

Privacy protocol aanpak ondermijning, fraude en criminaliteit

Beschrijft de verwerking van signalen van fraude, criminaliteit en ondermijning binnen de gemeentelijke organisatie.

1. Inleiding

1.1. Ondermijnende criminaliteit

Er wordt van gemeenten steeds meer verwacht in de aanpak van ondermijning. Bij ondermijnende criminaliteit is er sprake van verwevenheid tussen de onderwereld en de bovenwereld en aantasting van legale bestaande structuren, ook bij de overheid. Criminelen maken misbruik van deze legale structuren voor de uitvoering van hun activiteiten en zo kan de overheid onbewust en ongewild ook criminaliteit faciliteren.

De aanpak van ondermijning is in de gemeente Maashorst onderverdeeld in de navolgende thema's:

- Hennepkwekerijen en drugslaboratoria;
- Drugshandel;
- Mensenhandel (waaronder Illegale prostitutie);
- Witwassen;
- Malafide (horeca)bedrijven;
- Vastgoedfraude.

Met voornoemde vormen van criminaliteit worden vaak enorme geldbedragen verdiend die het mogelijk maken om te corrumperen, te bedreigen en burgers te verleiden om tegen betaling hand- en spandiensten te verrichten. De maatschappelijke integriteit wordt aangetast, de veiligheid en het veiligheidsgevoel van burgers wordt negatief beïnvloed en de lokale economie wordt verstoord.

Een effectieve aanpak van ondermijning vraagt om een georganiseerde overheid die alle middelen en instrumenten inzet die zij tot haar beschikking heeft en samenwerkt met diverse interne en externe ketenpartners. De gezamenlijke aanpak van ondermijning is namelijk niet uitsluitend gericht op opsporing en vervolging van daders maar kent ook een preventieve kant, een zorgkant en inzet van bestuurlijke instrumenten. Interne afdelingen van de gemeente moeten, beter dan voorheen, samenwerken door vroegtijdig informatie te delen en als één overheid te komen tot een mono-, multidisciplinaire of integrale aanpak. Voor integrale gemeente overstijgende aanpak is het RIEC- samenwerkingsverband opgericht.

1.2. Regierol gemeente in de aanpak van ondermijning

Gemeenten worden geacht de regie te voeren op de aanpak van ondermijning en moeten steeds een afweging maken welke signalen zij zelf bestuurlijk oppakken en bij welke signalen ketenpartners moeten worden betrokken. Dit kan eventueel door middel van opschaling naar het RIEC (integrale aanpak).

Dit document is een uitwerking van welke partij, in- en extern, op welk moment met welke (persoons)informatie in het kader van de aanpak van ondermijning aan de slag gaat. Dit alles met inachtneming van de bepalingen uit de Algemene Verordening Gegevensbescherming (AVG) en sectorale wetgeving, waarbij alle partijen hun eigen taak en bevoegdheden uitoefenen.

2. Algemene begrippenlijst

Beslissingsbevoegd: heeft de regie in de desbetreffende fase van het protocol en daarmee de bevoegdheid om (in overleg met betrokkenen) beslissingen te nemen.

Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

Dat-informatie/wat-informatie: Dat-informatie bevestigt dat het object/subject bekend is in de gemeentelijke systemen ('deze betrokkene is binnen het Participatiewet-domein bekend').

Wat-informatie geeft daarnaast ook aan wat er over het object/subject bekend is ('deze betrokkene maakt op grond van a, b en c aanspraak op x').

De (verwerking)verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Hit: als van een persoon bepaalde gegevens in een bronbestand van een gemeentelijk onderdeel voorkomen, is sprake van een 'hit': de betrokken persoon/bepaalde info is bekend binnen de gemeente in het kader van onrechtmatigheden dan wel maatschappelijke bedreigingen.

Informatie-coördinator/veiligheidsanalist: onderzoekt de relevante informatie omtrent een signaal met de daarvoor benodigde bronnen en legt deze vast in het zaakstelsel.

Lokaal Informatie Overleg (L.I.O.): gemeentelijk afdeling overstijgend overleg van een signaal met betrekking tot ondermijning, criminaliteit of fraude met regie vanuit Team veiligheid met diverse collega's die een hit op een signaal hebben of kunnen hebben. Het LIO kan een fysiek overleg met collega's zijn maar kan een vorm zijn waarbij over en weer informatie wordt verwerkt tussen de belanghebbende teams/afdelingen waarbij de regie bij team veiligheid blijft.

Ambtelijk Vooroverleg Ondermijning.): overleg vanuit Team veiligheid met de politie, belastingdienst en OM in het bijzijn van het RIEC, wanneer betrokkenheid vanuit de diensten mogelijk van toegevoegde waarde is bij de aanpak van het signaal. Tijdens dit overleg wordt mondeling aanvullende informatie ingewonnen vanuit de diensten en wordt een laatste afweging gemaakt over de benodigde aanpak van het signaal.

Meld Misdaad Anoniem: is een onafhankelijk meldpunt waar anoniem informatie kan worden gegeven over criminaliteit en misdaad.

Object: er is sprake van een object wanneer het signaal over ondermijning geen persoon betreft, maar een pand, auto of ander voorwerp waar vanuit ondermijnende criminaliteit plaatsvindt.

Ondermijnende criminaliteit: Bij deze vorm van criminaliteit is er sprake van de negatieve effecten van zware- en georganiseerde criminaliteit, al dan niet gecombineerd met de verwevenheid tussen de onderwereld en de bovenwereld: criminelen maken gebruik van legale structuren voor de uitvoering van hun activiteiten en zo kan de overheid ongewild en bewust criminaliteit faciliteren. Vormen van ondermijnende criminaliteit zijn (niet limitatief): hennepcultuur, drugshandel, mensenhandel, witwassen en vastgoedfraude. Allemaal delicten die ernstige consequenties hebben voor onze samenleving. De maatschappelijke integriteit wordt aangetast, de veiligheid en het veiligheidsgevoel van burgers wordt beïnvloed en de lokale economie wordt verstoord.

Plan van aanpak: door een gemeentelijk onderdeel, eventueel in gezamenlijkheid met andere gemeentelijke onderdelen, de integrale diensten of het RIEC-OB opgesteld plan ten behoeve van de toepassing van het wettelijke instrumentarium om ondermijning bestrijden en/of te voorkomen.

