intervention (par exemple, un risque de dénutrition résultant d'une analyse de l'évolution du poids de la personne).*

- **3 Prospection commerciale :** le fournisseur de service ou un tiers (partenaire commercial, etc.) utilisent les données personnelles de la personne concernée pour procéder à des opérations de prospection commerciale.

La Commission souligne que le code de la santé publique prohibe la cession à titre onéreux de données de santé, y compris avec l'accord de la personne concernée. Ces données ne peuvent donc pas être transmises par le responsable du traitement à des tiers à des fins de prospection commerciale.

- **4 Optimisation de modèles, amélioration des produits ou logiciels, élaboration de statistiques (sur la base d'une analyse des données d'usage des dispositifs).**

BASE LÉGALE :

- **S'agissant des dispositifs installés au domicile des personnes concernées :**

Pour les finalités 1 et 2 (prévention et renforcement de la sécurité et de la santé des personnes concernées et de l'espace privé), la base légale peut-être l'exécution du contrat de prestation de service ou de fourniture du dispositif auquel la personne concernée est partie lorsque le fonctionnement du dispositif ou le service fourni impliquent le traitement des données par le responsable de traitement.

Exemple : *dans le cas de la souscription d'un service de téléassistance des personnes, les personnes concernées doivent porter un bracelet qui génère une alerte en cas de chute. Dans ce cas, la société devra nécessairement disposer de certaines informations afin d'intervenir auprès de la personne. La base légale de ce traitement sera donc l'exécution du contrat de service et sera matérialisée par la souscription du contrat.*

Pour ces finalités, la base légale peut également être le consentement libre et éclairé de la personne concernée ou de ses représentants légaux, lorsque le responsable de traitement propose un service complémentaire n'impliquant pas que des données soient traitées afin de permettre le fonctionnement des produits ou la fourniture des services.

Exemple : *l'analyse des données générées par un pilulier connecté initialement utilisé pour alerter la personne concernée lors de la prise de médicament, afin de proposer un service complémentaire tel que des recommandations pour un régime alimentaire adapté.*

Exemple : *la réalisation d'opérations de prospection commerciale ciblée.*

Ce qui change avec le RGPD

Le RGPD prévoit que dans les cas où la validité du traitement repose sur le consentement, le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement.

Afin d'anticiper l'applicabilité de cette obligation, la Commission recommande d'ores et déjà aux responsables des traitements de formaliser le recueil du consentement des personnes par tout moyen adapté (exemple : case à cocher non pré-cochée figurant sur un formulaire électronique dédié ; mise sous séquestre du code source d'un site web permettant de prouver en cas de contestation qu'une case dédiée au recueil du consentement a bien été cochée, etc.).

Précision : La liberté du consentement implique que la personne concernée puisse le retirer à tout moment. La Commission rappelle que le retrait du consentement doit conduire à l'arrêt du traitement. Le retrait du consentement donné pour des services complémentaires n'entraine toutefois pas de conséquence sur le fonctionnement des produits ou sur la continuité des services réalisés dans le cadre du traitement initial.

- **S'agissant des dispositifs installés au sein d'établissements d'hébergement ou de soin :**

Pour les finalités 1 et 2, la base légale peut-être l'exécution d'un contrat (contrat de séjour, par exemple), le respect d'une obligation légale (incombant à l'établissement), le consentement libre et éclairé de la personne concernée ou de ses représentants légaux, la sauvegarde de la vie de la personne concernée ou la réalisation de l'intérêt légitime du responsable du traitement.

Précision : S'agissant plus spécifiquement des dispositifs permettant de localiser les résidents, par exemple, pour gérer les risques d'errance ou de fugue, la Commission estime que le choix d'un établissement d'hébergement ou de soin de s'appuyer sur une base légale alternative au consentement pour équiper des résidents de tels dispositifs doit conduire à favoriser la solution la moins intrusive pour les personnes concernées (principe de proportionnalité).

À ce titre, les responsables des traitements qui envisageraient de s'appuyer sur l'intérêt légitime pour mettre en œuvre de tels traitements devront prendre en compte l'ensemble des circonstances d'espèce pour déterminer si cette base légale est adéquate.

Ces derniers devront ainsi s'assurer que les intérêts ou les libertés et droits fondamentaux des personnes concernées ne prévalent pas sur les intérêts légitimes qu'ils entendent poursuivent.

Par exemple, l'intérêt légitime des établissements d'hébergement ou de soin ne permet pas de justifier systématiquement la mise en place de dispositifs permettant de localiser les résidents en raison d'un manque de personnel.

Par ailleurs, la mise en œuvre de tels dispositifs doit être limitée à la surveillance de résidents effectivement sujets à des risques d'errance ou de fugue ou être justifiée par la proximité d'un danger. La pertinence de la mise en œuvre de tels dispositifs doit ainsi faire l'objet d'une analyse au cas par cas, évaluée par des personnes compétentes.

FOCUS

Enfin, la Commission recommande que toute action d'un résident en incapacité de manifester son consentement pouvant être interprétée comme une tentative ou une volonté de désactivation ou de retrait d'un dispositif (par exemple, des tentatives répétées ou systématiques visant à ôter un bracelet « anti-fugue ») doit conduire l'établissement d'hébergement ou de soin et, le cas échéant, les représentants légaux, à favoriser une solution plus appropriée.

- **S'agissant de la finalité 3 (prospection commerciale) :**

Selon les modalités de prospection, la personne concernée doit être clairement informée et consentir expressément à être démarchée par le responsable de traitement ou un tiers (cas de l'« opt-in » : prospection par automate d'appel, télécopie ou par envoi de SMS ou MMS) ou pouvoir s'y opposer, au moment de la collecte de ses données (cas de l'« opt-out » : prospection par voie postale ou nécessitant une intervention humaine par téléphone).

La personne concernée doit pouvoir manifester son choix de manière simple et dénuée d'ambiguïté (par exemple, via une case à cocher non pré-cochée ou, lorsque cela est techniquement possible, via un dispositif physique ou logique aisément compréhensible et accessible).

- **S'agissant du traitement des données de santé :**

La Commission rappelle que les données de santé sont considérées par la loi « informatique et libertés » comme des données sensibles, dont le traitement et la collecte sont par principe interdits. Des dérogations à ce principe existent néanmoins.

En premier lieu, le traitement de données de santé dans le cadre du présent scénario « IN → OUT » serait possible sous réserve que la personne concernée y ait spécifiquement consenti.

