Gemeente Delft

GEMEENTEBLAD

Officiële uitgave van de gemeente Delft

Nr. 290734

5 juli

2023

Privacy Protocol Ondermijning

1 Inleiding

1.1 Algemeen

Het Privacy Protocol (vanaf nu: Protocol) is een afwegingskader voor de binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondermijnende criminaliteit in de gemeente Delft. In het Protocol is de aanpak Ondermijning van de gemeente in relatie tot de Algemene Verordening Gegevensbescherming (vanaf nu: AVG) beschreven.

1.1.1 Het doel van het Protocol

Het Protocol[1] beschrijf hoe binnen de gemeente Delft omgegaan wordt met persoonsgegevens binnen de aanpak Ondermijning. Dit Protocol bevat de waarborgen voor de aanpak van ondermijnende criminaliteit binnen de wet- en regelgeving op het gebied van privacy.
Uitgangspunten hierbij zijn:

- Fasering in het proces, waarbij stapsgewijs expliciete wegingen plaatsvinden: proportionaliteit door voorkomen van bovenmatig gebruik van persoonsgegevens;
- Transparantie: vaststellen van dit Protocol waarbij zichtbaar en inzichtelijk wordt voor betrokkene met welk doel en op welke wijze de gemeente Delft zijn of haar persoonsgegevens verwerkt;
- Noodzaak: zicht krijgen op waar ondermijning binnen de grenzen van de gemeente aanwezig is.

1.1.2 Evaluatie/ PDCA

Na vaststelling van het Protocol zal de gemeente periodiek evalueren of in de praktijk ook conform het Protocol wordt gehandeld. Daarnaast zal jaarlijks beoordeeld worden of het Protocol, de werkprocesbeschrijving inclusief bijlagen of de werkwijze moeten worden gewijzigd.

1.1.3 Leeswijzer

Hoofdstuk twee geeft een beschrijving van de aard van de ondermijnende criminaliteit en de noodzaak van de aanpak ondermijning. In hoofdstuk drie wordt ingegaan op de algemene bepalingen van het Protocol. In de hoofdstukken daarna zal per fase van het ondermijningsproces ingegaan worden op specifieke handelingen voor dit deel van het proces.

2 Aanpak van ondermijning

2.1 Wat is ondermijning?

Dit document bevat de stapsgewijze beschrijving van het gemeentelijke proces voor de aanpak van ondermijnende criminaliteit[2]. Hieronder wordt verstaan:

- georganiseerde criminaliteit; zij het vooral georganiseerd in flexibele netwerken en niet zozeer in hiërarchieën;
- waarmee meestal grote hoeveelheden geld worden verdiend;
- waarbij de criminele activiteiten en de gehanteerde methodes kunnen wisselen. Zij worden bepaald door winstgevendheid en de kans om onopgemerkt te blijven;
- waarbij de grote winsten worden gebruikt om de bovenwereld te ondermijnen (witwaspraktijken, normvervaging binnen gemeenschappen en wijken, inschakeling van advocaten, accountants en notarissen);
- waarbij de ondermijnende criminaliteit ook dreigt door te werken naar de overheid; corruptie, aantasting van integriteit;
- tevens sprake moet zijn van geweld, bedreiging en intimidatie.

2.2 Noodzaak aanpak ondermijning

Gemeenten hebben een belangrijke rol in de aanpak van ondermijning. De combinatie van omvangrijke criminele vermogens - verdiend met het plegen van strafbare feiten - en de toegang tot zware gewelds-

1) Dit Protocol is ontwikkeld op basis van het Model Privacy Protocol. De aanleiding voor het model Protocol is de voorlichting van de Afdeling advisering van de Raad van State van 20 maart 2019 over de rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning. De Afdeling adviseerde onder meer om te voorzien in een gemeentelijk model Privacy Protocol voor binnengemeentelijke gegevensuitwisseling rond ondermijnende criminaliteit.

2) Voor de definitie van georganiseerde criminaliteit wordt aangesloten bij de criteria in het "Het model Privacy Protocol - Handleiding binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondermijnende criminaliteit. Vooruitlopend op de WGS en de hierbij behorende Memorie van Toelichting, is daar een extra criterium aan toegevoegd, namelijk: " sprake van geweld of intimidate".

middelen stelt criminele netwerken in staat invloed te verwerven in maatschappelijke sectoren. Crimineel geld kan vanuit de onderwereld in de bovenwereld worden benut om maatschappelijk aanzien te verwerven, bijvoorbeeld door winkels, bedrijven of horecaondernemingen op te zetten[3]. Door de verwevenheid tussen de onder- en bovenwereld is het ook mogelijk dat de overheid ondermijnende activiteiten onbewust faciliteert middels subsidies, vergunningen, uitkering, etc. Dit leidt tot aantasting van de integriteit van de overheid. Het is daarom van belang dat ondermijning proactief, preventief en actief wordt aangepakt door de gemeente Delft.

