AUDITRAAMWERK PSEUDONI-MISEREN VAN VIACRYP B.V. 2017

VIACRYP B.V. Danzigerkade 19, 1013 AP Amsterdam

Inhoudsopgave

1. Introductie

Dit document beschrijft het auditraamwerk van Viacryp. Door audits uit te voeren op basis van dit raamwerk wil Viacryp haar rol als onafhankelijke Trusted Third Party bevestigen en aantonen dat zij op een veilige en gecontroleerde wijze persoons- en gedragsgegevens verwerkt.

1.1. Achtergronden

1.1.1. Pseudonimiseren

Onder 'pseudonimiseren' wordt verstaan het omzetten van een persoonsgegeven naar een niet tot de oorspronkelijke persoon herleidbare unieke code. Pseudonimiseren is een herhaalbaar proces waarbij de direct identificerende gegevens van één persoon binnen een afgesproken periode leidt tot eenzelfde pseudoniem. Hierdoor is het mogelijk zonder herleidbaarheid van de persoonsgegevens:

- Gepseudonimiseerde gegevens vanuit verschillende bronnen te koppelen;
- Gepseudonimiseerde gegevens op een later tijdstip te verrijken met nieuwe gegevens;

Hoewel pseudoniemen volgens de (privacy) wetgeving[1] nog steeds als persoonsgegeven moeten worden beschouwd, geldt dat met pseudoniemen meer verwerkingen mogelijk worden dan met niet gespeudonimiseerde persoonsgegevens[2].

- Overweging 26 uit de AVG geeft aan dat pseudoniemen niet als anoniem gegeven mogen worden beschouwd: “Gepseudonimiseerde persoonsgegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, moeten als gegevens over een identificeerbare natuurlijke persoon worden beschouwd.”
- Daarentegen wordt in overweging 28 van de verordering aangegeven: “De toepassing van pseudonimisering op persoonsgegevens kan de risico's voor de betrokkenen verminderen”

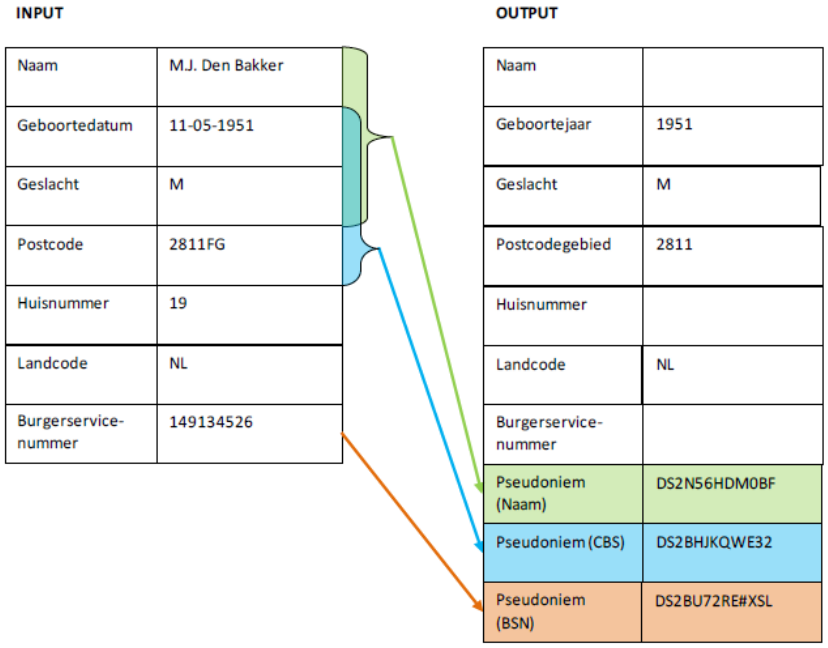
1.1.2. Privacy-verhogende diensten

Ook indien bij de opdrachtgever een grondslag bestaat voor verwerking, kunnen diensten van Viacryp ingezet worden als privacy-verhogende diensten. Een voorbeeld van een dergelijke dienst is de filterdienst.

1.1.3. Pseudonimiseerstraat

In de aangeboden oplossing van Viacryp vindt de pseudonimisering plaats binnen de context van een zgn. pseudonimiseerstraat. Het concept achter de pseudonimiseerstraat is dat daarbinnen niemand kan beschikken over de persoons- of gedragsgegevens, een combinatie van beide, of over een combinatie van gegevens die samen met andere gegevens kunnen leiden tot een verband tussen persoonsgegevens en gedrag. De oorspronkelijke persoons- en gedragsgegevens zijn alleen bij de bron bekend en leesbaar.

[1] 18 Mei 2018 treedt de Algemene Werordening Gegevensbescherming (AVG/GDPR) in werking en waarmee de huidige Wet Bescherming Persoonsgegevens (WBP) komt te vervallen.
[2] De (Nederlandse) Autoriteit Persoonsgegevens (AP) heeft aangegeven dat zij ook dit standpunt volgen in de periode dat de WBP nog van toepassing is.



Elke straat kent één of meerdere bronnen (aanbieders) van persoonsgegevens en één afnemer van de gepseudonimiseerde resultaten. Iedere Viacrypstraat bestaat uit drie op elkaar afgestemde componenten. Pseudoniemen bestaan alleen binnen een specifieke straat. Gegevens kunnen niet over straten heen met elkaar gecombineerd worden. Binnen één verwerkingsstraat zal een identificeerbaar gegeven altijd tot eenzelfde pseudoniem leiden.