En second lieu, en cas d'incapacité juridique de la personne ou d'impossibilité matérielle d'obtenir son consentement, le traitement de ces données pourrait également être justifié par la sauvegarde de la vie humaine.

En troisième lieu, ces données pourraient être traitées dans le cadre d'un dispositif médical ou d'une plateforme de télémédecine si elles sont nécessaires aux fins de suivi médical des personnes, de prévention, de diagnostic, d'administration de soins ou de traitements ou de gestion de services de santé mis en œuvre par des professionnels de santé (finalité 2).

- **S'agissant de la finalité 4 (optimisation de modèles, amélioration des produits ou logiciels) :**

Si les données sont anonymisées (données ne permettant en aucun cas l'identification directe ou indirecte d'une personne physique, y compris par recoupement d'informations), il ne s'agit pas de données personnelles. Ces informations peuvent être librement utilisées : aucune base légale n'est donc nécessaire pour cet usage.

Si le responsable du traitement peut justifier d'un besoin de conserver des données identifiantes ou pseudonymisées pour un tel usage (c'est-à-dire rendant possible la ré-identification des personnes physiques), la base légale peut être l'intérêt légitime du responsable de traitement.

QUELLES OBLIGATIONS AU REGARD DE LA LOI « INFORMATIQUE ET LIBERTÉS » ET DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) ?

La mise en place d'un traitement de données personnelles doit respecter les principes de protection des données prévus par la loi « Informatique et Libertés » et le RGPD.

Les précisions suivantes visent ainsi à fixer le cadre et les conditions dans lesquelles les dispositifs relevant du scénario « IN → OUT » peuvent être mis en œuvre. La Commission recommande aux responsables des traitements (fournisseurs, établissement d'hébergement ou de soin, etc.) et à leurs sous-traitants (prestataire, partenaire commercial, etc.) de prendre en compte ces impératifs dès la conception des dispositifs et par défaut.

DONNÉES COLLECTÉES :

Seules les données strictement nécessaires à la réalisation de l'objectif poursuivi peuvent être collectées (principe de minimisation de la collecte).

Dans le cas d'un contrat de prestation de service, seules les données indispensables à la fourniture du service en question peuvent être traitées.

***Par exemple**, des données de localisation des personnes concernées, ne peuvent être remontées au personnel d'un établissement médicalisé ou d'un centre d'appel que suite à une demande d'intervention de la part de l'utilisateur ou en raison d'une situation d'urgence nécessitant de connaître sa position.*

Ce qui change avec le RGPD

Dans la perspective de l'applicabilité du RGPD, la Commission rappelle par ailleurs que les personnes concernées devront pouvoir modifier aisément les paramétrages des dispositifs, afin notamment d'activer ou désactiver certains services dont la base légale est le consentement (par exemple, en désactivant le service de géolocalisation si la personne ne souhaite pouvoir être localisée qu'en cas d'urgence en dehors de son espace privé).

Précision : De plus, la Commission rappelle que les produits offrant une pluralité de traitements ou reposant sur un traitement ayant des finalités multiples, devront permettre aux utilisateurs de consentir « à la carte » à tout ou partie des finalités distinctes, sans que ce choix ait des conséquences sur les autres finalités.

DURÉES DE CONSERVATION :

Les données ne doivent être conservées dans les dispositifs que le temps nécessaire pour atteindre l'objectif poursuivi. La durée de conservation doit être définie dès la conception des dispositifs, pour chaque finalité.

Une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de conserver les données et elles doivent donc être supprimées de manière sécurisée. Certaines données peuvent toutefois faire l'objet d'un archivage dans une base dédiée lorsqu'elles présentent encore un intérêt (faire valoir un droit en justice ou réaliser des statistiques, par exemple). Lorsqu'un texte prévoit une obligation d'archivage, le responsable du traitement doit veiller à archiver uniquement les données utiles au respect de l'obligation prévue.

FOCUS

Sous réserve des contraintes techniques propres aux dispositifs, la Commission recommande aux fournisseurs de dispositifs d'adopter une démarche de privacy by design en permettant aux personnes concernées de définir et de modifier elles-mêmes, à tout moment, la durée de conservation des données. Cette capacité serait de nature à renforcer la maîtrise des usagers sur le fonctionnement des dispositifs en leur permettant de décider et de contrôler les usages faits des données les concernant.

Pour renforcer cette maîtrise, la Commission recommande en outre que les personnes concernées soient en mesure de désactiver ou de demander au responsable de traitement de désactiver à tout moment tout ou partie des fonctionnalités des dispositifs, d'une part, et en mesure d'accéder aux données traitées et d'effacer aisément les données enregistrées, d'autre part (notamment en cas de déménagement ou lorsqu'une opération de maintenance impliquant qu'un tiers accède aux données est nécessaire).

Cette suppression peut, **par exemple**, être réalisée au moyen :

- d'une interface d'administration prévue dans le dispositif lui-même (bouton d'arrêt, débranchement, etc.) ;
- ou via une application dédiée accessible depuis un smartphone ou tout autre terminal, facilement accessible et compréhensible.

Précision : La Commission souligne la nécessité pour les fournisseurs de prévoir des solutions adaptées à l'état des personnes ciblées, dès la conception des dispositifs, afin que ces dernières puissent en avoir une maîtrise effective, par exemple, en permettant à des résidents au sein d'un établissement d'hébergement ou de soin d'être accompagnées par un auxiliaire de vie spécifiquement formé à ces usages.

En tout état de cause, lorsqu'un responsable du traitement ou un sous-traitant récupère un dispositif qui n'a pas vocation à être réutilisé par la personne concernée, ces derniers doivent supprimer les données contenues dans ce dispositif (pour les produits reconditionnables ou loués), voire détruire le dispositif (pour les produits en fin de vie).

EXEMPLES :

- **Pour les finalités 1 et 2 (prévention et renforcement de la sécurité et de la santé des personnes concernées et de l'espace privé) :**
  - les données liées à l'identification et à l'état de santé de la personne concernée et le cas échéant à l'espace privé (nombre et emplacement des capteurs sans fil, etc.) doivent être conservées le temps nécessaire à la fourniture du service ;
  - les données « commerciales » (identification, données relatives aux transactions et aux moyens de paiement) peuvent être conservées pendant toute la durée du contrat.

- **Pour la finalité 3 (prospection commerciale) :** les données des clients peuvent être conservées pendant un délai de trois ans à compter de la fin de la relation commerciale (par exemple, à compter d'un achat, de la date d'expiration d'une garantie, du terme d'un contrat de prestations de services ou du dernier contact émanant du client).