2.3 Verwerkingsdoeleinden
Het doel van de binnengemeentelijke, bestuurlijke en geïntegreerde aanpak van ondermijnende criminaliteit is:
- ondermijnende activiteiten en gelegenheidsstructuren signaleren en analyseren;
- voorkomen dat de gemeente criminelen of criminele organisaties bewust of onbewust faciliteert en daardoor de democratische rechtstaat wordt ondermijnd;
- vroegtijdig kunnen signaleren en interveniëren door bestuurlijke interventies;
- onrechtmatigheden en maatschappelijke bedreigingen veroorzaakt door criminele activiteiten voorkomen, en daarmee bedreigingen voor de leefbaarheid en openbare orde in de gemeente voorkomen

2.4 De integrale aanpak
Om de minder zichtbare aspecten van criminaliteit zichtbaar(der) te maken, wijzen diverse onderzoeken uit dat het ondermijningsvraagstuk integraal en gebiedsgericht benaderd moet worden om tot een goede informatiepositie en tot resultaten te komen[4].

Een integrale aanpak van ondermijning heeft onder andere de volgende doelen:
- Ondermijnende activiteiten signaleren en analyseren;
- Voorkomen dat de gemeente ondermijnende activiteiten faciliteert;
- Vroegtijdig signaleren en interveniëren middels een bestuurlijke aanpak;
- Onrechtmatigheden en maatschappelijke bedreigingen, veroorzaakt door criminele activiteiten voorkomen, en daarmee bedreigingen voor de leefbaarheid en openbare orde in de gemeente voorkomen.

2.5 Rollen
In het proces zijn de volgende rollen / teams betrokken:

Coördinator VIK
- Verantwoordelijk voor de PDCA-cyclus van het proces Ondermijning en daarmee de periodieke evaluatie van dit Protocol.
- Verantwoordelijk voor het periodiek laten uitvoeren van een Data Protection Impact Assessment (DPIA).
- Bij verschil van inzicht tussen de Analist Ondermijning en de Privacy Officer beslist de Coördinator VIK en documenteert de gemaakte afweging.
- Stuurt de jaarlijkse rapportage aan de Functionaris Gegevensbescherming met daarin minimaal het aantal uitgevoerde privacycheck met uitkomst (go / no-go) en het aantal afwijkingen van het advies van de Privacy Officer.Indien gewenst kan de functionaris Gegevensbescherming de onderbouwing kan opvragen.

Analist Ondermijning
- Het managen en sturen van het informatieproces van lopende signalen;
- Het vertalen van het beoogd effect bij het vaststellen van een signaal naar ontwerp van een onderzoek (intelligence vraagstuk);
- Het vertalen van het intelligence vraagstuk naar een concrete informatiebehoefte;
- Het uitzetten van de informatievragen middels verzoeken tot informatie;
- Het ontvangen en controleren van de ontvangen informatie.
- Het analyseren van de ontvangen informatie en vertalen naar een intelligence of informatieproduct;
- Informatiestructuren beschikbaar stellen voor het gebruik in de ondersteunende analyse tooling door de analist;
- Informatie visualiseren in bruikbare vorm, zoals hot spot kaarten, dashboards e.d.
- Opstellen plan van aanpak en deze aanpassen gedurende de casus.

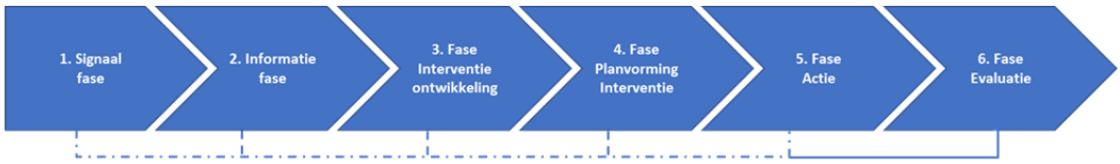
3) Tops, van der Torre, Wijk en aanpak en ondermijnende criminaliteit', a.w. 2014, p.38 e.v.
4) M. van der Steen e.a., Ondermijning ondermijnd. Hoe het rijk meer ruimte kan maken voor een (boven)lokale aanpak van georganiseerde ondermijnende criminaliteit, Den Haag

Privacy Officer
- Adviseert welke persoonsgegevens opgevraagd mogen worden bij een Hit / No hit.
- Adviseert welke persoonsgegevens gedeeld mogen worden met het GSO.
- Adviseert welke persoonsgegevens opgevraagd mogen worden tijdens een casus op basis van het plan van aanpak.
- De Privacy Officer controleert in de verschillende stadia van het proces of het gebruik van de gegevens verenigbaar is met het oorspronkelijke doel en of het gebruik noodzakelijk is en voldoet aan de proportionaliteits- en subsidiariteitsvereiste.
- Opstellen Hit / No hit gegevensset voor specifieke ondermijningsthema's.
- Draagt zorgt voor de informatieverstrekking aan de betrokkenen (Artikel 10. Recht op informatie).
- Is het aanspreekpunt voor Juridisch Zaken bij afhandelen van verzoeken van betrokkenen (Artikel 11. Rechten van betrokkenen).