Viacryp levert voor zowel de aanbieders als de afnemers, vooraf geconfigureerde software die het pseudonimiseringsproces ondersteunen. Voor de aanbieders betreft dit de “Supply” module. Bij Viacryp is software (Pseudonymizer) aanwezig waarmee de identificeerbare gegevens worden omgezet naar een pseudoniem. De afnemer kan vervolgens op basis van pseudoniemen gegevens uit verschillende bronnen combineren en analyseren zonder hierbij over persoonsgegevens te hoeven beschikken.

De werking van het pseudonimiseringsproces is gepubliceerd in het document “Factsheet Viacryp”.

1.2. Viacryp

Viacryp biedt diensten aan om persoonsgegevens veilig en gecontroleerd te verwerken tot pseudoniemen. Daarmee worden klanten in staat gesteld om binnen de voor hun geldende (privacy)wetgeving, persoonsprofielen op te stellen en gedrag te analyseren.

Viacryp biedt diensten aan voor gegevensverwerking achteraf en op realtime-basis. Tevens adviseert en ondersteunt Viacryp haar klanten bij het nemen van de juiste maatregelen om veilig en binnen de kaders van de van toepassing zijnde (privacy)wetgeving, verwerking van persoonsgegevens zodanig uit te voeren dat de privacy van de betrokken personen maximaal beschermd wordt. Het blijft echter de verantwoordelijkheid van de klant om binnen de kaders van de wet- en regelgeving te opereren.

Als Trusted Third Party (TTP) opereert Viacryp als intermediair tussen leverancier(s) van originele persoonsgegevens en de afnemer van de gepseudonimiseerde gegevens. In die rol waarborgt Viacryp dat:

- Viacryp altijd persoonsgegevens verwerkt, binnen de kaders van de geldende (privacy)wetgeving
- Viacryp een vakkundige versleuteling toepast op de persoonsgegevens
- Viacryp zorgdraagt voor zorgvuldig sleutelbeheer voor optimale geheimhouding van gegevens
- Viacryp een onafhankelijke en belangenvrije positie kan innemen door geen toegang te hebben tot een leesbare vorm van de te verwerken of verwerkte persoons- en andere gegevens

1.3. Doel van dit document

Dit document is de leidraad voor de audit op diensten van Viacryp. De audit heeft als doel om aan te tonen dat Viacryp in staat is om op veilige en gecontroleerde wijze persoonsgegevens te pseudonimiseren. De audit richt zich op de technische maatregelen en interne organisatorische maatregelen en verantwoordelijkheden die gezamenlijk zorgdragen voor de veilige en gecontroleerde verwerking van persoonsgegevens.

Viacryp heeft technologie ontwikkeld en een proces ingericht om persoonsgegevens te pseudonimiseren, waardoor herleidbaarheid van de versleuteling ('replay attack') aanzienlijk bemoeilijkt wordt[3]. Haar onafhankelijke en belangenvrije positie als TTP waarborgt Viacryp door technische en organisatorische maatregelen die het onmogelijk maken om gegevens tijdens het proces van verwerking, in leesbare vorm in te zien. Viacryp stelt zichzelf de volgende criteria om aan te tonen dat zij hiertoe in staat is:

- Er wordt vakkundig gebruikgemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens;
- Er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling ('replay attack') te voorkomen en om te voorkomen dat Viacryp inzicht krijgt in of toegang tot, voor mensen leesbare gegevens;
- Om iedere betrokkene in staat te stellen kennis te laten nemen welke garanties geboden worden, is de gehanteerde pseudonimisering-oplossing in een openbaar beschikbaar document beschreven.

1.4. Leeswijzer

In hoofdstuk 2 is een beschrijving opgenomen van de achtergronden en de soorten onderzoeken die worden uitgevoerd om conformiteit aan de criteria zoals gesteld in paragraaf 1.3. In hoofdstuk 3 worden de uit te voeren onderzoeken beschreven om aan te tonen dat in het proces wordt voldaan aan de gestelde criteria. Deze onderzoeken richten zich achtereenvolgens op de kwaliteit en veiligheid van de gebruikte techniek en de organisatorische maatregelen, de klantafspraken die gemaakt worden en de wijze waarop Viacryp haar klanten ondersteunt bij het verkrijgen van de mogelijkheid om met volledig anonieme gegevens te werken. In hoofdstuk 4 wordt de opzet en uitvoering van het auditproces beschreven.

In Bijlage A.1 is een lijst opgenomen met afkortingen en definities, zoals die worden gehanteerd binnen dit document. In Bijlage A.2 is een overzicht opgenomen van de te gebruiken controls en in Bijlage A.3 is een overzicht opgenomen van mogelijke tekortkomingen per criterium. Bijlage A.4 bevat een overzicht van de gebruikte encryptietechnieken.

[3] Volledige bescherming tegen Replay attack is alleen mogelijk indien de klant zelf hiervoor de juiste procedurele maatregelen treft.

2. Soorten onderzoeken

Om te kunnen beoordelen of Viacryp aan de gestelde criteria, opgenomen in paragraaf 1.3 voldoet, zijn de volgende onderzoeken voorzien.