Les données personnelles relatives à un prospect non client peuvent être conservées pendant un délai de trois ans à compter de leur collecte par le responsable du traitement ou du dernier contact émanant du prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un courriel).

Au terme de ce délai de trois ans, le responsable du traitement pourra reprendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées ou archivées.

- **Pour la finalité 4 (optimisation de modèles, amélioration des produits ou logiciels) :** les données anonymisées peuvent être conservées pour une durée illimitée.

En revanche, les données identifiantes ou pseudonymisées ne doivent être conservées que le temps nécessaire à la réalisation des études ou recherches.

DESTINATAIRES :

Dans le cadre des finalités du présent scénario « IN → OUT », le responsable du traitement peut être amené à transmettre des données personnelles à des destinataires auquel il fait appel pour participer à l'exécution du service proposé.

La Commission précise qu'en tout état de cause, il revient au responsable du traitement, avant chaque transmission des données, d'opérer un tri parmi ces dernières pour s'assurer que les destinataires n'accèdent qu'aux seules données nécessaires à la réalisation de l'objectif poursuivi par cette transmission.

EXEMPLES :

- **Pour la finalité 1** (prévention et renforcement de la sécurité des personnes concernées et de l'espace privé), peut être destinataires des données le personnel d'un centre d'appel de téléassistance agissant pour le compte d'un établissement d'hébergement ou de soin proposant un bracelet « anti-chute » à ses résidents.

- **Pour la finalité 2** (renforcement de la prévention dans le domaine de la santé), les professionnels de santé peuvent échanger des informations relatives à un même patient, sauf opposition de sa part, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge. Lorsque la personne concernée est prise en charge par une équipe de soins dans un établissement de santé, les informations sont réputées confiées à l'ensemble de l'équipe médicale.

Par ailleurs, les professionnels participant à un acte de télémédecine peuvent, sauf opposition de la personne concernée, s'échanger des informations relatives à cette dernière, par tout moyen.

La Commission rappelle que dans le cas où l'hébergement de données de santé, recueillies ou produites à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social s'inscrivant dans le cadre du présent scénario « IN → OUT » est confié à un prestataire tiers, celui-ci doit être certifié ou agréé à cet effet, qu'il soit situé en France ou à l'étranger (dans 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 relative à l'hébergement des données à caractère personnel).

- **Pour la finalité 3** (prospection commerciale), des partenaires commerciaux du responsable du traitement peuvent être destinataires des données (adresse électroniques ou postales, numéros de téléphones, etc. à l'exclusion des données de santé) permettant de démarcher les personnes concernées pour leur propre compte (en tant que responsables des traitements).

La Commission rappelle sur ce point qu'avant toute transmission de données ou de campagne de prospection commerciale par téléphone, les professionnels doivent s'assurer que les numéros de téléphone concernés ne figurent pas dans la liste anti-démarchage téléphonique (BLOCTEL).

INFORMATION ET DROITS DES PERSONNES :

La personne concernée doit être informée, préalablement à la mise en œuvre du traitement, de l'identité du responsable du traitement, de la finalité du traitement, des destinataires des données, des modalités d'exercice de ses droits d'accès, de rectification et d'opposition, des éventuels transferts de données hors de l'Union européenne ainsi que des durées de conservation.

Précision : Par ailleurs, le RGPD renforce l'information des personnes concernées. La Commission recommande que les nouvelles mentions suivantes soient d'ores et déjà portées à leur connaissance, préalablement à la mise en œuvre d'un traitement :

- les coordonnées du responsable du traitement et du délégué à la protection des données ;
- la base légale du traitement ;
- l'identification des intérêts légitimes poursuivis par le responsable du traitement (lorsqu'ils constituent la base légale du traitement) ;
- les critères utilisés pour déterminer la durée de conservation des données (lorsque celle-ci ne peut pas être précisément déterminée) ;
- la mention des nouveaux droits des personnes (la possibilité de demander la limitation du traitement, le droit à la portabilité des données, le droit de retirer le consentement à tout moment lorsque le traitement est fondé sur cette modalité, le droit d'introduire une réclamation auprès d'une autorité de contrôle) ;
- le caractère réglementaire ou contractuel de l'exigence de fourniture des données, le caractère obligatoire de cette fourniture (si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir ces données), ainsi que les conséquences éventuelles de leur non-fourniture (impossibilité de fournir le service demandé, etc.) ;
- le cas échéant, l'existence d'une prise de décision automatisée (y compris un profilage) produisant des effets juridiques ou affectant de manière significative les personnes concernées et des informations concernant la logique sous-jacente à cette prise de décision, l'importance et les conséquences prévues du traitement pour les personnes ;
- en cas de traitement ultérieur pour une finalité autre que celle pour laquelle les données ont été initialement collectées, des informations sur cette autre finalité ;
- en cas de collecte indirecte, l'origine des données (y compris si celles-ci étaient publiquement accessibles).

Le RGPD prévoit que les personnes concernées doivent être informées en des termes clairs, simples et aisément accessibles. Cette information peut, par exemple, être effectuée lors de la signature du contrat de fourniture du dispositif ou de prestation de service par la personne concernée ou ses représentants légaux (via des clauses ou des documents spécifique).

FOCUS

La Commission estime utile d'accompagner cette information d'icônes normalisées (facilement visibles, compréhensibles et clairement lisibles), afin d'offrir une bonne vue d'ensemble du traitement.

De plus, afin que les personnes concernées, aient une parfaite connaissance des modalités de traitement de leurs données, la Commission recommande que ces dernières soient en outre informées des fonctionnalités des dispositifs (en particulier des modalités d'accès et de suppression des données et des moyens permettant à tout moment d'en désactiver tout ou partie des fonctionnalités). Cette information peut être fournie par tout moyen adapté (notice remise lors de l'acquisition du dispositif, ou accessible directement depuis le dispositif, etc.).

Les personnes concernées disposent des droits d'accès, de rectification et de suppression de l'ensemble des données traitées, ainsi que d'opposition pour des motifs légitimes.

Pour la finalité 3 (prospection commerciale), les personnes concernées doivent par ailleurs pouvoir s'opposer, sans frais, au traitement de leurs données par le responsable du traitement initial ou le responsable d'un traitement ultérieur.

FORMALITÉS PRÉALABLES :

Précision : Les formalités préalables devant être réalisées par les responsables des traitements dépendront de la finalité des traitements et de la nature des données collectées, quel que soit le dispositif utilisé.