Functionaris Gegevensbescherming
- Beoordelen uitgevoerde DPIA's
- Geven second opinion indien daarom gevraagd wordt.

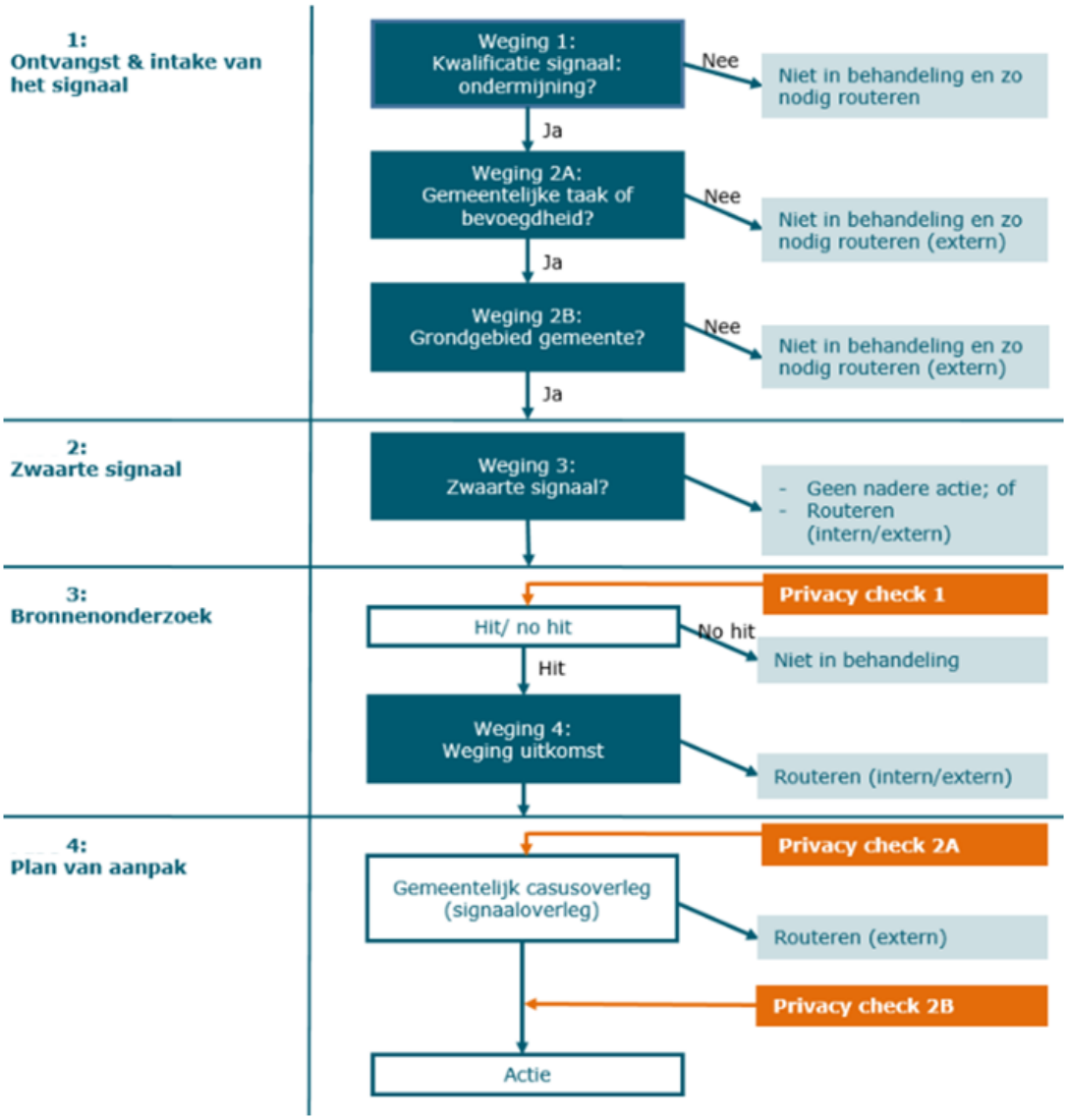
Gemeentelijk Signalen Overleg (GSO)
- Het GSO verwerkt, weegt en toetst de signalen;
- Het GSO besluit om een signaal te benoemen tot casus;
- Het GSO voert de inhoudelijke en operationele coördinatie op de lopende casuïstiek;
- Het GSO evalueert de afgesloten casuïstiek t.b.v. het doorvoeren van lessons learned.
- Het GSO beoordeelt en besluit wanneer een interventie gepleegd zal worden en wanneer een casus wordt afgerond.

