NOTA NR. 25/022 VAN 27 JANUARI 2025 BETREFFENDE DE ALGEMENE PRINCIPES OMTRENT DE VERWERKING VAN PERSOONSGEGEVENS, PSEUDONIMISERING EN VERDELING VAN VERWERKINGSVERANTWOORDELIJKHEDEN

Deze nota richt zich op de algemene principes omtrent de verwerking, pseudonimisering en rolverdeling van de verwerkingsverantwoordelijkheden in het kader van secundair gebruik van persoonsgegevens. Er wordt daarbij de nadruk gelegd op de passende waarborgen om de rechten en vrijheden van de betrokkenen te beschermen. De nota is *in casu* specifiek van toepassing op healthdata.be.

1. Het algemeen juridische kader

Elke zorgverstrekker of zorginstelling is verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens voor de verstrekking van kwalitatieve en continue zorg.

De verdere verwerking van persoonsgegevens voor wetenschappelijke of statistische doeleinden (hierna genoemd "secondary use") is krachtens de artikelen 5, 1. b) en e), en 89, 1. van de Algemene Verordening Gegevensbescherming (AVG) toegestaan mits ze is onderworpen aan "passende waarborgen in overeenstemming met de AVG voor de rechten en vrijheden van de betrokkene. Die waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Deze maatregelen kunnen pseudonimisering omvatten, mits aldus die doeleinden in kwestie kunnen worden verwezenlijkt. Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt."

In de Belgische Wet Verwerking Persoonsgegevens wordt verder aangegeven door wie er moet worden geanonimiseerd of gepseudonimiseerd. Wanneer er gegevens vanuit één bron worden verwerkt voor secondary use geschiedt de anonimisering of pseudonimisering door die bron. Wanneer er gegevens vanuit verschillende bronnen worden gekoppeld, geschiedt de anonimisering of pseudonimisering door één van de bronnen of door een derde vertrouwenspersoon (hierna genoemd "TTP"). In casu wordt geopteerd om bij koppeling van gegevens vanuit verschillende bronnen steeds beroep te doen op een TTP.

2. Het concept "pseudonimisering" en de concretisering ervan

Artikel 4, 5) van de AVG definieert pseudonimisering als "het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld".

Er moet dus aan 4 voorwaarden worden voldaan:

1° de gepseudonimiseerde gegevens mogen geen rechtstreeks identificerende persoonsgegevens (bv. INSZ, naam, precies adres, …) omvatten;
2° het geheel van gepseudonimiseerde gegevens mag op zich redelijkerwijs niet toelaten af te leiden over welke geïdentificeerde of identificeerbare persoon het gaat;

3° het mag voor de ontvangende partij redelijkerwijs niet mogelijk zijn om de gepseudonimiseerde gegevens te koppelen aan aanvullende gegevens waardoor kan worden afgeleid over welke geïdentificeerde of identificeerbare persoon het gaat;
4° de aanvullende gegevens waarmee kan worden afgeleid over welke geïdentificeerde of identificeerbare persoon het gaat, dienen dus apart te worden bewaard van de gepseudonimiseerde gegevens, waarbij de passende technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de ontvangende partij de gepseudonimiseerde gegevens redelijkerwijs niet (terug) kan linken aan de geïdentificeerde of identificeerbare persoon.

Om het principe van de gegevensminimalisatie maximaal te respecteren, is het een goede praktijk om de anonimisering of pseudonimisering door te voeren in 2 stappen.

1° om aan hogervermelde voorwaarde 1. te voldoen, worden de rechtstreeks identificerende persoonsgegevens zo vroeg mogelijk vervangen door een betekenisloze identificatiecode; indien alle gegevens uit één bron komen, of indien de gegevens uit verschillende bronnen komen, maar niet moeten kunnen worden gekoppeld, geschiedt dit door die bron of door elk van die bronnen; indien gegevens uit verschillende bronnen komen, maar wel moeten kunnen worden gekoppeld, geschiedt dit doordat elke bron via het eHealth-platform een betekenisloze identificatiecode bekomt, die voor eenzelfde persoon dezelfde is over de bronnen heen; het eHealth-platform krijgt daartoe geen inzicht in persoonsgegevens over de gezondheid, en treedt op als coderings-TTP.
2° om aan de hogervermelde voorwaarden 2. en 3. te voldoen, worden de persoonsgegevens die moeten worden geanonimiseerd of gepseudonimiseerd met vermelding van de betekenisloze identificatiecode bezorgd aan een andere TTP dan het eHealth-platform; deze TTP heeft dus nooit kennis van de rechtstreeks identificerende persoonsgegevens en treedt op als anonimiserings/pseudonimiserings-TTP.