Par exemple, si des données de santé sont traitées dans le cadre des finalités relevant du présent scénario (« IN → OUT »), et que celles-ci sont collectées avec le consentement des personnes concernées ou que leur traitement est nécessaire à des fins de diagnostic médical, les responsables des traitements doivent effectuer une déclaration normale sur le site web de la CNIL (www.cnil.fr).
Par ailleurs, dans certains cas, un engagement de conformité à l'autorisation unique n° AU-047, portant sur les traitements mis en œuvre dans le cadre de l'accueil, l'hébergement et le suivi des personnes handicapées et des personnes âgées pourra suffire. Cela sera notamment le cas lorsqu'un dispositif répond à l'une des finalités prévues dans cette autorisation unique et qu'il est mis en œuvre dans les conditions posées par cette norme.

FOCUS

La Commission souligne enfin que les traitements de données personnelles mis en œuvre dans le cadre du présent scénario « IN → OUT », pourront être concernés par l'obligation de réaliser une étude d'impact sur la vie privée (EIVP) prévue par le RGPD, s'ils sont susceptibles de créer des risques élevés pour la vie privée des personnes concernées. Ces risques doivent notamment être appréciés sur la base des critères suivants, fixés par le RGPD :

- existence d'une évaluation systématique et approfondie d'aspects personnels concernant les personnes physiques, fondée sur un traitement automatisé (y compris le profilage), et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative ;
- présence d'un traitement de données à large échelle (au regard du nombre de personnes concernées, du volume de données et de leur degré de sensibilité, de la durée du traitement et de son étendue géographique) ;
- présence de traitements à grande échelle portant sur des catégories « particulières » de données personnelles au sens de l'article 9 du RGPD (notamment des données de santé);
- vulnérabilité des personnes concernées (notamment en raison de leur âge, de leur état de santé ou d'un handicap) ;
- utilisation de nouvelles technologies ou de dispositifs « innovants » (par exemple, des objets connectés associés à des applications smartphone).

En pareille hypothèse, les fournisseurs de service devra mener une EIVP pour identifier les risques que le traitement est susceptible d'engendrer, de déterminer et de mettre en œuvre les mesures nécessaires à la protection de la vie privée des personnes.
La Commission recommande d'ores et déjà aux fournisseurs de réaliser des EIVP dès la conception des produits et services. Elle met à disposition des catalogues de bonnes pratiques destinées à accompagner les professionnels dans cette démarche (https://www.cnil.fr/fr/PIA-privacy-impact-assessment).

MESURES DE SÉCURITÉ :

De façon générale, le responsable du traitement doit mettre en place des mesures de sécurité tant techniques qu'organisationnelles afin de garantir la confidentialité, l'authenticité et l'intégrité des données traitées par les appareils qu'il fournit à la personne, et doit prendre toutes les précautions utiles pour en empêcher la prise de contrôle par toute personne non autorisée. Ces mesures doivent être adaptées au niveau de sensibilité des données et aux capacités de contrôle des appareils. Elles doivent notamment inclure, lorsqu'elles sont pertinentes au regard de la nature des dispositifs considérés :

- un chiffrement des échanges de données entre les différents appareils avec des algorithmes à l'état de l'art ;
- des mesures de protection des clés de chiffrement permettant d'en garantir la confidentialité ;
- des mécanismes d'authentification des appareils entre eux ;
- des mécanismes d'authentification de la personne préalablement à l'accès à des données personnelles.

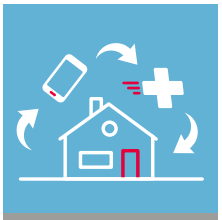
Le fournisseur de dispositifs doit également prendre toutes les précautions utiles pour en empêcher la prise de contrôle par toute personne non autorisée, en prévoyant notamment :

- des mécanismes d'authentification de la personne préalablement à la transmission d'ordre aux dispositifs ;
- des mécanismes d'authentification des appareils préalablement à la transmission d'ordre aux dispositifs.

Le traitement de données de santé peut nécessiter la mise en place de mesures de sécurité supplémentaires comme :

- la mise en œuvre de mesures de pseudonymisation (par exemple telles que le hachage avec clé secrète des données telles que le nom/prénom de la personne concernée) ;
- le chiffrement des données en base ou dans les dispositifs ;
- l'hébergement des données chez un prestataire tiers certifié ou agréé à cet effet.

Par ailleurs, l'utilisation de données personnelles pour la réalisation de statistiques doit faire l'objet de mécanismes d'anonymisation permettant de garantir que les données ne peuvent plus être reliées aux personnes concernées. Ces mécanismes peuvent par exemple d'appuyer sur des opérations de hachage des données associées à des clés secrètes qui seront ensuite supprimées. Dans tous les cas, les mécanismes d'anonymisation doivent être conformes à l'avis du G29 du 10 avril 2014 sur les mécanismes d'anonymisation.



SCÉNARIO N°3
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 SITUÉS DANS L'ESPACE PRIVÉ

PÉRIMÈTRE

Ce scénario couvre les cas dans lesquels les données :

- sortent de l'espace privé pour être transmises à des tiers autres que les représentants légaux ou les proches n'intervenant pas à titre professionnel de la personne concernée (fournisseurs de service, personnel d'un établissement d'hébergement ou de soin, personnel médical, intervenants professionnels (professionnels du service ou du soin intervenant à domicile, services d'urgence, etc.), sous-traitant, prestataires, partenaires commerciaux, etc.) ;
- sont traitées par des tiers pour permettre une intervention auprès de la personne concernée ou lui proposer un service impliquant un pilotage à distance ou une interaction avec un équipement situé dans l'espace privé.

EXEMPLES DE FINALITÉS :

- **1 Prévention et renforcement de la sécurité des personnes concernées et de l'espace privé :** service permettant à des tiers (fournisseur de service, prestataire, etc.) de déclencher une action automatique sur les équipements dans l'espace privé afin de permettre à des tiers d'intervenir auprès de la personne concernée.

Exemples : *ouverture à distance d'une porte pour permettre l'action des aidants ou des services d'intervention en cas d'urgence, coupure d'alimentation à distance en cas de départ de feu et alerte automatique des pompiers, etc.*

Exemple : *dispositifs équipés de sondes et de thermostats permettant de détecter la présence de l'occupant et d'alerter des tiers (fournisseur de service, prestataire, proches, etc.) en cas de variation inhabituelle de la température du logement (canicule, grand froid).*

Dans ce cas d'usage, les tiers ont la possibilité de commander et de piloter le système à distance pour réguler la température du logement. Ces derniers peuvent ainsi détecter la présence des usagers et connaître les caractéristiques du logement (isolation thermique, etc.).