- Onderzoek 1: Het functionele proces en technische inrichting van de technologie van Viacryp
  Een onderzoek naar de functionele en technische inrichting van de ontwikkelde technologie waarin vastgesteld wordt of de technologie voldoende waarborgen biedt voor de veilige, niet-leesbare en niet-herleidbare verwerking van gegevens.
- Onderzoek 2: Beheer van Viacryp
  Dit onderzoek betreft de beheeromgeving waarbinnen de technologie van Viacryp ondergebracht is. Hierbij worden de door de beheerorganisatie genomen technische en organisatorische maatregelen getoetst.
- Onderzoek 3: Klantafspraken
  Dit onderzoek toetst de afspraken die tussen Viacryp en haar klanten zijn gemaakt.

Het object van het onderzoek betreft de gerealiseerde technologie, de getroffen beheersmaatregelen rond de cryptografische systemen en (beheer)processen voor de generieke pseudonimisering van persoonsgegevens

De onderzoeken worden in het volgende hoofdstuk uitgewerkt. De te gebruiken controls voor het auditraamwerk vanuit ISO 27001 en ISO 20000 zijn opgenomen in bijlage A.2.

3. Onderzoeken

3.1. Onderzoek 1: Het functionele proces en technische inrichting van de technologie van Viacryp

3.1.1. Doelstelling

De doelstelling is om aan te tonen dat gerealiseerde technologie voldoende waarborgen biedt voor een vakkundige en veilige verwerking van persoons- en gedragsgegevens. Concreet betekent dit dat de technologie waarborgen biedt tegen replay attacks en voorkomt dat enig persoons- of gedragsgegeven leesbaar of herleidbaar is binnen de context van de Viacrypstraat. Tevens dient aangetoond te worden dat de publiek beschikbare documentatie in overstemming is met de gerealiseerde technologie.

3.1.2. Reikwijdte

- De te onderzoeken reikwijdte bestaat uit:
  - Eerste versleuteling: er wordt afgedwongen dat de eerste encryptie van de identificerende gegevens plaats vindt op locatie van de aanleverende partij.
  - Onomkeerbaar: de eerste encryptie van de identificerende gegevens (het 'Wie'-deel) dient onomkeerbaar te zijn opdat van de identificerende gegevens nergens in het verdere proces de oorspronkelijke waarden te herleiden zijn.
  - Encryptie van het 'Wat'-deel: de geïmplementeerde technologie maakt het onmogelijk om de niet-identificerende gegevens na encryptie, tot leesbare vorm te herleiden, anders dan na ontvangst bij de afnemer.
  - Genereren van keys en hashes: de geïmplementeerde technologie moet afdwingen dat hashes en public/private keys alleen door de daartoe geautoriseerde modules kan gebeuren.
  - Opslag van private keys: de geïmplementeerde technologie dwingt een veilige opslag van private keys af.
  - State of the art technologie: de gebruikte technieken en algoritmen voor encryptie zijn conform huidige stand van techniek door gebruik van 'good practices' en open standaarden.

3.1.3. Uitvoering

In dit onderzoek worden de volgende werkzaamheden uitgevoerd:

- Beoordeling van het functionele proces van pseudonimiseren van Supply tot Delivery module.
- Onderzoek naar de gebruikte Viacryp-software, de Supply module, om de volgende punten te beoordelen:
  - Wordt er daadwerkelijk een aantal logische controles uitgevoerd op de aangeboden gegevens?
  - Wordt er een scheiding afgedwongen tussen de identificerende gegevens (het 'Wie'-deel) en de bijbehorende data (het 'Wat'-deel)? Zodat nergens in de straat de gegevens in leesbare vorm aanwezig zijn, conform het volgende schema:

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

  - Is het 'Wie'-deel gehashed door middel van een one-way hashing techniek?
  - Wordt op het Supply-platform het 'Wie'-deel en 'Wat'-deel encrypted voordat de data het domein van de bron verlaat.
  - Worden beide delen op zodanige wijze beveiligd met encryptie dat het 'Wie'-deel enkel kan worden geopend door Viacryp en het 'Wat'- deel enkel kan worden geopend door de ontvangende partij?
  - De Supply module heeft mogelijkheden om de kans op (indirecte) herleidbaarheid van gegevens te verkleinen.
- Onderzoek naar de Pseudonymizer binnen het domein van Viacryp.nl
  - Pseudonymizer verifieert de authenticiteit van de aangeleverde data.
  - De pseudonymizer kan alleen het aangeleverde 'Wie'-deel decrypten om van de gehashte gegevens pseudoniemen te kunnen maken.
- Onderzoek naar de Delivery module
  - De Delivery module verifieert de authenticiteit van de aangeleverde data
  - Op het Delivery-platform worden de 'Wat'-delen gedecrypt en, indien van toepassing met de pseudoniemen, ter beschikking gesteld aan de afnemer.
- Onderzoek naar het beheer van private keys
  - Beschikken de betreffende modules over voldoende toereikende mogelijkheden om de private keys veilig te bewaren?
- Onderzoek naar de publicatie van de beschrijving van de Viacryp-oplossing:
  - Is er publiek beschikbare documentatie waarin de functionele en technische werking zodanig beschreven zijn dat betrokkenen voldoende inzicht krijgen in de wijze waarop persoons- en gedragsgegevens verwerkt worden?
  - Is de onderzochte Viacryp-oplossing gerealiseerd conform de publiek beschikbare documentatie?
- Onderzoek naar state of the art encryptie
  - Is er sprake van een periodieke en/of systematische (interne of externe) review van de gebruikte encryptietechnologie?
  - Worden de actuele ontwikkelingen op het gebied van encryptietechnologie en informatiebeveiliging op periodieke en/of systematische wijze gevolgd en vertaald naar consequenties voor de gebruikte technologie?
- Onderzoek naar professionele ontwikkelmethodieken
  - Vind softwareontwikkeling plaats volgens een geaccepteerde ontwikkelingsmethodiek, waarin alle fases van softwareontwikkeling beschreven zijn?