Privacyprotocol RIEC: het Privacyprotocol behorende tot en deel uitmakende van het RIEC- convenant.

Regisserende partij: de partij die de regie heeft bij het opstellen van een plan van aanpak ten behoeve van uitvoering van de zijnde wettelijke instrumenten om ondermijning te doen staken.

Regisseur ondermijning: heeft de regierol vanuit de gemeente vanuit Team veiligheid in RIEC-casus.

RIEC-convenant: het Convenant ten behoeve van de Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingssnelwegen en Bevordering Integriteitsbeoordelingen.

RIEC-samenwerkingsverband: Het RIEC (Regionaal Informatie en Expertise Centrum) ondersteunt aangesloten convenantpartners bij de aanpak van georganiseerde criminaliteit. De RIEC's ondersteunen partners door te dienen als informatieknoppunt voor casuïstiek. Vervolgens stelt het RIEC integrale handadviezen op en stemt projectmatig bestuursrechtelijke, strafrechtelijke en fiscale interventies af met de regionale partners. De RIEC's ondersteunen de samenwerking tussen de volgende convenantpartners: Gemeenten, Provincies, Openbaar Ministerie (OM), Nationale Politie, Belastingdienst, Douane, Fiscale Inlichtingen en Opsporingsdienst (FIOD), Inspectie Sociale Zaken en Werkgelegenheid (Inspectie SZW), Koninklijke Marechaussee, Immigratie- en Naturalisatiedienst (IND), Uitvoeringsinstituut Werknemersverzekeringen (UWV) en de Nederlandse Voedsel- en Warenautoriteit (NVWA).

Signaal: aanwijzing(-en) van één of meerdere professionals en/of burgers over subjecten en/of objecten dat bepaalde handelingen, gedragingen en/of situaties mogelijk verband kunnen houden met (verschijningsvormen van) ondermijnende activiteiten. Met een signaal wordt ook bedoeld: (een cluster van) signalen of een (cluster van) melding(-en).

Signaaldossier: een zaakdossier in het zaakstelsel, waarin alle informatie aangaande een signaal wordt opgeslagen.

Subject: de persoon waarover een signaal binnenkomt in het kader van ondermijnende criminaliteit.

Team veiligheid: medewerkers van de gemeente - bestaande uit een regisseur, juridische ondersteuning (vanuit beleidsuitvoering en rol als adviseur), een informatie-coördinator/veiligheidsanalist en administratieve ondersteuning - die zich gezamenlijk inzetten voor de aanpak van ondermijnende criminaliteit door signalen te onderzoeken middels het daarvoor opgestelde protocol.

Veiligheid Informatieknooppunt (VIK): Een knooppunt van veiligheidsinformatie ingaande signalen van fraude, criminaliteit en ondermijning. Het VIK vormt tevens het loket waar medewerkers en diensten hun signalen kunnen melden.

3. Aanpak ondermijning gemeente Maashorst

3.1. Informatie-gestuurde aanpak van ondermijning

De gemeente Maashorst ontvangt signalen van mogelijke ondermijnende activiteiten onder andere via meldingen die binnenkomen via o.a. het Veiligheidsinformatieknooppunt (afgekort, VIK) en via Meld Misdaad Anoniem. Van veel van deze signalen kan niet meteen worden vastgesteld dat er sprake is van ondermijnende criminaliteit. Toch zijn deze signalen van belang om te onderzoeken of de gemeente hierin een wettelijke taak heeft. Om regie op de aanpak van ondermijning te kunnen voeren is een goede informatiepositie van cruciaal belang.

In het Regionaal Veiligheidsplan (RVP) van de Veiligheidsregio Brabant Noord, het Integraal Veiligheidsplan van de gemeente Maashorst, het Uitvoeringsplan Veiligheid (UVP) van de gemeente Maashorst en de bijbehorende plannen van aanpak ondermijning wordt dan ook uitgebreid stilgestaan bij:

- De gezamenlijke opdracht van het beter en efficiënter delen van de beschikbare informatie,
- De ambitie om meer data- en informatie gestuurd te werken,
- De noodzaak om bij de aanpak van ondermijning als één overheid op te treden.

Daarnaast heeft de gemeente Maashorst in het Bestuursakkoord en Uitvoeringsprogramma het doel gesteld om data-gedreven te werken én te werken aan het verhogen van de gemeentelijke informatiepositie op veiligheid. Het ontwikkelen van het Veiligheidsinformatieknooppunt is daar een zichtbaar voorbeeld van.

De gemeente is veelal een toegangspoort voor burgers en organisaties om meldingen te doen van onrechtmatige zaken. De gemeente heeft hierdoor een belangrijke signaalfunctie en beschikt over veel informatie. Via haar organisatiestructuur heeft de gemeente over het algemeen ook goed zicht op de lokale (sociale) structuren.

Signalen, afkomstig van burgers en organisaties, dienen als input voor het uiteindelijk signaleren van ondermijnende criminaliteit.

Voor een effectieve aanpak van ondermijning is een geïntegreerde bestuurlijke aanpak binnen de gemeente een noodzakelijk vereiste omdat:

- Gemeenten een belangrijke schakel vormen om ondermijnende criminaliteit te kunnen signaleren vanwege:
 - Het zicht op de lokale sociale structuren;
 - De, vanwege wettelijke taken en bevoegdheden, beschikbare informatiebronnen.
- Diensten van gemeenten kunnen worden gebruikt door criminelen om geld wit te wassen, onder andere door:
 - Misbruik van vergunningen;
 - Misbruik van subsidies;
 - Misbruik van uitkeringen;
 - Misbruik van vastgoed in de krappe woningvoorraad;
 - Aankoop van onroerend goed;
 - BRP- en /adresfraude
 - Sociale zekerheidsfraude
 - Ontwikkelen van projecten;
- Bestuurders en ambtenaren onder druk kunnen worden gezet en criminelen kunnen infiltreren in het bestuur waardoor de geloofwaardigheid van gemeenten op het spel komt te staan.
- Wijken door ondermijnende criminaliteit verloederen.
- De criminaliteit een aanzuigende werking heeft op de jeugd.