- **2 Renforcement de la prévention dans le domaine de la santé :** dispositifs médicaux (au sens de la directive 93/42/CEE) visant à assurer le suivi de l'état de santé des personnes concernées et à identifier les cas d'urgence. La Commission rappelle que les dispositifs médicaux autres que les dispositifs médicaux de diagnostic in vitro seront soumis aux dispositions du règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux.

Exemple : *pilulier connecté couplé à un système de télésurveillance. Le dispositif permet un suivi médical via une plateforme externe dédiée (« télémédecine »). Les professionnels et les proches peuvent analyser les données relatives à la prise de médicament et piloter à distance le dispositif en modifiant l'horaire de déclenchement des alertes de prise de médicament.*

- **3 Prospection commerciale :** le fournisseur de service ou un tiers (partenaire commercial, etc.) utilisent les données personnelles de la personne concernée pour procéder à des opérations de prospection commerciale.

La Commission souligne que le code de la santé publique prohibe la cession à titre onéreux de données de santé, y compris avec l'accord de la personne concernée. Ces données ne peuvent donc pas être transmises par le responsable du traitement à des tiers à des fins de prospection commerciale.

- ***4* Amélioration de produits ou logiciels :** mise à jour à distance d'un logiciel embarqué dans un dispositif afin d'en améliorer les fonctionnalités suite à une analyse des données d'usage remontées au responsable de traitement.

BASE LÉGALE :

S'agissant des dispositifs installés au domicile des personnes concernées :

Pour les finalités 1 et 2 (prévention et renforcement de la sécurité et de la santé des personnes concernées et de l'espace privé), la base légale peut-être l'exécution du contrat de prestation de service ou de fourniture du dispositif auquel la personne concernée est partie lorsque le fonctionnement du dispositif ou le service fourni impliquent le traitement des données par le responsable de traitement.

Exemple : *dans le cas de la souscription d'un service d'assistance des personnes en cas d'urgence, les personnes concernées doivent permettre aux tiers d'agir à distance sur les équipements de l'espace privé. Dans ce cas, la société devra nécessairement disposer de certaines informations afin d'identifier les situations d'urgence et de permettre l'accès au logement par les services d'intervention. La base légale de ce traitement sera donc l'exécution du contrat de service et sera matérialisée par la souscription du contrat.*

Pour ces finalités, la base légale peut également être le consentement libre et éclairé de la personne concernée ou de ses représentants légaux, lorsque le responsable de traitement propose un service complémentaire n'impliquant pas que des données soient traitées afin de permettre le fonctionnement des produits ou la fourniture des services.

Exemple : *l'analyse des données générées par un pilulier connecté initialement utilisé pour alerter la personne concernée lors de la prise de médicament et en modifier au besoin l'horaire de déclenchement, afin de proposer un service complémentaire tel que des recommandations pour un régime alimentaire adapté.*

Exemple : *la réalisation d'opérations de prospection commerciale ciblée.*

Ce qui change avec le RGPD

Le RGPD prévoit que dans les cas où la validité du traitement repose sur le consentement, le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement.

Afin d'anticiper l'applicabilité de cette obligation, la Commission recommande d'ores et déjà aux responsables des traitements de formaliser le recueil du consentement des personnes par tout moyen adapté (exemple : case à cocher non pré-cochée figurant sur un formulaire électronique dédié ; mise sous séquestre du code source d'un site web permettant de prouver en cas de contestation qu'une case dédiée au recueil du consentement a bien été cochée, etc.).

Précision : La liberté du consentement implique que la personne concernée puisse le retirer à tout moment. La Commission rappelle que le retrait du consentement doit conduire à l'arrêt du traitement. Le retrait du consentement donné pour des services complémentaires n'entraine toutefois pas de conséquence sur le fonctionnement des produits ou sur la continuité des services réalisés dans le cadre du traitement initial.

- **S'agissant des dispositifs installés au sein d'espaces privés dans des établissements d'hébergement ou de soin :**

Pour les finalités 1 et 2, la base légale peut-être l'exécution d'un contrat (contrat de séjour, par exemple), le respect d'une obligation légale (incombant à l'établissement), le consentement libre et éclairé de la personne concernée ou de ses représentants légaux, la sauvegarde de la vie de la personne concernée ou la réalisation de l'intérêt légitime du responsable du traitement.

FOCUS

S'agissant plus spécifiquement des dispositifs permettant de localiser les résidents, par exemple, pour gérer les risques d'errance ou de fugue, la Commission estime que le choix d'un établissement d'hébergement ou de soin de s'appuyer sur une base légale alternative au consentement pour équiper des résidents de tels dispositifs doit conduire à favoriser la solution la moins intrusive pour les personnes concernées (principe de proportionnalité).

À ce titre, les responsables des traitements qui envisageraient de s'appuyer sur l'intérêt légitime pour mettre en œuvre de tels traitements devront prendre en compte l'ensemble des circonstances d'espèce pour déterminer si cette base légale est adéquate.

Ces derniers devront ainsi s'assurer que les intérêts ou les libertés et droits fondamentaux des personnes concernées ne prévalent pas sur les intérêts légitimes qu'ils entendent poursuivent.

Par exemple, l'intérêt légitime des établissements d'hébergement ou de soin ne permet pas de justifier systématiquement la mise en place de dispositifs permettant de localiser les résidents en raison d'un manque de personnel.

Par ailleurs, la mise en œuvre de tels dispositifs doit être limitée à la surveillance de résidents effectivement sujets à des risques d'errance ou de fugue ou être justifiée par la proximité d'un danger. La pertinence de la mise en œuvre de tels dispositifs doit ainsi faire l'objet d'une analyse au cas par cas, évaluée par des personnes compétentes.

Précision : Enfin, la Commission recommande que toute action d'un résident en incapacité de manifester son consentement pouvant être interprétée comme une tentative ou une volonté de désactivation ou de retrait d'un dispositif (par exemple, des tentatives répétées ou systématiques visant à ôter un bracelet « anti-fugue ») doit conduire l'établissement d'hébergement ou de soin et, le cas échéant, les représentants légaux, à favoriser une solution plus appropriée.

