

Pseudonimisering van het unieke cliënt identificatienummer (BSN) vindt plaats door een door de GGD Amsterdam extern gecontracteerde Trusted Third Party (verder te noemen: de TTP), die een totaalpakket van services en diensten biedt, inclusief de benodigde applicatie, op het gebied van privacybescherming van persoonsgegevens.

De omzetting verloopt in een aantal stappen:

1. De TTP-applicatie *pseudonimiseert* vóór verzending de BSN's bij de deelnemende partij van ZOOM-database. Deze applicatie wordt onder verantwoordelijkheid van de deelnemende partij van ZOOM-database gebruikt. De TTP heeft geen toegang tot de inhoud van de applicatie die is geïnstalleerd bij de deelnemende partij en krijgt door het gebruik van de applicatie geen BSN's aangeleverd.
2. Daarnaast wordt voor verzending bij de deelnemende partij ook een aantal velden *geanonimiseerd*, wat inhoudt dat ze worden opgeschaald (bijvoorbeeld, "geboortedatum" wordt "leeftijdscategorie").
3. Na pseudonimisatie en anonimisatie wordt het bestand via een beveiligde https route door de aanbiedende partij naar de TTP verzonden.
4. Het bestand wordt daarbij in twee delen gesplitst: pseudoniemen en de inhoudelijke data.
 - a. Op het bestand met de pseudoniemen wordt door de TTP met behulp van centrale pseudonimisatiesoftware een volgende bewerking uitgevoerd. Na deze bewerking is sprake van een definitief pseudoniem van het BSN, die niet meer door zowel de aanbiedende partij als de ontvangende partij (GGD Amsterdam) te relateren is aan het oorspronkelijke BSN.
 - b. De inhoudelijke data worden zo versleuteld dat de TTP er geen toegang toe heeft.
5. De versleutelde BSN's en inhoudelijke data worden uiteindelijk via een beveiligde internetverbinding (https) doorgestuurd naar de GGD Amsterdam die de ZOOM-database beheert.