Het doel van de informatie gestuurde en bestuurlijke aanpak van ondermijning is om door middel van binnengemeentelijke samenwerking:

- Ondermijnende activiteiten te signaleren en te analyseren;
- Voorkomen dat de gemeente ondermijnende activiteiten (bewust of onbewust) faciliteert;

- Vroegtijdig te signaleren en indien nodig interveniëren middels een bestuurlijke aanpak;
- Maatschappelijke bedreigingen die de leefbaarheid en openbare orde aantasten voorkomen.

4. Binnengemeentelijke gegevensdeling aanpak ondermijning

4.1. Raad van State

Voor de aanpak van fraude, criminaliteit en ondermijning en daarvoor benodigde binnengemeentelijke gegevensdeling sluit de gemeente Maashorst aan bij het oordeel van De Raad van State¹:

“Het mag duidelijk zijn dat ook de bestuurlijke aanpak van ondermijning tot de taak van de gemeente behoort. Vaak nestelt georganiseerde criminaliteit zich in lokale gemeenschappen. In de taak van gemeentelijke organen ligt besloten om georganiseerde criminaliteit niet ongemerkt en onbedoeld te faciliteren met subsidies, vergunningen of overheidsopdrachten. Daarnaast bestaat een samenhang met de taak van handhaving van de openbare orde in bredere zin en bevorderen van de leefbaarheid van (kwetsbare) wijken. De strafrechtelijke aanpak van ondermijning is een taak van politie en OM. De bestuurlijke aanpak is een taak van gemeenten, waarbij zowel het college van B&W als de burgemeester beschikken over bevoegdheden die uiterst effectief kunnen zijn bij het tegengaan van ondermijnende criminaliteit.”

4.2. Doel van het privacy protocol

Het doel van dit protocol is om de gemeentelijke regie op- en de aanpak van ondermijning volgens procesmatige randvoorwaarden en rechtmatigheidswaarborgen te laten verlopen.

In dit protocol is aan de hand van verschillende proces-fasen uitgewerkt, hoe een signaal van mogelijke ondermijning, fraude of criminaliteit binnenkomt, hoe het wordt opgevaardeerd om te kunnen wegen, hoe het wordt gewogen en wanneer een signaal binnengemeentelijk wordt besproken en/of wanneer er middels een signaalformulier wordt opgeschaald naar een aanpak via het RIEC-samenwerkingsverband, waarop het RIEC-convenant van toepassing is².

4.3. Procesmatige randvoorwaarden

De procesmatige randvoorwaarden van dit protocol bestaan uit:

1. Fasering (voorkomen van bovenmatig gebruik van gegevens); *en*
2. Transparantie (vaststellen van een protocol waarbij zichtbaar en inzichtelijk wordt met welk doel en op welke wijze de gemeente persoonsgegevens verwerkt); *en*
3. Noodzaak (zicht krijgen op waar ondermijning binnen de grenzen van de gemeente aanwezig is).

Hierdoor worden alleen de gegevens gebruikt die ten behoeve van het beoordelen van de binnengekomen signalen, de analyse daarvan en voor het plan van aanpak relevant zijn.

4.4. Rechtmatigheidswaarborgen

De procesmatige waarborgen worden gevormd door de opzet van een werkwijze, zoals opgenomen en toegelicht in hoofdstuk 5. Daarnaast gaat het om rechtmatigheidswaarborgen.

Dit betekent dat toepassing van het protocol steeds zoveel mogelijk in lijn moet zijn met privacy wet- en regelgeving. Afwijkingen daarvan moeten zijn onderbouwd en voldoen aan de waarborgen van subsidiariteit en proportionaliteit.

Bij beoordeling hiervan zijn de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG), maar ook tal van sectorale wetten van belang.

Deze wetten stellen in voorkomende gevallen beperkingen aan het uitwisselen en combineren van persoonsgegevens. Daarbij gaat het veelal om ruim omschreven abstracte normen die in iedere specifieke casus moeten worden geïnterpreteerd en toegepast.

Dit protocol biedt handvatten voor de beslissing die daarin steeds wordt gemaakt.

De rechtmatigheidswaarborgen zijn in de werkwijze opgenomen als privacy-checks en toegelicht in hoofdstuk 5. Aanvullende privacy waarborgen zijn vastgelegd in bijlage 3.

1) Zie het rapport van de Raad van State, 'De rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning', Voorlichting van de Afdeling advisering van de Raad van State van 20 maart 2019, p. 17.

2) <https://www.riec.nl/documenten/convenanten/2014/09/01/convenant-tbv-bestuurlijke-en-geïntegreerde-aanpak-georganiseerde-criminaliteit>

Dit model privacy protocol is opgesteld met inspiratie van De Vereniging van Nederlandse Gemeenten (VNG). Het protocol is opgesteld in opdracht van het Strategisch Beraad Ondernijning (SBO) Oost-Brabant en besproken in een klankbordgroep waarin gemeenten, de Vereniging Nederlandse Gemeenten (VNG) en Autoriteit Persoonsgegevens (AP) hebben deelgenomen.

4.5. Wettelijke taken en bevoegdheden gemeente

Bij de aanpak van ondernijning is er sprake van een grote groep van betrokken afdelingen binnen een gemeente. Bestuurlijke betrokkenheid is er bijvoorbeeld vanuit zowel de Burgemeester, het college van Burgemeester en Wethouders en zelfs de Gemeenteraad.

Daarnaast heeft iedere gemeentebtenaar een eigen verantwoordelijkheid in de aanpak van ondernijning die ligt besloten in het zijn van ambtenaar.