- **S'agissant de la finalité 3** (prospection commerciale) :

Selon les modalités de prospection, la personne concernée doit être clairement informée et consentir expressément à être démarchée par le responsable de traitement ou un tiers (cas de l'« opt-in » : prospection par automate d'appel, télécopie ou par envoi de SMS ou MMS) ou pouvoir s'y opposer, au moment de la collecte de ses données (cas de l'« opt-out » : prospection par voie postale ou nécessitant une intervention humaine par téléphone).

La personne concernée doit pouvoir manifester son choix de manière simple et dénuée d'ambiguïté (par exemple, via une case à cocher non pré-cochée ou, lorsque cela est techniquement possible, via un dispositif physique ou logique aisément compréhensible et accessible).

- **S'agissant du traitement des données de santé :**

La Commission rappelle que les données de santé sont considérées par la loi « informatique et libertés » comme des données sensibles, dont le traitement et la collecte sont par principe interdits. Des dérogations à ce principe existent néanmoins.

En premier lieu, le traitement de données de santé dans le cadre du présent scénario « IN → OUT → IN » serait possible sous réserve que la personne concernée y ait spécifiquement consentie.

En second lieu, en cas d'incapacité juridique de la personne ou d'impossibilité matérielle d'obtenir son consentement, le traitement de ces données pourrait également être justifié par la sauvegarde de la vie humaine.

En troisième lieu, ces données pourraient être traitées dans le cadre d'un dispositif médical ou d'une plateforme de télémédecine si elles sont nécessaires aux fins de suivi médical des personnes, de prévention, de diagnostic, d'administration de soins ou de traitements ou de gestion de services de santé mis en œuvre par des professionnels de santé (finalité 2).

- **S'agissant de la finalité 4** (amélioration des produits ou logiciels) :

Si les données sont anonymisées (données ne permettant en aucun cas l'identification directe ou indirecte d'une personne physique, y compris par recoupement d'informations), il ne s'agit pas de données personnelles. Ces informations peuvent être librement utilisées : aucune base légale n'est donc nécessaire pour cet usage.

Si le responsable du traitement peut justifier d'un besoin de conserver des données identifiantes ou pseudonymisées pour un tel usage (c'est-à-dire rendant possible la ré-identification des personnes physiques), la base légale peut être l'intérêt légitime du responsable de traitement.

QUELLES OBLIGATIONS AU REGARD DE LA LOI « INFORMATIQUE ET LIBERTÉS » ET DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) ?

La mise en place d'un traitement de données personnelles doit respecter les principes de protection des données prévus par la loi « Informatique et Libertés » et le RGPD.

Les précisions suivantes visent ainsi à fixer le cadre et les conditions dans lesquelles les dispositifs relevant du scénario « IN → OUT → IN » peuvent être mis en œuvre. La Commission recommande aux responsables des traitements (fournisseurs, établissement d'hébergement ou de soin, etc.) et à leurs sous-traitants (prestataire, partenaire commercial, etc.) de prendre en compte ces impératifs dès la conception des dispositifs et par défaut.

DONNÉES COLLECTÉES :

Seules les données strictement nécessaires à la réalisation de l'objectif poursuivi peuvent être collectées (principe de minimisation de la collecte).

Dans le cas d'un contrat de prestation de service, seules les données indispensables à la fourniture du service en question peuvent être traitées.

***Par exemple**, les données liées aux caractéristiques du logement (température, configuration, etc.) permettant de générer une notification d'alerte ou préventive (exemple : signal d'une fenêtre ouverte en cas de température basse ou d'un volet levé en cas de température élevée) ne peuvent être transmises à des tiers que dans des cas nécessitant une intervention à distance sur les équipements (exemple : ouverture des portes afin de faire intervenir les secours en cas de canicule et d'absence de réponse de la personne).*

Ce qui change avec le RGPD

Dans la perspective de l'applicabilité du RGPD, la Commission rappelle par ailleurs que les personnes concernées devront pouvoir modifier aisément les paramétrages des dispositifs, afin notamment d'activer ou désactiver certains services dont la base légale est le consentement (par exemple, en désactivant la possibilité pour les tiers de réguler à distance la température du logement, ces derniers ne pouvant dès lors qu'être alertés en cas de variation inhabituelle de la température ou, en désactivant l'autorisation d'accès à distance à certains paramètres ou réglages d'une installation domotique par un professionnel installateur, ce dernier ne recevant alors que des alertes de maintenance préventive).

De plus, la Commission rappelle que les produits offrant une pluralité de traitements ou reposant sur un traitement ayant des finalités multiples, devront permettre aux utilisateurs de consentir « à la carte » à tout ou partie des finalités distinctes, sans que ce choix ait des conséquences sur les autres finalités.

DURÉES DE CONSERVATION :

Les données ne doivent être conservées dans les dispositifs que le temps nécessaire pour atteindre l'objectif poursuivi. La durée de conservation doit être définie dès la conception des dispositifs, pour chaque finalité.

Une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de conserver les données et elles doivent donc être supprimées de manière sécurisée. Certaines données peuvent toutefois faire l'objet d'un archivage dans une base dédiée lorsqu'elles présentent encore un intérêt (faire valoir un droit en justice ou réaliser des statistiques, par exemple). Lorsqu'un texte prévoit une obligation d'archivage, le responsable du traitement doit veiller à archiver uniquement les données utiles au respect de l'obligation prévue.

FOCUS

Sous réserve des contraintes techniques propres aux dispositifs, la Commission recommande aux fournisseurs de dispositifs d'adopter une démarche de privacy by design en permettant aux personnes concernées de définir et de modifier elles-mêmes, à tout moment, la durée de conservation des données. Cette capacité serait de nature à renforcer la maîtrise des usagers sur le fonctionnement des dispositifs en leur permettant de décider et de contrôler les usages faits des données les concernant.

Pour renforcer cette maîtrise, la Commission recommande en outre que les personnes concernées soient en mesure de désactiver ou de demander au responsable de traitement de désactiver à tout moment tout ou partie des fonctionnalités des dispositifs, d'une part, et en mesure d'accéder aux données traitées et d'effacer aisément les données enregistrées, d'autre part (notamment en cas de déménagement ou lorsqu'une opération maintenance impliquant qu'un tiers accède aux données est nécessaire).

Cette suppression peut, **par exemple**, être réalisée au moyen :

- d'une interface d'administration prévue dans le dispositif lui-même (bouton d'arrêt, débranchement, etc.) ;
- ou via une application dédiée accessible depuis un smartphone ou tout autre terminal, facilement accessible et compréhensible.