3.2. Onderzoek 2: Beheer van Viacryp

3.2.1. Doelstelling

De doelstelling is om aan te tonen dat er technische en organisatorische maatregelen genomen zijn die voldoende waarborgen bieden voor een veilige verwerking van persoons- en gedragsgegevens. Concreet betekent dat de technologie en organisatorische maatregelen waarborgen bieden tegen replay attacks en voorkomt dat enig persoons- of gedragsgegeven leesbaar of herleidbaar is binnen de context van de Viacrypstraat. In dit onderzoek wordt uitgegaan van de huidige

situatie van outsourcing van hosting en beheer van de technische oplossing bij een derde partij (hierna de 'hosting-leverancier' genoemd).

3.2.2. Reikwijdte

De te onderzoeken reikwijdte bestaat uit:

- Gestelde eisen aan beheerprocessen: Onderzoek of de contractering en de eisen die Viacryp aan de hosting-leverancier stelt, voldoende zekerheden bieden voor een veilige verwerking van gegevens. Het gaat hierbij om de inrichting van processen als incident, problem, change en configuration management, conform ISO 20000-1 paragraaf 8.1 incident management, 8.2 problem management, 9.1 configuration management en 9.2 change management.
    - Informatiebeveiliging: Onderzoek of de contractering en de eisen die Viacryp stelt aan de hosting-leverancier met betrekking tot de getroffen securitymaatregelen om ervoor te zorgen dat encryptie adequaat blijft. Als norm hiervoor worden de ISO 27001:2013 / ISO 27002:2013 *Norm* cq. *Praktijkrichtlijnen voor informatiebeveiliging* gebruikt. Een SOA Statement of Applicability dient te worden aangeleverd door Viacryp. De audit richt zicht op de controlemaatregelen in de Statement of Applicability. Het gaat hierbij specifiek om de paragrafen A.9.1 (Bedrijfseisen voor toegangsbeveiliging), A.10.1 (Cryptografische beheersmaatregelen), A13.2 (Informatietransport) en A.15.1 (Informatiebeveiliging in leveranciersrelaties).
- Verificatie door Viacryp: Onderzoek of Viacryp in voldoende mate heeft geverifieerd of de hosting-leverancier de gestelde eisen heeft gerealiseerd.
    - Monitoring, autorisatie, development, change- en releasemanagement, backup, conform ISO 27001 / ISO 27002 paragrafen: A.12 (Beveiliging bedrijfsvoering) en A.16.1 (Beheer van informatiebeveiligingsincidenten en -verbeteringen)

3.3. Onderzoek 3: Klantafspraken

3.3.1. Doelstelling

Doelstelling is om aan te tonen dat Viacryp met klanten goede, heldere afspraken maakt over de uit te voeren werkzaamheden. Tevens dient dit onderzoek om aan te tonen dat Viacryp een onafhankelijke positie inneemt die past bij de rol van Trusted Third Party.

3.3.2. Reikwijdte

- Worden klanten op passende wijze gewezen op risico's en verantwoordelijkheden, rekening houdend met de mate waarin de klant zelf in staat is om een gekwalificeerd oordeel te geven over de validiteit van de uit te voeren verwerking.
- Worden voldoende maatregelen beschreven op basis van 'industry good practices' en/of ervaringen van Viacryp

3.3.3. Uitvoering

In dit onderzoek worden de volgende werkzaamheden uitgevoerd:

- Verificatie van de algemene voorwaarden van Viacryp.
- Verificatie van contracten met de klanten van Viacryp.
- Verificatie van wettelijk verplichte documenten, zoals bewerkingsovereenkomsten.
- Verificatie van eventuele adviesdocumenten.

4. Het auditproces

4.1. Inleiding

In dit hoofdstuk wordt uiteengezet hoe het onafhankelijke auditonderzoek dient te verlopen. Er is rekening gehouden met de NEN-EN-ISO 19011 Richtlijnen voor het uitvoeren van audits. Een audit is een systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijsmateriaal en het objectief beoordelen daarvan om vast stellen in welke mate aan overeengekomen auditcriteria is voldaan. Deze internationale norm stelt geen eisen maar geeft richtlijnen voor het managen van een auditprogramma, het plannen en uitvoeren van een audit van het managementsysteem, en voor de competentie en beoordeling van een auditor en een auditteam.

4.2. Principes van het uitvoeren van een audit

Het uitvoeren van een audit is gebaseerd op een aantal principes. Deze principes behoren te helpen om van de audit een doeltreffend en betrouwbaar instrument te maken ter ondersteuning van beleid en beheersmaatregelen van de directie van Viacryp, door informatie te verschaffen op grond waarvan een organisatie maatregelen kan nemen om haar prestaties te verbeteren. Naleving van deze principes is een eerste vereiste voor het genereren van auditconclusies die relevant en toereikend zijn, en om auditoren in staat te stellen onafhankelijk van elkaar te werken en tot vergelijkbare conclusies in vergelijkbare omstandigheden te komen.

