PSEUDONIMISEREN VAN PERSOONSGEGEVENS

Factsheet

VIACRYP B.V. Danzigerkade 19, 1013 AP Amsterdam

Inhoudsopgave

1 Introductie

1.1 Viacryp en het pseudonimiseren van persoonsgegevens

Viacryp is gespecialiseerd in het helpen van organisaties die te maken hebben met de verwerking van persoonsgegevens en in het bijzonder met de Algemene Verordening Gegevensbescherming (AVG) of General Data Protection Regulation (GDPR). Organisaties die voor hun communicatie met de doelgroep en hun interne processen, persoonsgegevens nodig hebben om hun doelstellingen te behalen, zijn door de AVG aan strenge richtlijnen gebonden. Viacryp levert verschillende diensten die bijdragen aan het beschermen van persoonsgegevens door de hoeveelheid leesbaar opgeslagen en verwerkte persoonsgegevens te minimaliseren en te pseudonimiseren.

Viacryp is een onafhankelijke organisatie die vanaf 1 juli 2013 werkzaam is als Trusted Third Party op het gebied van pseudonimisering van persoonsgegevens.

1.2 Regelgeving met betrekking tot persoonsgegevens

De AVG[1] stelt strenge eisen aan het verwerken van gegevens die op enigerlei wijze te herleiden zijn tot natuurlijke personen. Hierbij geldt dat deze herleidbaarheid in de breedste zin van het woord moet worden opgevat. Dit houdt in dat wordt gekeken naar zowel de direct identificeerbare gegevens zoals BSN-nummer, naam en adresgegevens of IP-adres, als naar de indirect identificeerbare gegevens zoals de geboortedatum of een volledig gevulde postcode.
Voor het mogen verwerken van persoonsgegevens is een grondslag noodzakelijk. Deze grondslagen staan beschreven in de AVG. De AVG baseert zich verder op een aantal algemene uitgangspunten met betrekking tot het opslaan en verwerken van deze persoonsgegevens:

- Dataminimalisatie (niet meer opslaan dan noodzakelijk);
- Niet langer bewaren dan noodzakelijk;
- Passende beveiligingsmaatregelen om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Indien er geen grondslag is, mogen persoonsgegevens niet worden verwerkt.

Viacryp voldoet bij de toepassing van pseudonimisering aan de volgende voorwaarden:

I. Er wordt vakkundig gebruik gemaakt van pseudonimisering, waarbij de eerste van de twee uitgevoerde versleutelingen van gegevens plaatsvindt bij de aanbieder van de gegevens;
II. Er zijn technische en organisatorische maatregelen getroffen om herhaalbaarheid van de versleuteling (“replay attack”) te voorkomen;
III. De verwerkte gegevens zijn niet indirect identificerend[2];
IV. Deze drie voorwaarden worden onderworpen aan periodiek te houden audits.
V. Daarnaast is de pseudonimiseringsoplossing op heldere en volledige wijze beschreven in een actief openbaar gemaakt document, zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt.

1.3 Doel van dit document

Dit document dient om te voldoen aan voorwaarde V. dat de pseudonimiseeroplossing op heldere en volledige wijze in een actief openbaar gemaakt document gepubliceerd is. Met dit doel wordt in hoofdstuk 2 de als pseudonimiseeroplossing geïntroduceerde pseudonimiseerstraat in detail beschreven.

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf
[2] Dit is de verantwoordelijkheid van de verwerkingsverantwoordelijke; Viacryp kan hier slechts in adviseren

2 De pseudonimiseerstraat

2.1 Inleiding

Een pseudonimiseerstraat bestaat uit één of meerdere bronnen, die via een supply-platform data aanleveren aan Pseudonymizer. Als de data van deze bronnen gepseudonimiseerd is, wordt deze via een delivery-platform aangeleverd aan één afnemer, die op basis van pseudoniemen gegevens uit de verschillende bronnen kan combineren en analyses kan doen op gedrag, zonder hierbij over persoonsgegevens te hoeven beschikken.

Indien dit vereist is, wordt in bepaalde configuraties het combineren van verschillende bronnen uitgevoerd vóór aflevering aan de afnemer. In dat geval worden géén pseudoniemen aangeleverd aan de afnemer en wordt de data geprepareerd voor analysedoeleinden, dit om indirecte herleidbaarheid van deze gegevens te voorkomen.