4.6. Taken en bevoegdheden burgemeester

De taken van de Burgemeester in de aanpak van ondernijning vloeien voort uit diens wettelijke taken en bevoegdheden. De ambtelijke organisatie ondersteunt de Burgemeester hierbij. De taken behelzen onder andere:

- Handhaving van de openbare orde en het bestrijden van overlast (art. 172 en 172a Gemeentewet), waarbij de politie onder zijn gezag staat (art. 11 Politiewet).
- Het opstellen en uitvoeren van een Integraal veiligheidsplan (IVP), in het verlengde van de regionale strategische visie, met daarin doelen op het gebied van handhaving van de openbare orde, waaronder de aanpak van ondernijning (art. 39 Politiewet).
- Bevoegdheden op basis van de Algemene Plaatselijke Verordening (APV) op het terrein van openbare orde en veiligheid (art. 121 Gemeentewet): Onder meer sluitingsbevoegdheid van publiek toegankelijke gelegenheden en woningen (art. 174a Gemeentewet) en drugspannen (art. 13b Opiumwet)

4.7. Taken en bevoegdheden college van B&W:

Het college van Burgemeester en Wethouders is onder andere verantwoordelijk voor de navolgende processen:

- Vergunningverlening en toezicht en handhaving op diverse wetten. Onder meer de Omgevingswet en de Alcoholwet;
- Bestrijding heling (art. 437 Wetboek van Strafrecht);
- Taken en bevoegdheden met betrekking tot de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (Bibob), waarmee het bestuur in staat wordt gesteld om vergunningen te weigeren of in te trekken wegens:
 - Ernstig gevaar dat de vergunning zal worden gebruikt voor het plegen van strafbare feiten of witwassen van gelden die zijn verkregen met strafbare feiten;
 - Slecht levensgedrag' of 'schijnbeheer'.

Ook kan de Wet Bibob worden gebruikt bij het nemen van besluiten over:

- Subsidieverlening;
- Gunnen van overheidsopdrachten;
- Aangaan van vastgoedtransacties.

4.8. Overige wetgeving en bevoegdheden

Instrumenten voor de bestuurlijke aanpak van ondernijning zijn ook te vinden in:

- Woningwet;
- Huisvestingswet (eventueel in samenhang met de Wet bijzondere maatregelen Grootstedelijke problematiek);
- Wet milieubeheer (bij het heffen van gemeentelijke belastingen ex art. 220 t/m 229 Gemeentewet).

4.9. Rol gemeentebtenaren in de aanpak van ondernijning

Omdat de bestuurlijke aanpak van ondernijning een taak is van de gemeente, dragen alle medewerkers van de gemeente Maashorst de verantwoordelijkheid om georganiseerde criminaliteit niet ongemerkt en onbedoeld te faciliteren. (Dit zou kunnen door het onterecht verlenen van subsidies, vergunningen, uitkeringen, gunnen van vastgoedtransacties en overheidsopdrachten of het beheer van openbare ruimten.

In geval van een vermoeden van ondernijnende criminaliteit heeft de medewerker de taak om dit te melden bij het bevoegd gezag van de gemeente. In geval van het kennis dragen van een misdrijf, met welke vervolging men niet is belast, is men zelfs verplicht aangifte te doen bij een officier van justitie.⁸ Het spreekt voor zich dat dit protocol betrekking heeft op mogelijke signalen van ondernijnende criminaliteit en niet op de aangifteverplichting als bedoeld in artikel 162 Wetboek van Strafvordering.

In Maashorst worden deze meldingen gedaan via Meld Misdaad Anoniem of via de diverse andere kanalen waardoor deze meldingen op een centraal punt (Veiligheidsinformatieknooppunt) binnenkomen en door het Team veiligheid worden behandeld.

5. Protocol: de werkwijze

5.1. Procesfasen

In dit hoofdstuk wordt besproken aan de hand van welke procesfasen een melding van mogelijke ondermijning, fraude of criminaliteit wordt verwerkt door het Team veiligheid en wie er betrokken zijn bij een binnengekomen signaal van start tot einde.

Bij ondermijning, criminaliteit of fraude is het vaak niet direct zichtbaar óf en waarvan misbruik wordt gemaakt. Daarom is het essentieel dat signalen van ondermijning na binnenkomst eerst worden opge- waardeerd en geanalyseerd voordat tot actie wordt overgegaan.

Dit biedt de mogelijkheid om met minimale impact op de persoonlijke levenssfeer het binnengekomen signaal te verrijken met benodigde basisinformatie.

De route die het signaal aflegt van begin tot einde is onderverdeeld in een zestal fasen:

- 1) Het ontvangen en verwerken van het signaal, waaronder het opwaarderen van het binnengekomen signaal door verrijking met informatie uit eigen en open bronnen en het analyseren en het duiden daarvan.
- 2) Weging van het opgewaardeerde signaal in het Afstemmingsoverleg periodiek.
- 3) Doorgeleiding naar- en weging van het signaal in het Lokaal Informatie Overleg.
- 4) Doorgeleiding naar- en weging van het signaal in Lokaal Ambtelijke Vooroverleg Ondermijning (AVO-O) voor een eventuele Integrale aanpak middels het RIEC-samenwerkingsverband.
- 5) Plan van aanpak tot resultaat.
- 6) Afsluiting en verwijdering van gegevens.

5.2. Werkwijze

5.2.1. Fase 1 - Ontvangst & verwerking signaal

Fase 1	Status	Toelichting
Ont- vangst & ver- werking sig- naal Bevoegd Informatie- coördinator Te raadple- gen bron- nen Zie 5.1.2.	Binnenkomst	Het signaal komt binnen bij de informatiecoördinator van Team Veiligheid.
	Verwerking	Ieder signaal dat binnenkomt wordt vastgelegd in het zaaksysteem en voorzien van een mutatie/registratienummer en eventueel een MMA-nummer waardoor altijd een relatie naar de bron kan worden gelegd. In het zaaksysteem wordt een dossier aangemaakt met de omschrijving en gegevens van het signaal/melding. Bijvoorbeeld de datum van binnenkomst, uitdraai van de Kamer van Koophandel en het Kadaster en een kopie van de melding.
	Routing	Een signaal dat binnenkomt en waarvan duidelijk is dat het door een andere instantie (politie) of afdeling binnen de gemeente wordt behandeld zal, terstond na binnenkomst en vastlegging in de database, naar de desbetreffende afdeling of instantie worden doorgeleid. Het signaal wordt hierbij overgedragen.
	Weging 1	Is er sprake van een gemeentelijke taak, bevoegdheid of toepassingsmogelijkheid van een bestuurlijk instrument?
	Weging 2	Is het subject, het object, of de plaats van het feit gelegen binnen het grondgebied van de gemeente Maashorst of is er een geografische koppeling met Maashorst (V.b. adresfraude)?
	Weging 3	Kwalificatie signaal: Is er mogelijk sprake van ondermijning? <i>Zie bijlage 1 voor wanneer een signaal als ondermijning beschouwd kan worden.</i>
	Zijn de antwoorden op de vragen uit weging 1 t/m 3 positief en is gehandeld conform privacy check 1 dan kan het signaal door naar fase 2.	
	<i>Privacy check 1</i>	Zie bijlage 2 voor de randvoorwaarden inzake de privacy check 1.