Het verdient aanbeveling dat de TTP die de pseudonimisering bewerkstelligt, voor elke use-case een aangepaste set of combinatie aan privacybevorderende technieken of maatregelen toepast die ervoor zorgen dat de mogelijkheden van de ontvangende partij om de gepseudonimiseerde gegevens te linken aan een geïdentificeerd of identificeerbaar persoon redelijkerwijs worden beperkt.

3. De concrete rolverdeling en de bepaling van de verwerkingsverantwoordelijkheden

Indien persoonsgegevens door Healthdata.be ter ondersteuning van secondary use worden ingezameld hetzij bij één bron, hetzij bij verschillende bronnen, maar niet moeten kunnen worden gekoppeld, wordt elk aan Healthdata.be meegedeeld record door de bron voorzien van een betekenisloze identificatiecode. De bron deelt geen rechtstreeks identificerende persoonsgegevens (bv. naam, precies adres, …) mee aan Healthdata.be.

Indien persoonsgegevens door Healthdata.be ter ondersteuning van secondary use worden ingezameld bij meerdere bronnen en wel moeten kunnen worden gekoppeld, verkrijgt elke bron via het eHealth-platform voor elk aan Healthdata.be mee te delen record een betekenisloze identificatiecode gekoppeld aan het INSZ van de betrokkene. Voor eenzelfde INSZ krijgen alle bronnen via het eHealth-platform dezelfde betekenisloze code. Het eHealth-platform is als coderings-TTP verwerkingsverantwoordelijke voor het aanmaken en

doorgeven van de betekenisloze identificatiecode. Elke bron voorziet elk aan Healthdata.be meegedeeld record van de betekenisloze identificatiecode. Geen enkele bron deelt rechtstreeks identificerende persoonsgegevens (bv. naam, precies adres, …) mee aan Healthdata.be.

Indien Healthdata.be (niet rechtstreeks identificerende) persoonsgegevens verkrijgt vanuit verschillende bronnen die met mekaar moeten kunnen worden gekoppeld, kan Healthdata.be de koppeling doorvoeren op basis van de gemeenschappelijke betekenisloze identificatiecode.

Healthdata.be is als anonimiserings/pseudonimiserings-TTP verwerkingsverantwoordelijke om de verkregen (niet rechtstreeks identificerende) persoonsgegevens te anonimiseren of te pseudonimiseren vooraleer ze voor secondary use worden doorgegeven aan een derde (KCE, RIZIV, andere afdeling binnen Sciensano, wetenschappers, …).

Noch het eHealth-platform, noch Healthdata.be mogen zelf als verwerkingsverantwoordelijke gegevens verwerken voor secondary use. Dat is immers in strijd met hun rol als TTP.

In de gevallen voorzien krachtens de wet, vereist de mededeling van persoonsgegevens een beraadslaging van het Informatieveiligheidscomité. In deze beraadslaging wordt beschreven

- welke gegevens
- over welke categorieën van personen
- door wie
- aan wie worden meegedeeld
- voor welke rechtmatige verwerkingsdoeleinden
- met welke maatregelen inzake gegevensbescherming
- gedurende welke periode de gegevens mogen worden bewaard
- met een motivering van de wijze waarop de beginselen van doelbinding en minimale gegevensverwerking worden nageleefd.

De derde waaraan Healthdata.be gepseudonimiseerde persoonsgegevens doorgeeft voor secondary use is verwerkingsverantwoordelijke voor de verwerking van deze gegevens voor secondary use.

Indien een derde, verwerkingsverantwoordelijke voor secondary use, daarbij beroep wil doen op Healthdata.be als verwerker, dient

- hetzij een andere instantie dan Healthdata.be als anonimiserings/pseudonimiserings-TTP op te treden voor de anonimisering of pseudonimisering van de betrokken gegevens;
- hetzij binnen Healthdata.be een strikte scheiding te worden voorzien tussen enerzijds de personen en middelen die worden voorzien voor het optreden als anonimiserings/pseudonimiserings-TTP en anderzijds de personen en middelen ingezet voor het optreden als verwerker, zodat er geen risico bestaat dat de gegevens gebruikt voor secondary use gedeanonimiseerd of gedepseudonimiseerd kunnen worden.

In dat geval moet ook

- een verwerkersovereenkomst worden opgesteld tussen de derde en Healthdata.be
- omtrent het optreden van Healthdata.be als verwerker en omtrent de organisatie van de vermelde scheiding de nodige informatie worden verstrekt bij de aanvraag van een beraadslaging van het Informatieveiligheidscomité.