2.2 Splitsing van data

De straat waarmee Viacryp als Trusted Third Party werkt zorgt voor zowel 'Splitsing van data', waarbij persoonsgegevens (Wie) en te analyseren gedrag (Wat) vroeg in het proces van elkaar gesplitst worden, als 'Scheiding van data', waarmee door op de gesplitste **Wie** en **Wat** hashing en encryptie toe te passen wordt bereikt dat nergens in het proces (uitgezonderd bij de bron van de oorspronkelijke gegevens) zowel de **Wie** als de **Wat** in leesbare vorm te raadplegen zijn. Dit kan worden toegelicht aan de hand van de volgende tabel:

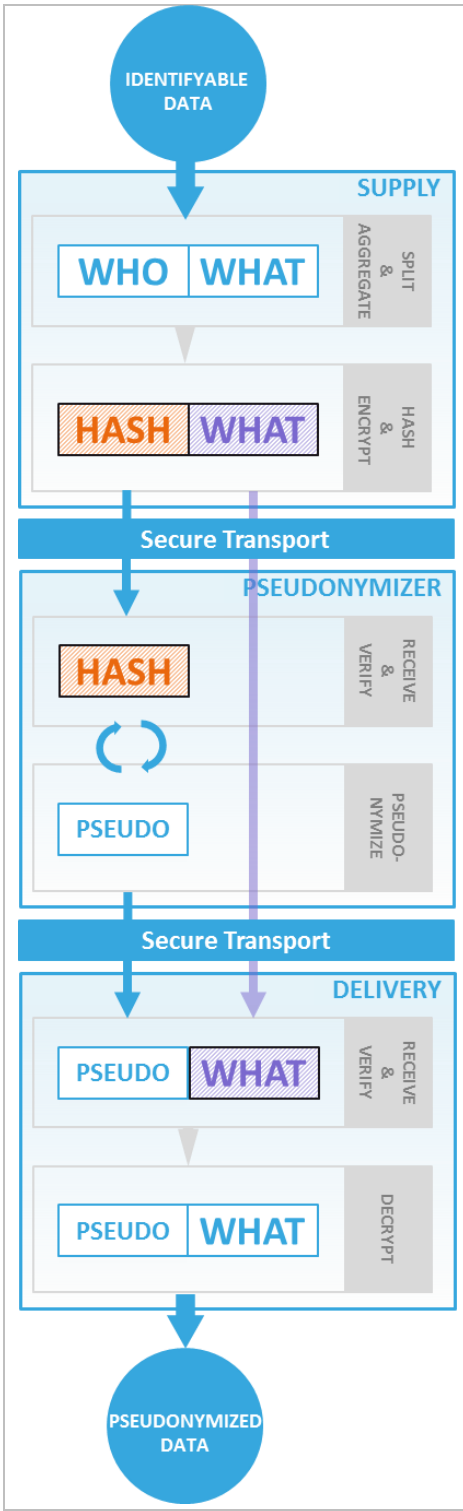
	Bron	Supply	Pseudonymizer	Delivery	Afnemer
Wie	Origineel	Hashed	Hashed	Pseudoniem*	Pseudoniem*
Wat	Origineel	Encrypted	Encrypted	Encrypted	Origineel

*) Optioneel

- Alleen de bron beschikt over de originele **Wie** en **Wat.**
- Op het supply-platform wordt de **Wie** gehashed en encrypted en de **Wat** encrypted voordat de data het domein van de bron verlaat.
- Pseudonymizer beschikt alleen over de gehashte **Wie** om daar pseudoniemen van te kunnen maken die danwel (samen met gehashte **Wat**) gebruikt worden om data te prepareren voor analysedoeleinden, danwel worden gecombineerde met de encrypted **Wat.** Vervolgens wordt deze data aangeleverd aan het delivery-platform bij de afnemer.
- Op het delivery-platform worden de ontvangen gegevens decrypted en ter beschikking gesteld aan de afnemer, die hierop analyses kan uitvoeren zonder beschikking te hebben over persoonsgegevens.

2.3 Architectuur

De hele straat die ieder bestand van een bron doorloopt, wordt schematisch weergegeven aan de hand van de volgende architectuur:



Bron
Levert data in een afgesproken formaat aan op de Supply-module, die draait in het domein van de bron.

Split & Aggregate
Brondata wordt gescheiden in identificerende gegevens (**Wie**) en gedrag (**Wat**). **Wat** wordt op een zodanig niveau geaggregeerd dat dit niet (indirect) tot een persoon herleidbaar is.

Hash & Encrypt
Wie wordt door middel van eenrichtingsversleuteling (hash) onleesbaar gemaakt. **Wat** wordt encrypted, zodanig dat alleen de afnemer deze kan decrypten.

Receive & Verify
Deze data wordt via een veilige verbinding naar de TTP verstuurd, waar de Pseudonymizer-module de herkomst van de data valideert.

Pseudonymize
In de pseudonymize-stap worden hashes vertaald naar pseudoniemen.

Receive & Verify
Pseudoniemen en (nog steeds) encrypted **Wat** worden via een veilige verbinding getransporteerd naar de delivery-module, die draait bij de afnemer van de gepseudonimiseerde data. Hier wordt wederom de herkomst van de data gevalideerd.

Decrypt
In de laatste stap wordt **Wat** door de afnemer decrypted.

Afnemer
De afnemer beschikt nu over gepseudonimiseerde data en kan hierop analyses uitvoeren zonder beschikking te hebben over persoonsgegevens.