Toelichting fase 1: signalen ontvangen en verwerken

Alle binnengekomen signalen worden door de informatie-coördinator geregistreerd in het zaaksysteem. De informatie-architectuur is zo ingericht dat de alleen medewerkers van Team Openbare Orde & Veiligheid met de juiste rechten deze informatie digitaal kunnen raadplegen. Ter verificatie en juiste invoer van het binnengekomen signaal in het zaaksysteem kunnen onderstaande informatiebronnen worden gebruikt:

- o Informatie uit het handelsregister van de Kamer van Koophandel (NHR)
- o Informatie uit de basisregistratie Adressen en Gebouwen (BAG)
- o Informatie uit de basisregistratie personen (BRP)
- o Informatie uit het basisregistratie kadaster (BRK)
- o Informatie afkomstig van het internet.
- o Informatie uit de Bestemmingsplannen van de gemeente Maashorst.
- o Informatie over vergunningen/handhaving/toezicht, voor zover dit geen opsporing betreft en niet valt onder de reikwijdte van de Wet Politiegegevens (Wpg).
- o Informatie uit de Basisregistratie voer- en vaartuigen (BRV) van de RDW.

Weging 1: gemeentelijke taak, bevoegdheid of bestuurlijk instrument

Het is van belang na te gaan of het signaal in beginsel tot gemeentelijk optreden en/of bestuurlijke interventie kan leiden. Derhalve is verrijking van het signaal met eigen- en open bronnen in deze fase noodzakelijk.

Wanneer het signaal op geen enkele wijze aanleiding kan vormen voor inzet van een gemeentelijke taak of bevoegdheid dan wordt het signaal niet in behandeling genomen. Zo nodig wordt het signaal geretourneerd naar de wel daarvoor bevoegde instantie. Als bewaartermijn worden de geldende termijnen gehanteerd.

Weging 2: geografische koppeling gemeente:

Voor weging 2 moeten de vragen, als genoemd onder 1 t/m 3, achtereenvolgens worden beantwoord.

1. Gaat het om een object, subject of rechtspersoon?
 - o In het geval van een object: is het object binnen de gemeentegrenzen gelegen of is er anderszins een link met de gemeente Maashorst?
 - o In het geval van een subject: is het subject woonachtig binnen de gemeentegrenzen of is er anderszins een link met de gemeente Maashorst?
2. Indien het geen subject of object onder 2 of 3 betreft: vindt het feit op het grondgebied van de gemeente Maashorst plaats of zijn er risico's voor de gemeente en/of kunnen er bestuurlijke maatregelen worden toegepast.

Wordt een van de vragen onder weging twee met 'nee' beantwoordt dan stopt verdere behandeling van het signaal. Zo nodig wordt het signaal geretourneerd naar de wel daarvoor bevoegde instantie. Als bewaartermijn worden de geldende termijnen gehanteerd.

Weging 3: kwalificatie ondermijning

Deze weging betreft de vraag of het signaal betrekking heeft op mogelijke ondermijning. Het vaststellen daarvan gebeurt aan de hand van een checklist die is opgenomen in bijlage 1.

Privacy check 1

Deze privacy check dient om de vragen van weging 1 tot en met 3 te beantwoorden. Indien één van de drie antwoorden op de wegingen negatief is stopt verdere behandeling van het signaal. Zo nodig wordt het signaal geretourneerd naar de wel daarvoor bevoegde instantie. Als bewaartermijn worden de geldende termijnen gehanteerd.

5.2.2. Fase 2 - Analyse & weging signaal

Fase 2	Status	Toelichting
Analyse & weging signaal	Analyse	De informatie afkomstig uit fase 1 wordt nader geanalyseerd en relevante koppelingen worden gelegd. Hierbij wordt de voor het signaal bruikbare informatie bewaard en geregistreerd in het zaaksysteem.
Bevoegd Informatie-coördinator & Adviseur	Weging 4	Het signaal wordt gewogen aan de hand van gemeentelijke criteria. De gemeente Maashorst heeft hiervoor de volgende criteria opgesteld, weergegeven onder 5.1.2. Toelichting fase 1, weging 4: <ol style="list-style-type: none"> a. Is het signaal voldoende concreet? b. Is het signaal van recente datum?

seur ondermijning Te raadplegen bronnen Zie 5.1.2. & 5.1.3. Weging 5		c. Heeft hetsignaal betrekking op een van de prioriteiten van het RIEC en/of de gemeente Maashorst? d. Is het signaal afkomstig van een professional? e. Is er sprake van omstandigheden in openbare bronnen, waaronder op internet, op basis waarvan onderzoek kan worden gedaan naar het signaal? Wanneer meer dan de helft van de antwoorden op de vragen met ja kan worden beantwoord dan wordt het signaal verder behandeld onder weging 5.
	Weging 5	Weging 5 betreft een hit/no hit-check om te beoordelen welke informatie (mogelijk) relevant is voor het signaal. Daarnaast worden de uitkomsten van de hit(s), afkomstig uit de informatiebronnen van weging 5 gewogen. Er dient hierbij sprake te zijn van één van de onder weging 5 genoemd indicatoren. Hierna vindt beslismoment 1 plaats.
	Beslismoment 1	1. Er gebeurt niets met het signaal (waarbij het signaal gedurende de geldende termijnen wordt bewaard en daarna verwijderd). 2. Het onderzoek naar het signaal wordt voortgezet en er volgt een Lokaal Informatie Overleg (hierna: LIO) waarmee fase 3 ingaat.
	<u>Privacy check 2</u>	Privacy check 2 houdt in dat er wordt vastgesteld of en zo ja, welke van de verzamelde gegevens worden gedeeld met de relevante, bij het signaal betrokken, gemeentelijke onderdelen. <i>Zie bijlage 2 voor de randvoorwaarden inzake de privacy check 2.</i>

5.1.3. Toelichting fase 2: signaalanalyse

Weging 4

In weging 4 van fase 2 wordt het signaal geanalyseerd en gewogen aan de hand van gemeentelijke criteria. De gemeente Maashorst heeft hiervoor de volgende criteria opgesteld:

a. Is het signaal voldoende concreet?