4.2.1. Integriteit

Integriteit: de basis van professionaliteit. Auditoren en de persoon die een auditprogramma managen behoren:

- Hun werk op eerlijke, toegewijde en verantwoordelijke wijze uit te voeren;
- Zich te houden aan geldende wettelijke eisen en deze na te leven;
- Bij de uitvoering van hun werk blijk te geven van hun competentie;
- Hun werk op onpartijdige wijze uit te voeren, dat wil zeggen altijd eerlijk en onbevooroordeeld te blijven tijdens hun aanpak;
- Alert te zijn op alle factoren die hun oordeel kunnen beïnvloeden bij het uitvoeren van een audit.

4.2.2. Eerlijke verslaglegging

Eerlijke verslaglegging is de plicht waarheidsgetrouw en nauwkeurig te rapporteren. Auditbevindingen, auditconclusies en auditrapporten behoren de auditactiviteiten waarheidsgetrouw en nauwkeurig weer te geven. Substantiële belemmeringen tijdens de audit en onopgeloste meningsverschillen tussen het auditteam en de auditee behoren te worden gerapporteerd. De communicatie behoort waarheidsgetrouw, nauwkeurig, objectief, tijdig, duidelijk en volledig te zijn.

4.2.3. Gepaste beroepsmatige zorgvuldigheid

Gepaste beroepsmatige zorgvuldigheid heeft betrekking op toewijding en oordeelsvorming bij het uitvoeren van audits.

Auditoren behoren zorgvuldig te werk te gaan, in overeenstemming met het belang van de taak die ze uitvoeren en het vertrouwen dat in hen is gesteld door Viacryp en andere belanghebbende partijen. Een belangrijke factor bij het met gepaste beroepsmatige zorgvuldigheid uitvoeren van hun werk, is het vermogen om in alle situaties die voorkomen tijdens een audit onderbouwde oordelen te kunnen vellen.

4.2.4. Vertrouwelijkheid

Het gaat hier om de beveiliging van informatie. Auditoren behoren discreet te werk te gaan bij het gebruik en de bescherming van informatie die ze tijdens hun werkzaamheden verzamelen. De auditor behoort auditinformatie niet ongepast aan te wenden voor persoonlijk voordeel of op een wijze die schadelijk kan zijn voor de legitieme belangen van de auditee. Dit begrip omvat het correct omgaan met gevoelige of vertrouwelijke informatie.

4.2.5. Onafhankelijkheid

Onafhankelijkheid is de basis voor onpartijdigheid van de audit en objectiviteit van de auditconclusies. Als het praktisch uitvoerbaar is, behoren auditoren onafhankelijk te zijn van de activiteit waarop een audit wordt uitgevoerd. Auditoren behoren in alle gevallen te handelen zonder vooringenomenheid en zonder strijdigheid van belangen. Voor interne audits behoren de auditoren onafhankelijk te zijn van de uitvoerende managers van de functie waarop de audit wordt uitgevoerd. Auditoren behoren gedurende het gehele auditproces een objectieve houding te handhaven om te waarborgen dat de auditbevindingen en de auditconclusies alleen op het auditbewijsmateriaal zijn gebaseerd.

4.2.6. Aanpak op grond van bewijs

Het doel is om betrouwbare en reproduceerbare auditconclusies te bereiken door middel van een systematisch auditproces. Auditbewijsmateriaal behoort verifieerbaar te zijn. Auditbewijsmateriaal is doorgaans gebaseerd op steekproeven van de beschikbare informatie, aangezien een audit wordt uitgevoerd gedurende een eindige tijdsperiode en met eindige middelen. Er behoort een geschikte steekproefkeuze te worden toegepast omdat dit nauw samenhangt met het vertrouwen dat in de auditconclusies kan worden gesteld.

4.3. Uitvoering van de audit

Viacryp laat de audit periodiek uitvoeren, door een onafhankelijke derde partij, binnen een door Viacryp-gedefinieerd kader. De audit heeft als doel heeft om met een onafhankelijk deskundig oordeel, de onafhankelijke en belangenvrije positie van Viacryp te bevestigen. Als Trusted Third Party opereert Viacryp als intermediair tussen leverancier(s) van originele persoonsgegevens en de afnemer van de gepseudonimiseerde gegevens.

Hieronder volgt in hoofdlijnen de werkwijze die wordt gevolgd voor het afgeven van een assurance conformiteitsverklaring.

4.4. Opstellen van een auditplan

Voorafgaand aan de onderzoeken zoals beschreven in hoofdstuk 2 zal samen met de betrokken partij (Viacryp) een auditplan worden opgesteld. Dit auditplan behoort de volgende aspecten te omvatten:

- De auditdoelstellingen;
- De reikwijdte van de audit, inclusief identificatie van organisatorische en functionele eenheden, evenals processen waarop de audit moet worden uitgevoerd;
- De auditcriteria en eventuele referentiedocumenten;
- De locaties, data, verwachte tijdstip en duur van de uit te voeren auditactiviteiten, inclusief bijeenkomsten met het management van Viacryp;
- De auditmethoden die worden gebruikt, inclusief de omvang waarin het nemen van steekproeven nodig is om voldoende auditbewijsmateriaal te verkrijgen, en het ontwerp van het steekproefschema, indien van toepassing;
- De taken en verantwoordelijkheden van de auditteamleden, begeleiders en waarnemers;
- De toewijzing van toepasselijke middelen aan kritische onderdelen van de audit.