> ***Précision :*** *La Commission souligne la nécessité pour les fournisseurs de prévoir des solutions adaptées à l'état des personnes ciblées, dès la conception des dispositifs, afin que ces dernières puissent en avoir une maîtrise effective, par exemple, en permettant à des résidents au sein d'un établissement d'hébergement ou de soin d'être accompagnées par un auxiliaire de vie spécifiquement formé à ces usages.*

FOCUS

La Commission souligne la nécessité pour les fournisseurs de prévoir des solutions adaptées à l'état des personnes ciblées, dès la conception des dispositifs, afin que ces dernières puissent en avoir une maîtrise effective, par exemple, en permettant à des résidents au sein d'un établissement d'hébergement ou de soin d'être accompagnées par un auxiliaire de vie spécifiquement formé à ces usages.

En tout état de cause, lorsqu'un responsable du traitement ou un sous-traitant récupère un dispositif qui n'a pas vocation à être réutilisé par la personne concernée, ces derniers doivent supprimer les données contenues dans ce dispositif (pour les produits reconditionnables ou loués), voire détruire le dispositif (pour les produits en fin de vie).

EXEMPLES :

- **Pour la finalité 1** (prévention et renforcement de la sécurité des personnes concernées et de l'espace privé) :
  - les données liées à l'identification et à l'état de santé de la personne concernée et le cas échéant à l'espace privé (nombre et emplacement des capteurs sans fil, etc.) doivent être conservées le temps nécessaire à la fourniture du service ;

- les données « commerciales » (identification, données relatives aux transactions et aux moyens de paiement) peuvent être conservées pendant toute la durée du contrat.

- **Pour la finalité 2** (renforcement de la prévention dans le domaine de la santé), les professionnels de santé peuvent échanger des informations relatives à un même patient, sauf opposition de sa part, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge. Lorsque la personne concernée est prise en charge par une équipe de soins dans un établissement de santé, les informations sont réputées confiées à l'ensemble de l'équipe médicale.

Par ailleurs, les professionnels participant à un acte de télémédecine peuvent, sauf opposition de la personne concernée, s'échanger des informations relatives à cette dernière, par tout moyen.

- **Pour la finalité 3** (prospection commerciale) : les données des clients peuvent être conservées pendant un délai de trois ans à compter de la fin de la relation commerciale (par exemple, à compter d'un achat, de la date d'expiration d'une garantie, du terme d'un contrat de prestations de services ou du dernier contact émanant du client).

Les données personnelles relatives à un prospect non client peuvent être conservées pendant un délai de trois ans à compter de leur collecte par le responsable du traitement ou du dernier contact émanant du prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un courriel).

Au terme de ce délai de trois ans, le responsable du traitement pourra reprendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées ou archivées.

DESTINATAIRES :

Dans le cadre des finalités du présent scénario « IN → OUT → IN », le responsable du traitement peut être amené à transmettre des données personnelles traitées par des dispositifs situés dans l'espace privé à des destinataires afin qu'ils interagissent avec ces équipements et puissent intervenir auprès de la personne concernée au besoin.

La Commission précise qu'en tout état de cause, il revient au responsable du traitement, avant chaque transmission des données, d'opérer un tri parmi ces dernières pour s'assurer que les destinataires n'accèdent qu'aux seules données nécessaires à la réalisation de l'objectif poursuivi par cette transmission.

EXEMPLES :

Pour la finalité 1 (prévention et renforcement de la sécurité des personnes concernées et de l'espace privé), peut être destinataires des données le personnel d'un centre d'appel de téléassistance agissant pour le compte d'un fournisseur de thermostat connecté afin de détecter les variations inhabituelles de températures et de les réguler à distance.

Pour la finalité 2 (prospection commerciale), des partenaires commerciaux du responsable du traitement peuvent être destinataires des données (adresse électroniques ou postales, numéros de téléphones, etc. à l'exclusion des données de santé) permettant de démarcher les personnes concernées pour leur propre compte (en tant que responsables des traitements).

La Commission rappelle sur ce point qu'avant toute transmission de données ou de campagne de prospection commerciale par téléphone, les professionnels doivent s'assurer que les numéros de téléphone concernés ne figurent pas dans la liste anti-démarchage téléphonique (BLOCTEL).

La Commission rappelle que dans le cas où l'hébergement de données de santé, recueillies ou produites à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, s'inscrivant dans le cadre du présent scénario « IN → OUT → IN » est confié à un prestataire tiers, celui-ci doit être certifié ou agréé à cet effet, qu'il soit situé en France ou à l'étranger (dans 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 relative à l'hébergement des données à caractère personnel).

INFORMATION ET DROITS DES PERSONNES :

La personne concernée doit être informée, préalablement à la mise en œuvre du traitement, de l'identité du responsable du traitement, de la finalité du traitement, des destinataires des données, des modalités d'exercice de ses droits d'accès, de rectification et d'opposition, des éventuels transferts de données hors de l'Union européenne ainsi que des durées de conservation.

Ce qui change avec le RGPD

Par ailleurs, le RGPD renforce l'information des personnes concernées. La Commission recommande que les nouvelles mentions suivantes soient d'ores et déjà portées à leur connaissance, préalablement à la mise en œuvre d'un traitement :

- les coordonnées du responsable du traitement et du délégué à la protection des données;
- la base légale du traitement ;
- l'identification des intérêts légitimes poursuivis par le responsable du traitement (lorsqu'ils constituent la base légale du traitement) ;
- les critères utilisés pour déterminer la durée de conservation des données (lorsque celle-ci ne peut pas être précisément déterminée) ;
- la mention des nouveaux droits des personnes (la possibilité de demander la limitation du traitement, le droit à la portabilité des données, le droit de retirer le consentement à tout moment lorsque le traitement est fondé sur cette modalité, le droit d'introduire une réclamation auprès d'une autorité de contrôle) ;
- le caractère réglementaire ou contractuel de l'exigence de fourniture des données, le caractère obligatoire de cette fourniture (si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir ces données), ainsi que les conséquences éventuelles de leur non-fourniture (impossibilité de fournir le service demandé, etc.) ;
- le cas échéant, l'existence d'une prise de décision automatisée (y compris un profilage) produisant des effets juridiques ou affectant de manière significative les personnes concernées et des informations concernant la logique sous-jacente à cette prise de décision, l'importance et les conséquences prévues du traitement pour les personnes ;
- en cas de traitement ultérieur pour une finalité autre que celle pour laquelle les données ont été initialement collectées, des informations sur cette autre finalité ;
- en cas de collecte indirecte, l'origine des données (y compris si celles-ci étaient publiquement accessibles).