Bevat het signaal na verrijking voldoende informatie die aanknopingspunten biedt om verder in behandeling te nemen. Veel signalen die binnenkomen zijn niet concreet genoeg. Veelal zijn deze signalen te concretiseren door het raadplegen van gemeentelijke en open bronnen. Alleen dan kan een signaal worden geduid, op waarde worden geschat en de risico's en bestuurlijke mogelijkheden voor de gemeente worden beoordeeld.

b. Is het signaal van recente datum?

Het Team veiligheid moet daarin een afweging maken op basis van haalbaarheid en relevantie.

c. Heeft het signaal betrekking op een van de onderstaande prioriteiten van het RIEC en/of de gemeente Maashorst?

- Georganiseerde hennepcultuur & drugslaboratoria
- Drugshandel
- Mensenhandel- en smokkel
- Illegale prostitutie
- Misbruik en fraude binnen de vastgoedsector
- Witwassen
- Malafide bedrijven
- Cybercrime
- Criminele motorbendes

d. Is het signaal afkomstig van een professional?

Komt de melding van een professional die in verband met zijn of haar functie ervaring heeft met het signaleren van malafide en/of criminele activiteiten of andere verdachte situaties? Dan is het aannemelijk dat deze informatie concreet is en als betrouwbaar kan worden bestempeld.

e. Is er sprake van omstandigheden in openbare bronnen, waaronder op internet, op basis waarvan onderzoek kan worden gedaan naar het signaal?

Is er op basis van informatie uit open bronnen reden om het signaal verder in behandeling te nemen?

Wanneer meer dan de helft van de criteria geldt dan wordt het signaal verder in behandeling genomen en gaat het signaal door naar weging 5.

Weging 5

Weging 5 betreft een hit/no hit-check om te beoordelen welke informatie (mogelijk) relevant is voor het signaal. Daarnaast worden de uitkomsten van de hit(s), afkomstig uit de navolgende informatiebronnen, gewogen:

- Relevante informatie over objecten of subjecten uit de systemen van andere gemeentelijke afdelingen;
- Aanleiding en afdoening van handhavingsverzoeken;
- Constateringen uit controlerapporten;
- Aanleiding en afhandeling van bestuurlijke boetes (WVG);
- Bestuurlijke boetes en andersoortige beschikkingen (Wet Mulder);
- Bestuurlijke boetes Alcoholwet (gesloten bron);
- Informatie vanuit de Rijksdienst voor het wegverkeer (RDW);
- Informatie vanuit Bouw en Woning Toezicht (Omgevingswet);
- Informatie vanuit Economische zaken;
- Belasting Samenwerking Oost-Brabant (BSOB);
- Omgevingsdienst Brabant-Noord (ODBN).

N.B. Informatie afkomstig uit de heffing van gemeentelijke belastingen valt niet onder de doorbreking van de geheimhoudingsplicht als bedoeld in artikel 43c lid 1 onder m van de Uitvoeringswet Algemene Wet Rijksbelastingen (UAWR). Daar waar informatie gebruikt wordt vanuit de gemeentelijke belastingen wordt dit gedekt door een collegebesluit dat de geheimhoudingsplicht opheft.

Voor het vaststellen van een hit is er tenminste sprake van één van onderstaande indicatoren:

- Incongruenties (omstandigheden en gedragingen); feit dat indicaties niet goed bij elkaar passen, niet goed overeenstemmen in aard, omvang en intensiteit;
- Malafide en/of criminele activiteiten, hinder en/of overlast
 - o Veelal systematisch en structureel gepleegd;
 - o Verborgen aanwezig;
 - o Hoge mate van complexiteit

Als van een persoon bepaalde, voor het signaal relevante, gegevens in een bronbestand van een gemeentelijk onderdeel voorkomen, is sprake van een ‘hit’. In dat geval wordt de beschikbare informatie geraadpleegd en gaat men door naar beslismoment 1.

Als er geen hit is dan wordt het signaal niet verder in behandeling genomen en zo nodig gerouteerd naar een andere instantie of afdeling.

Beslismoment 1

- De uitkomsten van weging 1 t/m 5 worden gewogen. Concreet gaat het om de vraag of de hit(s) en eerder verkregen informatie het signaal in voldoende mate bevestigen om door te gaan met het onderzoek naar het signaal (beslismoment 2).
 - o Er gebeurt niets met het signaal (waarbij het signaal gedurende de geldende termijnen bewaard wordt en daarna verwijderd wordt).
 - o Het onderzoek naar het signaal wordt voortgezet en er volgt een Lokaal (Gemeentelijk) Informatie Overleg, dat bestaat uit gemeentelijke professionals (hierna: LIO) waarmee fase 3 ingaat.

Privacy check 2

Privacy check 2 houdt in dat er wordt vastgesteld of en zo ja, welke van de verzamelde gegevens worden gedeeld met de relevante, bij het signaal betrokken, gemeentelijke onderdelen. Dit ten behoeve van het vaststellen van de verdere aanpak.

Deze privacy check vindt plaats vóór het LIO om zo al van tevoren transparantie te verschaffen over gegevens met wie mogen worden gedeeld. Bij het delen van informatie wordt rekening gehouden met de AVG (noodzakelijkheid: proportionaliteit en subsidiariteit van de verwerking).