- Contactpersoon waar klachten ingediend kunnen worden;

4.5. Informatie verzamelen en verifiëren

Gedurende de audit behoort door middel van geschikte steekproeven informatie te worden verzameld en geverifieerd die relevant is voor de doelstellingen, reikwijdte en criteria van de audit, inclusief informatie die betrekking heeft op de raakvlakken tussen functies, activiteiten en processen. Alleen verifieerbare informatie behoort als auditbewijsmateriaal te worden geaccepteerd. Auditbewijsmateriaal dat tot auditbevindingen leidt, behoort te worden geregistreerd. Als het auditteam tijdens het verzamelen van bewijsmateriaal verneemt dat er nieuwe of veranderde omstandigheden of risico's zijn, behoren deze als zodanig door het team te worden behandeld.

Methoden om informatie te verzamelen zijn onder meer:

- Interviews;
- Waarnemingen;
- Beoordeling van documenten, inclusief registraties.

4.6. Auditbevindingen formuleren

Auditbewijsmateriaal behoort te worden beoordeeld aan de hand van auditcriteria om auditbevindingen vast te stellen. Auditbevindingen kunnen duiden op conformiteit met of afwijking van de auditcriteria. Als dit in het auditplan is gespecificeerd behoren de afzonderlijke auditbevindingen ook conformiteit en 'good practices' te omvatten, met het bewijsmateriaal hiervoor, mogelijkheden voor verbetering en eventuele aanbevelingen voor de auditee.

Afwijkingen en het bijbehorende auditbewijsmateriaal behoren te worden geregistreerd. Het schrijven van een afwijking door de auditor gebeurt volgens het eis-afwijking-bewijs principe. Afwijkingen kunnen worden geclassificeerd. Afwijkingen behoren te worden besproken met de auditee om bevestiging te verkrijgen dat het auditbewijsmateriaal nauwkeurig is en dat de afwijkingen worden begrepen. Men behoort zich optimaal in te zetten om eventuele meningsverschillen met betrekking tot het auditbewijsmateriaal of de auditbevindingen op te lossen, en onopgeloste problemen behoren te worden geregistreerd. Indien verschillen worden aangetroffen maakt het toetsingskader onderscheid in twee soorten bevindingen:

- Non-conformiteit: een materiële tekortkoming ten opzichte van de auditeisen. Indien sprake is van één of meerdere non-conformiteiten, dan dienen deze te worden opgelost dan wel zal de audit niet met een positief resultaat kunnen worden afgerond.
- Observatie: Een waarneming van de auditor die betrekking heeft op mogelijke verbeterpunten of optimalisaties, maar heeft geen betrekking heeft op de auditeisen. Observaties leiden dus niet tot non-conformiteiten.

Bij de toetsing kunnen min of meer ernstige tekortkomingen worden gesignaleerd. Afhankelijk van de ernst van de gesignaleerde tekortkomingen zal de auditor vaststellen of het om een major dan wel om een minor non-conformiteit gaat (categorisatie van bevindingen). Minor non-conformiteiten corresponderen doorgaans met beperkte risico's. Meerdere minor non-conformiteiten kunnen door de auditor gelijk worden gesteld aan een major non-conformiteit, dit op basis van zijn professional judgement, overwegende de ernst van de afwijking. Zowel minor NC's als major NC's dienen binnen 13 weken, aantoonbaar met bewijslast, te worden opgelost.

Voor elke observatie zal Viacryp een afweging maken of deze zal worden opgevolgd of niet.

4.7. Opvolgingsonderzoek (Follow-up audit)

Afhankelijk van de auditdoelstellingen kunnen de conclusies van de audit erop duiden dat correcties nodig zijn of corrigerende of preventieve maatregelen, of maatregelen voor verbetering. Gewoonlijk neemt de auditee een besluit over

deze maatregelen en voert ze uit binnen een overeengekomen tijdsbestek. De auditee behoort de persoon die het auditprogramma managet en het auditteam op de hoogte te houden van de status van deze maatregelen, voor zover van toepassing. De voltooiing en doeltreffendheid van deze maatregelen behoren te worden geverifieerd. Deze verificatie kan deel uitmaken van een vervolgaudit.

4.8. Auditrapportage

Van de initiële beoordeling zal een auditrapportage worden gemaakt conform de Risk Based Certification™ MSC rapportage van DNV GL. Hierin kunnen mogelijkheden tot verbetering en positieve indicaties worden opgenomen, maar in de rapportage zullen geen specifieke oplossingen worden opgenomen. De rapportage zal een duidelijke en beknopte vastlegging zijn van het uitgevoerde onderzoek. Uit deze vastlegging moet duidelijk zijn of de betreffende audit al dan niet met een positief resultaat is afgerond.

Het auditrapport behoort een volledige, nauwkeurige, bondige en duidelijke weerslag van de audit te

vormen, en behoort de volgende aspecten te omvatten of hiernaar te verwijzen:

a. De auditdoelstellingen;
b. De reikwijdte van de audit, in het bijzonder de identificatie van de organisatorische en functionele eenheden of processen waarop de audit is uitgevoerd;
c. Identificatie van de auditklant;
d. Identificatie van het auditteam en de deelnemers van de auditee aan de audit;
e. De data waarop, en de locaties waar de auditactiviteiten zijn uitgevoerd;
f. De auditcriteria;
g. De auditbevindingen en het bijbehorende bewijsmateriaal;
h. De auditconclusies;
i. Een verklaring waarin staat in welke mate aan de auditcriteria is voldaan.