Le RGPD prévoit que les personnes concernées doivent être informées en des termes clairs, simples et aisément accessibles. Cette information peut, par exemple, être effectuée lors de la signature du contrat de fourniture du dispositif ou de prestation de service par la personne concernée ou ses représentants légaux (via des clauses ou des documents spécifique).

Précision : *La Commission estime utile d'accompagner cette information d'icônes normalisées (facilement visibles, compréhensibles et clairement lisibles), afin d'offrir une bonne vue d'ensemble du traitement.*

De plus, afin que les personnes concernées, aient une parfaite connaissance des modalités de traitement de leurs données, la Commission recommande que ces dernières soient en outre informées des fonctionnalités des dispositifs (en particulier des modalités d'accès et de suppression des données et des moyens permettant à tout moment d'en désactiver tout ou partie des fonctionnalités). Cette information peut être fournie par tout moyen adapté (notice remise lors de l'acquisition du dispositif, ou accessible directement depuis le dispositif, etc.).

Les personnes concernées disposent des droits d'accès, de rectification et de suppression de l'ensemble des données traitées, ainsi que d'opposition pour des motifs légitimes.

Pour la finalité 2 (prospection commerciale), les personnes concernées doivent par ailleurs pouvoir s'opposer, sans frais, au traitement de leurs données par le responsable du traitement initial ou le responsable d'un traitement ultérieur.

FORMALITÉS PRÉALABLES :

FOCUS

Les formalités préalables devant être réalisées par les responsables des traitements dépendront de la finalité des traitements et de la nature des données collectées, quel que soit le dispositif utilisé.

***Par exemple**, si des données de santé sont traitées dans le cadre des finalités relevant du présent scénario (« IN → OUT → IN »), et que celles-ci sont collectées avec le consentement des personnes concernées ou que leur traitement est nécessaire à des fins de diagnostic médical, les responsables des traitements doivent effectuer une déclaration normale sur le site web de la CNIL (www.cnil.fr).*

Par ailleurs, dans certains cas, un engagement de conformité à l'autorisation unique n° AU-047, portant sur les traitements mis en œuvre dans le cadre de l'accueil, l'hébergement et le suivi des personnes handicapées et des personnes âgées pourra suffire. Cela sera notamment le cas lorsqu'un dispositif répond à l'une des finalités prévues dans cette autorisation unique et qu'il est mis en œuvre dans les conditions posées par cette norme.

FOCUS

La Commission souligne enfin que les traitements de données personnelles mis en œuvre dans le cadre du présent scénario « IN → OUT → IN », pourront être concernés par l'obligation de réaliser une étude d'impact sur la vie privée (EIVP), s'ils sont susceptibles de créer des risques élevés pour la vie privée des personnes concernées. Ces risques doivent notamment être appréciés sur la base des critères suivants, fixés par le RGPD :

- existence d'une évaluation systématique et approfondie d'aspects personnels concernant les personnes physiques, fondée sur un traitement automatisé (y compris le profilage), et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative ;
- présence d'un traitement de données à large échelle (au regard du nombre de personnes concernées, du volume de données et de leur degré de sensibilité, de la durée du traitement et de son étendue géographique) ;
- présence de traitements à grande échelle portant sur des catégories « particulières » de données personnelles au sens de l'article 9 du RGPD (notamment des données de santé) ;
- vulnérabilité des personnes concernées (notamment en raison de leur âge, de leur état de santé ou d'un handicap) ;
- utilisation de nouvelles technologies ou de dispositifs « innovants » (par exemple, des objets connectés associés à des applications smartphone).

En pareille hypothèse, les fournisseurs de service devra mener une EIVP pour identifier les risques que le traitement est susceptible d'engendrer, de déterminer et de mettre en œuvre les mesures nécessaires à la protection de la vie privée des personnes.

La Commission recommande d'ores et déjà aux fournisseurs de réaliser des EIVP dès la conception des produits et services. Elle met à disposition des catalogues de bonnes pratiques destinées à accompagner les professionnels dans cette démarche (https://www.cnil.fr/fr/PIA-privacy-impact-assessment).

MESURES DE SÉCURITÉ :

De façon générale, le responsable de traitement doit mettre en place des mesures de sécurité tant techniques qu'organisationnelles afin de garantir la confidentialité, l'authenticité et l'intégrité des données traitées par les appareils qu'il fournit à la personne, et doit prendre toutes les précautions utiles pour en empêcher la prise de contrôle par toute personne non autorisée. Ces mesures doivent être adaptées au niveau de sensibilité des

données et aux capacités de contrôle des appareils. Elles doivent notamment inclure, lorsqu'elles sont pertinentes au regard de la nature des dispositifs considérés :

- un chiffrement des échanges de données entre les différents appareils avec des algorithmes à l'état de l'art ;
- des mesures de protection des clés de chiffrement permettant d'en garantir la confidentialité ;
- des mécanismes d'authentification des appareils entre eux ;
- des mécanismes d'authentification de la personne préalablement à l'accès à des données personnelles.

Le fournisseur de dispositifs doit également prendre toutes les précautions utiles pour en empêcher la prise de contrôle par toute personne non autorisée, en prévoyant notamment :

- des mécanismes d'authentification de la personne préalablement à la transmission d'ordre aux dispositifs ;
- des mécanismes d'authentification des appareils préalablement à la transmission d'ordre aux dispositifs ;
- des mécanismes de sûreté permettant à la personne de couper le pilotage distant depuis l'intérieur du logement ;
- des mesures de sécurité renforcées au niveau des infrastructures responsables du pilotage à distance afin de garantir l'impossibilité pour des tiers d'en prendre le contrôle.

Le traitement de données de santé peut nécessiter la mise en place de mesures de sécurité supplémentaires comme :

- la mise en œuvre de mesures de pseudonymisation (par exemple telles que le hachage avec clé secrète des données telles que le nom/prénom de la personne concernée) ;
- l'hébergement des données chez un prestataire tiers certifié ou agréé à cet effet.

Par ailleurs, l'utilisation de données personnelles pour la réalisation de statistiques doit faire l'objet de mécanismes d'anonymisation permettant de garantir que les données ne peuvent plus être reliées aux personnes concernées. Ces mécanismes peuvent par exemple d'appuyer sur des opérations de hachage des données associées à des clés secrètes qui seront ensuite supprimées. Dans tous les cas, les mécanismes d'anonymisation doivent être conformes à l'avis du G29 du 10 avril 2014 sur les mécanismes d'anonymisation.