5.2.3. Fase 3 - Lokaal Informatie Overleg (LIO)

Fase 3	Status	Toelichting
Lokaal Informatie		

<p>Overleg (LIO)</p> <p>Bevoegd Informatie-coördinator & Adviseur ondermijning</p> <p>Te raadplegen bronnen</p> <ul style="list-style-type: none"> • 5.1.2. • 5.1.3. • 5.1.4. 	Informatie-Analyse met LIO leden	<p>Fase 3 betreft de behandeling van het signaal in het LIO met verschillende gemeentelijk professionals.</p> <p>Daarbij worden alleenpersoonsgegevens verwerkt vanuit de taken en verantwoordelijkheden van elke professional behorende bij de uitvoering van diens specifieke wettelijke taak.</p> <p>Wat volgt is een informatie-uitvraag over subject(en) en object(en) bij de navolgende en niet limitatieve LIO-leden:</p> <ul style="list-style-type: none"> • Burgerzaken; • Vergunningen, Toezicht & Handhaving; • Bedrijfscontactfunctionaris economische zaken; • Sociaal onderzoeker; • Toezichthouder bouw.
	Toevoeging LIO-leden	<p>Naast de initiële deelnemers van het LIO kunnen, optioneel en niet limitatief, professionals van afdelingen waarbij in fase 2 een hit heeft plaatsgevonden deelnemen aan het overleg.</p> <p>Kortom, alle afdelingen, voor zover relevant in relatie tot signaal, subject en/of object en niet gehouden aan een geheimhoudingsplicht volgens sectorale wetgeving worden op informatie bevraagd.</p>
	Beslismoment 2	<p>In samenspraak met de verschillende gemeentelijke collega's wordt bepaald of er gezamenlijk actie moet worden ondernomen op basis van het signaal, met regie vanuit Team veiligheid.</p> <p>Daarbij zijn er drie opties:</p> <ul style="list-style-type: none"> • Het signaal wordt niet verder in behandeling genomen waar nodig gerouteerd naar andere (vak)afdelingen; • Lokale bestuurlijke aanpak; • Door naar fase 4: het Ambtelijk Vooroverleg Ondermijning.

Toelichting fase 3: Lokaal Informatie Overleg

Fase 3 betreft de behandeling van het signaal in het LIO met verschillende gemeentelijk professionals. Daarbij worden alleen persoonsgegevens verwerkt vanuit de taken en verantwoordelijkheden van elke professional behorende bij de uitvoering van diens specifieke wettelijke taak.

In bijlage 3 is uitgewerkt op basis van welke wettelijke grondslagen per professional informatie kan en mag worden gedeeld t.b.v. de integrale bestuurlijke aanpak ondermijning. Vanuit de benodigde expertise, passend bij het signaal, wordt van tevoren een agenda samengesteld voor deelnemers aan het LIO.

Primaire deelnemers van het LIO zijn medewerkers Burgerzaken, Vergunningen, Toezicht & handhaving, adviseur veiligheid, informatiecoördinator, bedrijfscontactfunctionaris economische zaken, sociaal onderzoeker en een toezichthouder bouw. Signaalafhankelijk kunnen deelnemers optioneel aan het LIO worden toegevoegd.

De informatie-coördinator van het Team veiligheid voegt de informatie toe aan de dossiermap in het zaakstelsel. Tijdens het LIO wordt alle onderweging 6 beoordeelde en benodigde informatie bij elkaar gebracht, zodat waar nodig nog aanvullingen kunnen worden gegeven en de informatie gezamenlijk kan worden geduid.

Beslismoment 2

In samenspraak met de verschillende gemeentelijke collega's wordt bepaald of er gezamenlijk actie moet worden ondernomen op basis van het signaal, met regie vanuit Team veiligheid.

Daarbij zijn er drie opties:

- Het signaal wordt niet verder in behandeling genomen en waar nodig gerouteerd naar andere (vak)afdelingen.
- Door naar fase 4: het AVO.
Het AVO bestaat uit Team veiligheid, politie, Belastingdienst, OM en vertegenwoordiging vanuit het RIEC. In dit overleg wordt bekeken of betrokkenheid vanuit de diensten mogelijk van toege-

voegde waarde is bij de aanpak van het signaal en of dit signaal mono- of multidisciplinair wordt opgepakt. Daarbij wordt eerst vastgesteld of, en zo ja welke van de verzamelde gegevens (of onderliggende gegevens uit een bepaald dossier) mogen worden gedeeld buiten de gemeente/ met de politie.

- Lokale bestuurlijke aanpak. Daarbij gaat men gelijk door naar fase 5. De Informatiecoördinator/ regisseur ondermijning overlegt, afhankelijk van het signaal en de informatie uit fase 1 en 2, met professionals uit betrokken domeinen over een plan van aanpak. Na vaststelling van het plan van aanpak voeren betrokken gemeentelijke professionals het plan van aanpak uit.

5.2.4. Fase 4 - Ambtelijk Vooroverleg Ondermijning (AVO)

Fase 4	Status	Toelichting
Ambtelijk Vooroverleg Ondermijning (AVO) Bevoegd Adviseur ondermijning Te raadplegen bronnen Gegevens Fase 1,2,3.	Behandeling signaal in AVO	Tijdens dit overleg wordt een laatste afweging gemaakt over de noodzaak van opschaling naar het RIEC-samenwerkingsverband.
	Weging 6	Weging 6 bepaalt of het ondermijningssignaal mogelijk moet worden doorgeleid naar het RIEC- samenwerkingsverband. De uitkomstweging in het AVO kan leiden tot: <ul style="list-style-type: none"> • Het invullen van een signaalformulier RIEC. • Een lokale aanpak. Na deze weging kan fase 5 aanvangen.

Toelichting fase 4: Ambtelijk Vooroverleg Ondermijning (AVO)

Het AVO is een overleg tussen team veiligheid en de politie, belastingdienst en OM met het RIEC als adviseur. Het AVO vormt een belangrijke schakel tussen de gemeentelijke aanpak en de integrale aanpak van het RIEC- samenwerkingsverband.

Tijdens dit overleg wordt de afweging gemaakt over de noodzaak van opschaling naar het RIEC-samenwerkingsverband. Een signaaldocument voor opschaling naar het RIEC-samenwerkingsverband dient bij voorkeur te worden opgesteld door meerdere RIEC-partners. Het vooroverleg bepaalt welke casussen de gemeente Maashorst vanuit openbare orde oppakt en waar ketenpartners vanuit het RIEC moeten worden betrokken.

Weging 6

Deze weging bepaalt of het signaal mogelijk moet worden doorgeleid naar het RIEC- samenwerkingsverband. Vereiste voor een RIEC-aanpak is dat de uitwisseling van gegevens concrete vervolgcacties ten gevolge moet hebben waarmee zichtbare resultaten tegen ondermijning worden geboekt.

De informatie besproken in het AVO wordt in Fileshare gezet, een digitaal en beveiligd informatie-uitwisselingsprogramma van het RIEC. Notulen van de vergaderingen van het AVO worden in Fileshare geplaatst in een omgeving die alleen toegankelijk is voor reguliere deelnemers aan het AVO.