2.6 Proces
Het Protocol gaat over het gehele ondermijningsproces van de Signaal fase t/m de evaluatie fase.



De inrichting van het proces en dit Protocol is in lijn met het Model privacy Protocol binnengemeentelijke gegevensdeling[5] van het Ministerie van Justitie en Veiligheid. Dit Protocol wijkt niet af van het Model Privacy Protocol maar geeft daar waar nodig aanvullende informatie die specifiek is voor de Delftse situatie. Het Model Privacy Protocol beperkt zich ook tot het begin van het Ondermijningsproces (Signaal fase en deels Informatie fase). Dit Protocol gaat verder. Daar waar in het Model Privacy Protocol gesproken wordt over "fase of fases" wordt in dit Protocol gesproken over "stap of stappen". Dit om eventuele verwarringen met het de fases uit het gehele ondermijningsproces te voorkomen.

5) https://www.rijksoverheid.nl/documenten/rapporten/2022/10/27/model-privacy-protocol-binnengemeentelijke-gegevensdeling



3 Algemene bepalingen

Artikel 1. Doel van het Protocol

De aanpak Ondermijning dient met inachtneming van privacy wet- en regelgeving plaats te vinden. Dit Protocol bevat de benodigde waarborgen om dat te realiseren. Dit Protocol beschrijft hoe er gewerkt wordt binnen de aanpak Ondermijning conform de privacy wet- en regelgeving. Daarnaast biedt dit Protocol een betrokkene inzicht in de wijze waarop de gemeente Delft bij deze aanpak zijn/haar persoonsgegevens verwerkt en met welk doel dat gebeurt.

Artikel 2. (Verwerkings)verantwoordelijke

a. De gegevensverwerkingen die plaatsvinden in het kader van de aanpak van ondermijnende criminaliteit zal worden uitgevoerd in het kader van openbare orde taken en bevoegdheden. Deze taken en bevoegdheden vallen onder de verwerkingsverantwoordelijkheid van de Burgemeester.
b. De Burgemeester is hiermee ook eindverantwoordelijk (Accountable) voor de verwerking.
c. Het hoofd van de afdeling Advies, Cluster Veiligheid van de gemeente Delft draagt de dagelijkse verantwoordelijkheid (Responsible) voor de verwerking. Het hoofd draagt zorg voor het dagelijks beheer van de verwerking, waaronder de beveiliging van de persoonsgegevens, de informatieverstrekking aan betrokkene en de ondersteuning bij de afhandeling van de door betrokkene uitgeoefende rechten.

Artikel 3. Grondslag voor de verwerking
De grondslag voor de verwerking is dat de gegevensverwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (artikel6.e AVG). De wettelijke onderbouwing hiervoor is terug te vinden in artikel 172 Gemeentewet. Per casus vinden privacychecks plaats om te bepalen of de verwerking noodzakelijk is en of er wordt voldaan aan subsidiariteit en proportionaliteit.

Artikel 4. De verwerkte persoonsgegevens
Van de melders worden uitsluitend de in het signaal opgenomen persoonsgegevens verwerkt ten behoeve van communicatie met de melder dat het signaal in goede orde is ontvangen. Daarna worden de persoonsgegevens direct verwijderd.

Artikel 5. Categorieën van ontvangers
Voor zover noodzakelijk voor de in paragraaf 2.3 genoemde doelen, kunnen gegevens (signaal en aanvullingen uit open bronnen) worden verstrekt aan gemeentelijke onderdelen ten behoeve van een plan van aanpak, voor zover zij die behoeven voor de uitvoering van hun wettelijke taak.

Artikel 6. Beveiliging van persoonsgegevens
a. Het hoofd van de afdeling Advies, Cluster Veiligheid draagt zorg voor passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
b. Alle verwerkingen (inzage, aanmaken, wijzigingen, verwijderen) worden gelogd.
c. Autorisaties zijn vastgelegd in een autorisatiematrix en wijzigingen hierin worden gelogd.

Artikel 7. Bewaartermijn
Het uitgangspunt is dat de persoonsgegevens alleen worden bewaard voor zover dat noodzakelijk is voor de geformuleerde doelstellingen.
a. Persoonsgegevens die bij een signaal verwerkt zijn die niet verder gaat dan stap 1, worden binnen 2 weken na constatering vernietigd. Het signaal zelf blijft bewaard, maar alle persoonsgegevens worden eruit verwijderd.
b. Persoonsgegevens die bij een signaal verwerkt zijn die niet leiden tot een daadwerkelijke casus (stap 4) worden maximaal 1 jaar bewaard en daarna vernietigd, Het signaal zelf blijft bewaard, maar alle persoonsgegevens worden eruit verwijderd.
c. De persoonsgegevens worden na beëindigen van een casus 5 jaar bewaard in een niet actieve omgeving en daarna vernietigd. De gehele casus wordt vernietigd.
d. Logbestanden worden maximaal 5 jaar bewaard en nooit langer dan het signaal of casus waarop de logging betrekking heeft.

