# NOTE N° 25/022 DU 27 JANVIER 2025 CONTENANT LES PRINCIPES GÉNÉRAUX CONCERNANT LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL, LA PSEUDONYMISATION ET LE PARTAGE DE RESPONSABILITÉS DE TRAITEMENT

La présente note définit les principes généraux concernant le traitement, la pseudonymisation et le partage de responsabilités de traitement, dans le cadre de l'utilisation secondaire de données à caractère personnel. Elle insiste, à cet égard, sur les garanties appropriées pour protéger les droits et libertés des personnes concernées. La note est, en l'espèce, spécifiquement applicable à healthdata.be.

1. Le cadre juridique général

Chaque prestataire de soins ou établissement de soins est le responsable du traitement en ce qui concerne le traitement de données à caractère personnel pour la prestation de soins de qualité et continus.

Le traitement ultérieur de données à caractère personnel pour des finalités scientifiques ou statistiques (dénommé ci-après « utilisation secondaire ») est autorisé, conformément aux articles 5, 1, b) et e), et 89, 1, du Règlement général relatif à la protection des données (RGPD), dans la mesure où il est soumis à des « garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties garantissent la mise en place de mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données. Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière. Chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière ».

La loi belge relative au traitement de données à caractère personnel précise par ailleurs qui est chargé de l'anonymisation ou de la pseudonymisation. Lorsque des données en provenance d'une seule source sont traitées dans le cadre d'une utilisation secondaire, l'anonymisation ou la pseudonymisation est effectuée par cette source. Lorsque des données en provenance de différentes sources sont couplées, l'anonymisation ou la pseudonymisation est effectuée par une de ces sources ou par un tiers de confiance (dénommé ci-après 'TTP'). En l'occurrence, il est opté pour le recours à un TTP lorsqu'il est question d'une couplage de données en provenance de plusieurs sources.

2. Le concept de « pseudonymisation » et sa concrétisation

L'article 4, § 5, du RGPD définit la pseudonymisation comme « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

Quatre conditions doivent donc être remplies :

1° les données pseudonymisées ne peuvent pas comprendre de données à caractère personnel permettant une identification directe (p.ex. NISS, nom, adresse exacte, ...) ;

2° l'ensemble de données pseudonymisées ne peut raisonnablement pas permettre de déduire de quelle personne identifiée ou identifiable il s'agit ;
3° il ne peut raisonnablement être possible pour la partie destinataire d'associer les données pseudonymisées à des données complémentaires de sorte à pouvoir déduire de quelle personne identifiée ou identifiable il s'agit ;
4° les données complémentaires dont on peut déduire de quelle personne identifiée ou identifiable il s'agit, doivent donc être sauvegardées séparément des données pseudonymisées pour lesquelles des mesures techniques et organisationnelles appropriées sont prises afin de garantir que la partie destinataire ne puisse raisonnablement pas (à nouveau) associer les données pseudonymisées à la personne identifiée ou identifiable.

Afin de respecter au maximum le principe de minimisation des données, un bonne pratique consiste à réaliser l'anonymisation ou la pseudonymisation en deux phases.

1° pour répondre à la condition 1 précitée, les données à caractère personnel permettant une identification directe sont remplacées, dès que possible, par un code d'identification sans signification ; si toutes les données sont issues d'une seule source ou si les données proviennent de plusieurs sources mais ne doivent pas être couplées, l'anonymisation ou la pseudonymisation sont effectuées par cette source ou par chacune de ces sources ; si les données proviennent de sources différentes et doivent pouvoir être couplées, la Plate-forme eHealth transmet à chaque source un code d'identification sans signification qui est le même à travers toutes les sources pour une même personne ; pour ce faire, la Plate-forme eHealth n'a pas accès aux données à caractère personnel relatives à la santé et elle agit comme TTP de codage.
2° pour répondre aux conditions 2 et 3 précitées, les données à caractère personnel à anonymiser ou pseudonymiser sont transmises avec mention du code d'identification sans signification à un autre TTP que la Plate-forme eHealth ; ce TTP n'a donc pas connaissance des données à caractère personnel d'identification directe et agit comme TTP d'anonymisation/pseudonymisation.