De rapportage van het onderzoek zal worden afgestemd met Viacryp en zal in finale vorm slechts worden verstrekt aan Viacryp; het is aan Viacryp of deze wordt verstrekt aan de Afnemer. Viacryp en Afnemer kunnen het assurance-rapport en de bijbehorende rapportage aanbieden aan het CBP ter onderbouwing van hun conformiteit. Partijen mogen het assurance-rapport publiceren, bijvoorbeeld op hun website. Dit laatste geldt niet voor de bijbehorende auditrapportage; verstrekking aan andere partijen van de auditrapportage kan slechts geschieden na afstemming met de auditor.

Bijlage A.1. Afkortingen en definities

Hieronder volgt een lijst met afkortingen, die worden gebruikt in dit document, en de daarbij behorende betekenis:

Afkorting	Betekenis
AP	Authoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming. Europese wetgeving, vervangt per 18 mei 2018 de Nederlandse Wet Bescherming Persoonsgegevens.
CBP	College Bescherming Persoonsgegevens (oude naam van de Authoriteit Persoonsgegevens)
GDPR	General Data Protection Regulation Engelse naamgeving voor de AVG
ISO	International Organization for Standardization
SOA	Statement of Applicability ook wel toepasselijkheidsverklaring
TTP	Trusted Third Party
WBP	Wet bescherming persoonsgegevens
XML	Extensible Markup Language

Verder volgt hier een lijst met definities met bijbehorende omschrijving:

Begrip	Omschrijving
Aanbieder	Partij, die persoonsgegevens aanlevert aan Viacryp
Afnemer	Partij, die gebruik maakt van de door Viacryp gepseudonimiseerde gegevens.
Afwijking	Niet voldoen aan een eis
Anonimiseren	Het proces waarmee de relatie tussen de identificerende data en de individu wordt verwijderd.
Audits	Systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijsmateriaal en het objectief beoordelen daarvan om vast te stellen in welke mate aan de auditcriteria is voldaan. Drie typen audits worden in dit document onderscheiden, namelijk: (1) initiële beoordeling (ook wel initiële audit): dit zijn de eerste audits die zich concentreren op opzet en bestaan van maatregelen in conformiteit met de Viacryp criteria; (2) herhalingsonderzoek: dit zijn de audits, die jaarlijks worden uitgevoerd nadat de initiële audit is uitgevoerd, ook wel herhalingsaudits genoemd die concentreren zich op de werking van de maatregelen onderzocht tijdens de initiële beoordeling over de afgelopen periode, en; (3) opvolgingsonderzoek: audits naar correctieve acties naar aanleiding van geconstateerde non-conformiteiten bij initiële of jaarlijkse audits;

Begrip	Omschrijving
	(4) herbeoordeling: dit is een audit die wordt uitgevoerd als het object van onderzoek essentieel wijzigt.
Auditcriteria	Geheel van beleidslijnen, procedures of eisen dat wordt gebruikt als referentie waaraan auditbewijsmateriaal wordt getoetst.
Auditbewijsmateriaal	Registraties, beweringen op basis van feiten of andere informatie welke relevant zijn voor de auditcriteria en verifieerbaar.
Auditbevindingen	Resultaten van de beoordeling van het verzamelde auditbewijsmateriaal aan de hand van auditcriteria.
Auditconclusie	Resultaat van een audit, na overweging van de auditdoelstellingen en alle auditbevindingen.
Auditklant	Organisatie of persoon die een audit aanvraagt.
Auditee	Organisatie die een audit ondergaat.
Auditor	Persoon die een audit uitvoert.
Auditteam	Een of meer auditoren die een audit uitvoer(t)(en), indien nodig ondersteund door technisch deskundigen.
Auditplan	Beschrijving van de activiteiten en voorzieningen voor een audit .
Begeleider	Persoon die door de auditee is aangewezen om het auditteam te assisteren.
Chinese Wall	Scheiding tussen de gepseudonimiseerde gegevens en de overige gegevens.
Competentie	Vermogen om kennis en vaardigheden toe te passen om de beoogde resultaten te bereiken.
Conformiteit	Voldoen aan een eis.
Delivery module	Doelmodule die zorg draagt voor het afleveren van de data bij de afnemer.
Klanten	Combinatie van aanbieders en afnemer binnen één Viacrypstraat .
Major non-conformiteit	Een materiële tekortkoming ten opzichte van de van Viacryp voorwaarden. Indien niet aan de Viacryp criteria wordt voldaan, dan is sprake van een major non-conformiteit. Indien sprake is van één of meerdere non-conformiteiten, dan dienen deze te worden opgelost dan wel zal de audit niet met een positief resultaat kunnen worden afgerond.
Minor non-conformiteit	Een niet-materiële tekortkoming ten opzichte van de Viacryp criteria.
Viacrypstraat	Elke straat kent één of meerdere aanbieders van persoonsgegevens en één afnemer van de gepseudonimiseerde resultaten. Viacryp verzorgt daarbij de pseudonimisering van de persoonsgegevens afkomstig van de Aanbieder(s) en levert deze uit aan de Afnemer.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor

Begrip	Omschrijving
	de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (AVG Art. 4, lid 1).
Pseudonimiseren	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 (AVG Art.1, lid 5).
Pseudonymizer	Centrale Module TTP waarbinnen de pseudonimisering van de data plaatsvindt.
Replay attack	Een onrechtmatige inbreuk op een informatiesysteem bedoeld om inzicht te krijgen in de relatie tussen identificerende persoonsgegevens en de gebruikte pseudoniemen.
Reikwijdte van de audit	Toepassingsgebied en grenzen van een audit.
Risico	Effect van onzekerheid op het behalen van doelstellingen.
Supply module	Verzendmodule voor de aanbieder waarin het splitsen van de data alsmede het versleuteld verzenden van de data plaatsvindt.
Technisch deskundige	Persoon die specifieke kennis of deskundigheid aan het auditteam levert.
Toepasselijkheidsverklaring	Document waarin aangegeven wordt welke maatregelen zijn getroffen in het kader van de NEN-ISO 27002 “Code voor informatiebeveiliging” en SOA ISO 27001.
Verwerken	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens (AVG Art. 1, lid 2).
Waarnemer	Persoon die het auditteam vergezelt, maar geen audits uitvoert.

Bijlage A.2. Te gebruiken controls voor het auditraamwerk

ISO 27001:2013
A.9.1 Bedrijfseisen voor toegangsbeveiliging **Doelstelling:** Toegang tot informatie en informatieverwerkende faciliteiten beperken.
A.9.1.1 Beleid voor toegangsbeveiliging **Beheersmaatregel:** Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
A.10.1 Cryptografische beheersmaatregelen **Doelstelling:** Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.
A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen **Beheersmaatregel:** Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.
A.10.1.2 Sleutelbeheer **Beheersmaatregel:** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.
A.12.1 Bedieningsprocedures en verantwoordelijkheden **Doelstelling:** Correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen.
A.12.1.2 Wijzigingsbeheer **Beheersmaatregel:** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.
A.12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen **Beheersmaatregel:** Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.
A.12.3 Back-up **Doelstelling:** Beschermen tegen het verlies van gegevens.
A.12.3.1 Back-up van informatie **Beheersmaatregel:** Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.
A.12.4 Verslaglegging en monitoren **Doelstelling:** Gebeurtenissen vastleggen en bewijs verzamelen.

A.12.4.1 Gebeurtenissen registreren

Beheersmaatregel:

Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.

A.12.4.2 Beschermen van informatie in logbestanden

Beheersmaatregel:

Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.

A.12.4.3 Logbestanden van beheerders en operators

Beheersmaatregel:

Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.

A.13.2 Informatietransport

Doelstelling:

Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.

A.13.2.1 Beleid en procedures voor informatietransport

Beheersmaatregel:

Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.

A.13.2.2 Overeenkomsten over informatietransport

Beheersmaatregel:

Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.

A.13.2.3 Elektronische berichten

Beheersmaatregel:

Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.

A.13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst

Beheersmaatregel:

Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.

A.15.1 Informatiebeveiliging in leveranciersrelaties

Doelstelling:

De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.

A.15.1.1 Informatiebeveiligingsbeleid in leveranciersrelaties

Beheersmaatregel:

Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.

A.16.1 Beheer van informatiebeveiligingsincidenten en –verbeteringen

Doelstelling:

Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen in zwakke plekken in de beveiliging.

	A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen **Beheersmaatregel:** Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.
ISO20000-1	8.1 Incident management 8.2 Problem management 9.1 Configuration management 9.2 Change management

Bijlage A.3. Indicatieve lijst van onderwerpen per onderzoek

Onderzoek	Mogelijk te signaleren tekortkomingen
1	• Er wordt geen gebruik gemaakt van pseudonimisering • Private keys worden niet daadwerkelijk door de eigenaren aangemaakt • De pseudonimisering opzet voldoet niet aan de 'good practice' van de encryptie technologie (onvoldoende vakkundig) • De eerste stap van de encryptie vindt niet plaats bij de aanbieder van de gegevens • De eerste stap van de encryptie is omkeerbaar, zonder gebruik te maken van additionele bestanden • De pseudonimisering is niet adequaat geïmplementeerd in de code • De geïmplementeerde oplossing is niet consistent met de beschreven oplossing • Er is geen beheerproces ingericht • Het beheerproces vertoont tekortkomingen • De wijze waarop de organisatie kennis vergaard over actuele ontwikkelingen op het gebied van encryptie en informatiebeveiliging is onvoldoende of ad hoc.
2	• De maatregelen die genomen zijn in het kader van informatiebeveiliging zijn dusdanig dat ongeautoriseerde personen mogelijk in staat zijn de versleuteling te herleiden. • De maatregelen welke genomen zijn in het kader van informatiebeveiliging zijn dusdanig dat geautoriseerde personen (te kwader trouw) mogelijk in staat zijn de versleuteling te herleiden. • De afspraken met de hostingpartij zijn onvoldoende helder of worden niet geverifieerd.
3	• De algemene voorwaarden zijn onvoldoende specifiek • Er zijn geen bewerkingsovereenkomsten met klanten afgesloten • Er zijn geen sluitende afspraken gemaakt tussen aanbieders en afnemer met Viacryp

Bijlage A.4. *Encryptie technieken*

Type	Algoritme
Asymmetric encryption	RSA-2048
Symmetric encryption	AES-256-GCM
Signing	SHA-256 with RSA
Hashing	HMAC-SHA-512