Artikel 8. Vastleggen van informatie
a. Alle informatie die wordt verzameld wordt vastgelegd en opgeslagen in PGAx.
b. Alle wegingen, privacychecks en beslissingen worden gemotiveerd vastgelegd en opgeslagen in PGAx.
c. Afwijkingen van adviezen van de Privacy Officer worden gemotiveerd vastgelegd in PGAx.

Artikel 9. Controle en Audit
a. Jaarlijks rapporteert de afdeling aan de Functionaris Gegevensbescherming het aantal uitgevoerde privacycheck met uitkomst (go / no-go); Het aantal afwijkingen van het advies van de Privacy Officer.
b. Minimaal om de 3 jaar wordt er een DPIA uitgevoerd op de verwerking van persoonsgegevens binnen het proces. Of vaker indien de Privacy Officer of Functionaris Gegevensbescherming dit wenselijk acht.
c. Bij het uitvoeren van de DPIA wordt minimaal 10% van de uitgevoerde privacychecks en eventuele afwijkingen getoetst.

Artikel 10. Recht op informatie
a. Betrokkenen worden via de website van de gemeente Delft geïnformeerd over de verwerking en hun rechten en plichten.
b. Indien bronnenonderzoek heeft plaatsgevonden (stap 3), maar dit niet heeft geleid tot een casus wordt de betrokkene hierover over geïnformeerd.

c. Indien bronnenonderzoek heeft plaatsgevonden (stap 3) en dit leidt tot een casus wordt de betrokkenen hierover geïnformeerd.
d. De plicht tot Informeren kan uitgesteld worden indien dit niet kan i.v.m.de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid door een andere afdeling of organisatie. Bijvoorbeeld als het informeren het casusonderzoek zou verstoren.
e. Indien gebruik wordt gemaakt van artikel 10 lid d, dient dit gemotiveerd vastgelegd te worden door het GSO en wanneer zij verwachten dat betrokkene wel geïnformeerd kan worden, alsook van welke omstandigheden dit afhankelijk is, hoe periodiek wordt getoetst of deze omstandigheden nog aanwezig zijn en hoe dan wel wanneer Betrokkene geïnformeerd zal worden.
f. Informeren van de betrokkene dient uiterlijk 3 maanden voor het verlopen van bewaartermijn te hebben plaatsgevonden om betrokkene de mogelijkheid te geven om zijn rechten uit oefenen.

Artikel 11. Rechten van betrokkenen

a. De rechten van betrokkene, zoals het recht op inzage in zijn gegevens, het verbeteren, aanvullen, verwijderen of afschermen van gegevens indien die feitelijk onjuist zijn, het recht op bezwaar, etc., worden door de verwerkingsverantwoordelijke uitgeoefend overeenkomstig de artikelen 15 tot en met 22 van de Algemene Verordening Gegevensbescherming (AVG)
b. De verzoeken als bedoeld in lid a van dit artikel, kunnen worden ingediend via de website van de gemeente Delft of schriftelijk bij Juridische Zaken
c. De Privacy Officer fungeert als aanspreekpunt voor de afdeling Juridische Zaken en levert indien nodig de benodigde informatie aan.

4 Signaal fase

Het proces van het signaleren en aanpakken van signalen van ondermijnende activiteiten verloopt met het oog op proportionaliteit en subsidiariteit in vier stappen. Daarbij geldt dat de beoordeling van een binnengekomen signaal het startpunt van het Protocol vormt. Er wordt in dit Protocol dan ook tot uitgangspunt genomen dat het delen van signalen met het VIK op rechtmatige wijze geschiedt. Vanzelfsprekend zal een verstrekker van een signaal wel steeds moeten vaststellen of die verstrekking in lijn is met de privacyregelgeving.