Il est indiqué, pour chaque cas d'utilisation, que la TTP réalisant la pseudonymisation mette en œuvre un ensemble ou une combinaison appropriés de techniques ou de mesures de protection de la vie privée qui garantissent que les possibilités de la partie destinataire à associer les données pseudonymisées à une personne identifiée ou identifiable soient raisonnablement limitées.

3. La répartition des rôles concrète et la détermination des responsables du traitement

Si des données à caractère personnel sont collectées par Healthdata.be à des fins d'utilisation secondaire soit auprès d'une seule source, soit auprès de différentes sources, mais qu'elles ne doivent pas être couplées, la source prévoit un code d'identification sans signification pour chaque enregistrement transmis à Healthdata.be. La source ne communique pas de données à caractère personnel d'identification directe (p.ex. le nom, l'adresse exacte, ...) à Healthdata.be.

Si des données à caractère personnel sont collectées par Healthdata.be à des fins d'utilisation secondaire auprès de plusieurs sources et qu'elles doivent pouvoir être couplées, chaque source reçoit de la part de la Plate-forme eHealth, pour chaque enregistrement à communiquer à Healthdata.be, un code d'identification sans signification associé au NISS de l'intéressé. Pour un même NISS, toutes les sources reçoivent le même code sans signification via la Plate-forme

eHealth. La Plate-forme eHealth, en tant que TTP de codage, est le responsable du traitement pour la création et la transmission du code d'identification sans signification. Chaque source ajoute le code d'identification sans signification à chaque enregistrement transmis à Healthdata.be. Aucune source ne communique des données à caractère personnel qui permettent une identification directe (p.ex. le nom, l'adresse exacte, ...) à Healthdata.be.

Si Healthdata.be reçoit des données à caractère personnel (d'identification non directe) en provenance de plusieurs sources qui doivent être couplées entre elles, Healthdata.be peut réaliser le couplage sur la base du code d'identification sans signification commun.
Healthdata.be, en tant que TTP d'anonymisation/pseudonymisation, est le responsable du traitement pour l'anonymisation ou la pseudonynimisation des données à caractère personnel (d'identification non directe) obtenues, préalablement à leur transmission à un tiers (KCE, INAMI, autre section au sein de Sciensano, scientifiques, ...) pour utilisation secondaire.

Ni la Plate-forme eHealth, ni Healthdata.be ne peuvent eux-mêmes traiter des données en tant que responsable du traitement pour une utilisation secondaire. Ceci est contraire à leur rôle de TTP.

La communications de données à caractère personnel requiert une délibération du Comité de sécurité de l'information dans les cas prévus par la loi. Il est décrit dans cette délibération :

- quelles données
- concernant quelles catégories de personnes
- peuvent être communiquées
- par qui à qui
- pour quelles finalités de traitement légitimes
- moyennant quelles mesures de protection des données
- et pendant quel délai les données peuvent être conservées
- avec une motivation de la façon dont les principes de limitation de la finalité et de minimisation des données sont respectés.

Le tiers auquel Healthdata.be transmet les données à caractère personnel pseudonymisées pour une utilisation secondaire est le responsable du traitement en ce qui concerne le traitement de ces données pour une utilisation secondaire.

Dans la mesure où un tiers, en tant que responsable du traitement pour une utilisation secondaire, souhaite avoir recours à Healthdata.be en tant que sous-traitant :

- soit une instance autre que Healthdata.be doit intervenir comme TTP d'anonymisation/pseudonymisation pour l'anonymisation ou la pseudonymisation des données concernées ;
- soit une séparation de fonctions stricte doit être prévue au sein de Healthdata.be entre, d'une part, les personnes et ressources prévues pour agir comme TTP d'anonymisation/pseudonymisation et, d'autre part, les personnes et ressources prévues pour agir comme sous-traitant, de sorte à ce qu'il n'y ait aucun risque que les données traitées pour une utilisation secondaire soient dé-anonymisées ou dépseudonymisées.

Dans ce cas, il y a lieu :

- d'établir un contrat de sous-traitance entre le tiers et Healthdata.be
- de fournir les informations utiles en ce qui concerne l'intervention de Healthdata.be comme sous-traitant et l'organisation de la séparation de fonctions précitée, dans la

demande adressée au Comité de sécurité de l'information en vue d'obtenir une délibération.