4.1 Stap 1 – Ontvangst & intake van het signaal

Stap 1 heeft betrekking op de ontvangst en de intake van een signaal. Een signaal kan op verschillende manieren binnenkomen:

- via een telefonische, schriftelijke (vaak digitale) melding van een burger of professional
- via Meld Misdaad Anoniem
- via een binnengemeentelijk signaal afkomstig van een afdeling van de gemeente

Artikel 12. Eerste weging

Het signaal wordt na ontvangst beoordeeld door de Analist Ondermijning. Voor de beoordeling van een signaal is van belang wat het signaal inhoudt en of het betrekking heeft op ondermijning. Een signaal wordt bij intake beoordeeld op grond van een aantal kenmerken en indicatoren.

a. Het signaal wordt beoordeeld op basis van de checklist zoals uitgewerkt in bijlage 1 van de werkprocesbeschrijving Ondermijning.
b. Indien uit de eerste weging blijkt dat er mogelijk sprake is van ondermijning wordt doorgegaan met de tweede weging.
c. Indien uit de eerste weging blijkt dat er geen sprake is van ondermijning worden de gegevens vernietigd conform artikel 7a; of
d. Doorgezet naar een andere afdeling van de gemeente indien er geen sprake is van ondermijnende activiteiten maar wel van overige onrechtmatigheden die betrekking heeft op deze afdeling.
e. Indien lid d van toepassing is, wordt na doorzetting de persoonsgegevens vernietigd uit de ondermijningssystemen conform artikel 7a.

Artikel 13. Tweede weging (2a)

De Analist Ondermijning beoordeelt of het signaal een taak of bevoegdheid van de gemeente is en niet op een taak of bevoegdheid van een andere instantie (bijvoorbeeld van de politie, belastingdienst, etc.). Het is hierbij dus van belang na te gaan of het signaal in beginsel tot gemeentelijk optreden kan leiden. Een dergelijke gemeentelijke taak is bijvoorbeeld een van de openbare orde bevoegdheden van de burgemeester.
Vervolgens zijn er twee opties:

a. Er wordt vastgesteld of het signaal aanleiding vormt voor de inzet van een gemeentelijke taak of bevoegdheid.
b. Indien het signaal een aanleiding vormt voor de inzet van een gemeentelijke taak of bevoegdheid wordt doorgegaan met weging 2b.
c. Indien uit weging 2a blijkt dat er het signaal geen aanleiding vormt voor de inzet van een gemeentelijke taak of bevoegdheid worden de gegevens vernietigd conform artikel 7a; of
d. Doorgezet naar een andere bevoegde instantie.
e. Indien lid d van toepassing is, wordt na doorzetting de persoonsgegevens vernietigd uit de ondermijningssystemen conform artikel 7a.

Artikel 14. Tweede weging (2b)

De Analist Ondermijning beoordeelt of het signaal betrekking heeft op het grondgebied van de gemeente. Het gaat, met andere woorden, om de vraag of het subject of object waar het signaal betrekking op heeft binnen de gemeente woont respectievelijk is gevestigd. De volgende vragen moeten daarbij achtereenvolgend worden beantwoord:

- Gaat het om een object of een subject?
- In het geval van een object: is het object binnen de gemeentegrenzen gelegen (dan wel is er anderszins een link met de gemeente)?
- In het geval van een subject: is het subject woonachtig binnen de gemeentegrenzen (dan wel is er anderszins een link met de gemeente)?

a. In geval van een object wordt gekeken in de Basisregistratie adressen en gebouwen (BAG) en/of informatie van het Kadaster.
b. In geval van een subject wordt gekeken in het handelsregister van de Kamer van Koophandel en/of de Basis Registratie Personen (BRP).
c. Als het signaal betrekking heeft op het grondgebied van de gemeente wordt doorgegaan met stap 2.
d. Indien uit weging 2b blijkt dat er het signaal geen betrekking heeft op het grondgebied van de gemeente worden de gegevens vernietigd conform artikel 7a; of
e. Doorgezet naar een andere gemeente of bevoegde instantie.
f. Indien lid e van toepassing is, wordt na doorzetting de persoonsgegevens vernietigd uit de ondermijningssystemen conform artikel 7a.

4.2 Stap 2 – Zwaarte bepalen van het signaal

In deze stap vindt de beoordeling van signalen van burgers en professionals plaats. Hier vindt dan ook de derde weging plaats. De gemeente weegt de zwaarte van het signaal en beoordeelt of en beoordeelt hoeveel prioriteit het signaal heeft. Indien het signaal niet (direct) wordt opgepakt, worden de gegevens maximaal 1 jaar bewaard. In deze periode kan op elk moment besloten worden om het signaal toch door te zetten naar stap 3.

Artikel 15. Derde weging

Het signaal wordt beoordeelt of:

a. het signaal betrekking heeft op een prioriteit binnen de aanpak van ondermijning.
b. het signaal betrekking heeft op een actualiteit.
c. het signaal informatie bevat die duidt op een groot risico op de verstoring van de openbare orde en veiligheid.
d. het signaal afkomstig is van een ketenpartner (i.p.v. van een burger), RIEC informatieverzoeken krijgen voorrang.
e. Als het signaal binnen Ondermijning wordt opgepakt, wordt doorgegaan met stap 3.
f. Indien uit weging 3 blijkt dat er het signaal niet (direct) wordt opgepakt binnen Ondermijning worden de gegevens vernietigd conform artikel 7b; of
g. Doorgezet naar een andere afdeling van de gemeente; of
h. Doorgezet naar het LSO.
i. Indien lid d of lid e van toepassing is, wordt na doorzetting de persoonsgegevens vernietigd uit de ondermijningssystemen conform artikel 7b.

4.3 Stap 3 - Bronnenonderzoek

In deze stap wordt gebruik gemaakt van gemeentelijke bronnen om meer informatie over het signaal te verkrijgen. De opgevraagde informatie beperkt zich tot informatie die nodig is om een “Hit / No hit” check uit te voeren.

Artikel 16. Privacycheck 1 – Hit / No Hit

a. De Analist Ondermijning maakt een inschatting van de benodigde gegevens op basis van het signaal en legt deze ter beoordeling voor aan de Privacy Officer.
b. De Privacy Officer adviseert of deze gegevens opgevraagd mogen worden of niet. Indien BRP-informatie nodig is, overlegt de Privacy Officer hierover met de BRP-functionaris.
c. De Privacy Officer controleert hierbij of het gebruik van de gegevens verenigbaar is met het oorspronkelijke doel en of het gebruik noodzakelijk is en voldoet aan de proportionaliteits- en subsidiariteitsvereiste.
d. Indien de Analist Ondermijning en de Privacy Officer geen overeenstemming kunnen bereiken wordt het verzoek neergelegd bij de Coördinator VIK.
e. Indien de Coordinator VIK afwijkt van het advies van de Privacy Officer wordt dit gedocumenteerd en voorzien van motivatie.
f. Indien gewenst kunnen alle partijen contact opnemen met de Functionaris Gegevensbescherming voor een second opinion.
g. Er hoeft geen advies aan de Privacy Officer gevraagd te worden indien het signaal past in een specifiek ondermijningsthema waarvoor de Privacy Officer een Hit / No Hit gegevensset heeft gedefinieerd.
h. De Hit / No Hit gegevenssets zoals bedoeld in lid g. is terug te vinden in bijlage 2 van de werkprocesbeschrijving Ondermijning.

Artikel 17. Vierde weging

a. Op basis van de Hit / No Hit bepaalt de Analist Ondermijning of het signaal wordt doorgezet naar het Gemeentelijk Signalen Overleg (GSO).
b. Voordat het signaal wordt doorgezet naar het GSO vindt eerst privacycheck 2a plaats.
c. Indien uit de vierde weging blijkt dat er het signaal niet wordt doorgezet naar het GSO dan worden de gegevens vernietigd conform artikel 7b; of
d. Doorgezet naar een andere afdeling van de gemeente; of
e. Doorgezet naar het Lokaal Signalen Overleg (LSO).
f. Indien lid d of lid e van toepassing is, wordt na doorzetting de persoonsgegevens vernietigd uit de ondermijningssystemen conform artikel 7b.

4.4 Stap 4 – Plan van Aanpak

Artikel 18 Gemeentelijk Signalen Overleg (GSO)

Voorafgaand en aan het GSO vindt privacycheck 2a plaats (zie Artikel 19. Privacycheck 2a).
a. Het GSO bepaalt welke concrete aanpak en bevoegdheden de gemeente wil inzetten en welke binnengemeentelijke gegevensuitwisseling daarvoor nodig is,
b. Op basis van de uitkomsten van het GSO stelt de Analist Ondermijning een Plan van Aanpak op.
c. Het GSO beoordeelt dit Plan van Aanpak en draagt de verantwoording over het vervolg.
d. Voordat het Plan van Aanpak wordt goedgekeurd vindt eerst Privacycheck 2b plaats.
e. Het Plan van Aanpak bevat het eerstvolgend moment dat de betrokkene actief geïnformeerd wordt over de verwerking.

Artikel 19. Privacycheck 2a

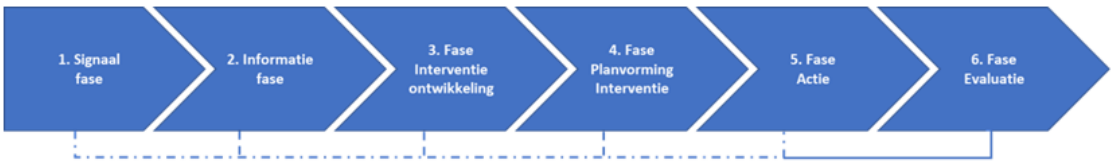
a. De Analist Ondermijning maakt een inschatting welke gegevens gedeeld moeten worden met het GSO en welke gegevens met specifieke gemeentelijke onderdelen en legt deze ter advies voor aan de Privacy Officer.
b. De Privacy Officer adviseert of deze gegevens gedeeld mogen worden of niet.
c. De Privacy Officer controleert hierbij of het delen van de gegevens noodzakelijk is en voldoet aan de proportionaliteits- en subsidiariteitsvereiste.
d. Indien de Analist Ondermijning en de Privacy Officer geen overeenstemming kunnen bereiken wordt het verzoek neergelegd bij de Coördinator VIK.
e. Indien de Coordinator VIK afwijkt van het advies van de Privacy Officer wordt dit gedocumenteerd en voorzien van motivatie.
f. Indien gewenst kunnen alle partijen contact opnemen met de Functionaris Gegevensbescherming voor een second opinion.
g. Er hoeft geen advies aan de Privacy Officer gevraagd te worden indien het signaal past in een specifiek ondermijningsthema waarvoor de Privacy Officer een gegevensset heeft gedefinieerd voor deze stap.

Artikel 20. Privacycheck 2b

a. De Analist Ondermijning maakt een inschatting welke gegevens nodig zijn voor de uitvoering van het Plan van Aanpak en legt deze ter advies voor aan de Privacy Officer.
b. De Analist Ondermijning maakt een inschatting welke gegevens met specifieke gemeentelijke onderdelen gedeeld mogen worden en legt deze ter advies voor aan de Privacy Officer.
c. De Privacy Officer adviseert of deze gegevens verwerkt mogen worden of niet. Indien BRP-informatie nodig is, overlegt de Privacy Officer hierover met de BRP-functionaris.
d. De Privacy Officer controleert hierbij of het delen van de gegevens noodzakelijk is en voldoet aan de proportionaliteits- en subsidiariteitsvereiste.
e. Indien de Analist Ondermijning en de Privacy Officer geen overeenstemming kunnen bereiken wordt het verzoek neergelegd bij de Coördinator VIK.
f. Indien de Coordinator VIK afwijkt van het advies van de Privacy Officer wordt dit gedocumenteerd en voorzien van motivatie.
g. Indien gewenst kunnen alle partijen contact opnemen met de Functionaris Gegevensbescherming voor een second opinion.

5 Vervolg fases

Na de signaalfase worden de overige fases uitgevoerd.



Vanuit elke fase kan worden doorgegaan naar een volgende fase of teruggegaan naar een willekeurige eerdere fase.

5.1 Informatiefase

Nadat de besluitvormers het plan van aanpak hebben goedgekeurd, wordt het informatieproces geïnitieerd.

Artikel 21. Informatiefase

a. De Analist Ondermijning verzameld uit de open bronnen en de gemeentelijke bronnen en verwerkt deze tot intelligence producten.
b. De intelligence producten worden toegevoegd aan het dossier in PGAx.
c. Voorafgaand aan het verzamelen van extra informatie vindt er een privacycheck plaats conform Privacycheck 1.
d. De intelligence producten worden getoetst op inhoud en voortgang in het GSO.
e. Voorafgaand aan de besprekingen in het GSO vindt er een pricacycheck plaats conform Privacycheck 2a.

5.2 Fase interventieontwikkeling

Op basis van het plan van aanpak en het intelligenceproduct maakt de casushouder, samen met de GSO, een interventieadvies. In dit advies staan de voorgestelde interventie(s) om de eerder geformuleerde doelstellingen te bereiken. Het interventieadvies wordt voorgelegd aan het besluitvormend gremium, het Gemeentelijk Signalen Overleg (GSO)

5.3 Fase planvorming interventie

Dit plan wordt door de casushouder, samen met relevante afdelingen in de uitvoering, gemaakt op basis van het interventieadvies. Waar het interventieadvies nog richtinggevend was zorgt het interventieplan voor de concrete uitvoering van de actie. Het verloop van de interventie wordt in detail opgeschreven met daarin de taken voor de deelnemende afdelingen.

5.4 Fase actie

Nadat een interventieplan gemaakt is, wordt er overgegaan tot actie waarmee één of meerdere afdelingen de doelstelling proberen te behalen. De interventies kunnen gelijktijdig en volgordelijk plaatsvinden. In dit geval vormt de interventie als het ware het sluitstuk van de casus.

5.5 Fase evaluatie
De laatste stap betreft de evaluatie. In de evaluatie wordt beoordeeld of de doelstellingen van de casus bereikt zijn. De evaluatie wordt uitgevoerd door het GSO.

Artikel 21. Fase evaluatie

a. De evaluatie kan leiden tot het wijzigen van het Plan van Aanpak, overdragen of het afsluiten van de casus.
b. In de evaluatie wordt het eerstvolgend moment bepaald / heroverwogen dat de betrokkene actief geïnformeerd wordt over de verwerking.
c. Na beëindigen van een casus wordt de casus bewaard conform artikel 7c.
d. Na beëindiging van een casus zijn persoonsgegevens alleen nog in te zien door een beperkt aantal bevoegde medewerkers in verband met het afhandelen van klachten dan wel rechten betrokkene maar ook ter verantwoording van verrichtingen.