De uitkomstweging in het AVO kan leidentot:

- Het invullen van een signaalformulier RIEC. Daarmee wordt het signaal doorgeleid naar het RIEC-samenwerkingsverband, omdat er sprake is van georganiseerde criminaliteit waarop het RIEC-convenant van toepassing is en waarbij de partners van het RIEC benodigd zijn. De opslag van informatie vindt vanuit het RIEC-convenant plaats in het beveiligde systeem RIEC-IS.
- Een lokale aanpak in samenwerking met betrokken afgevaardigden van de desbetreffende gemeentelijke onderdelen en/of de politie (als 'sterke arm'), waarbij Team veiligheid de regie heeft.

5.2.5. Fase 5 - Plan van Aanpak

Fase 5	Status	Toelichting
Plan van Aanpak Bevoegd	Opstellen Plan van Aanpak	Het signaal wordt gebruikt voor een gemeentelijke aanpak of het signaal wordt behandeld door de RIEC-partners. In beide gevallen is er een regisserende partij aangewezen die het plan van aanpak samenstelt met een concreet resultaat als gevolg.

Regisserende partij	<u>Privacy check 3</u>	Hier wordt bepaald welke gegevensuitwisseling, vergaard in fasen 1,2,3 noodzakelijk is om het doel uit het plan van aanpak te verwezenlijken. Deze check wordt geïnitieerd door iedere afzonderlijke deelnemer aan het overleg. Er wordt geen onderscheid gemaakt tussen RIEC-aanpak of gemeentelijke aanpak.
Te raadplegen bronnen		
• 5.1.2.		
• 5.1.3.		
• 5.1.4.		

Toelichting fase 5: Plan van Aanpak

De regisserende partij stelt een plan van aanpak c.q. interventieadvies op, dat leidt tot interventies die bijdragen aan het te behalen doel en beoogde effect. Daarbij wordt ook de laatste privacy check uitgevoerd:

Privacy check 3

Deze check houdt in dat wordt vastgesteld welke gegevensuitwisseling nodig is voor het verwezenlijken van de vastgestelde aanpak en of dat toelaatbaar is. Een beknopte beschrijving van het plan van aanpak, inclusief de gemaakte afspraken over te ondernemen acties, wordt toegevoegd aan de casus.

5.2.6. Fase 6 - Afsluiting en verwijdering van gegevens

Fase 6	Status	Toelichting
Afsluiting en verwijderen van gegevens	Afronden casus	Na afronden van het plan van aanpak wordt het dossier gesloten. Het resultaat van de ondernomen acties en een evaluatie worden verwerkt in het zaakstelsel. Het gehele digitale dossier wordt volgens de geldende termijnen bewaard.
Bevoegd Adviseur ondermijning & Informatie-coördinator		Het zaakstelsel wordt beheerd door de functioneel beheerders van gemeente Maashorst. De functioneel beheerder borgt de werkprocessen, inrichting, autorisaties en bewaking van de bewaartermijnen.

Toelichting fase 6: Afsluiting en verwijderen van gegevens

Betrokkenen ten aanzien van wie persoonsgegevens zijn verwerkt worden niet actief geïnformeerd. Via de privacyverklaring op de gemeentelijke website wordt actief geïnformeerd over de gegevens die de gemeente kan verwerken om fraude, criminaliteit en ondermijning te voorkomen en te beëindigen. Daarnaast wordt per casus de afweging gemaakt of inzageverzoeken gehonoreerd kunnen worden. Besluitvorming hieromtrent wordt gemotiveerd vastgelegd. De Teammanager veiligheid draagt zorg voor het scheppen van de juiste randvoorwaarden voor veilige gegevensopslag en bewaking van de bewaar- en vernietigingsstermijnen. Inzageverzoeken mogen alleen worden verstrekt na schriftelijke toestemming van de adviseur ondermijning en de informatiecoördinator/-analist in samenspraak met de privacy-officer.

Bijlage 1: checklist vaststellen ondermijning

Aan de hand van onderstaande checklist wordt stapsgewijs beoordeeld of het signaal betrekking heeft op ondermijning. De checklist is afhankelijk van maatschappelijke ontwikkelingen en kan reeds daarom niet als limitatief worden beschouwd. Vanzelfsprekend kan de checklist worden aangepast al naar gelang de eigen gemeentelijke praktijk en ervaringen.

De ontvangst van een signaal door de frontofficemedewerker veiligheid c.q. informatie-coördinator/analist ondermijning vormt het startpunt voor het protocol.

Er wordt tot uitgangspunt genomen dat het delen van signalen met de regisseur ondermijning op rechtmatige wijze geschiedt. Vanzelfsprekend zal een verstrekker van een signaal wel steeds moeten vaststellen of die verstrekking in lijn is met de privacyregelgeving.

Stap 1: het signaal heeft betrekking op een dan wel meer van de volgende categorieën personen.

Openbare inrichtingen

- a. Pandeigenaar
- b. Verhuurder
- c. Huurder/pachter
- d. Exploitant
- e. Beheerder/Leidinggevende
- f. Tussenpersoon
- g. Geldschieters
- h. Betrokkene

Georganiseerde hennepcultuur/drugs(-handel)

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Tussenpersoon (verhuurmakelaar, evt. andere vormen?)
- e. Betrokkene

Mensenhandel, -smokkel en uitbuiting (o.a. illegale prostitutie)

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Eigenaar (illegale) seksinrichting
- e. Eigenaar (illegale) massagesalon
- f. Exploitant van een vergunde seksinrichting
- g. Beheerder van een vergunde seksinrichting
- h. Sekswerker
- i. Betrokkene

Fraude in de vastgoedsector

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Betrokkene
- e. Tussenpersoon (verhuurmakelaar, andere vormen?)
- f. Stichting, vereniging of andere ondernemingsvorm (of bestuurders hiervan)

Misbruik in de vastgoedsector

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Tussenpersoon (verhuurmakelaar, andere vormen?)
- e. Stichting/vereniging of andere ondernemingsvorm (of bestuurders hiervan)
- f. Betrokkene

Fraude en/of witwassen en daaraan gerelateerde vormen of andere vormen van financieel- economische criminaliteit (o.a. ook illegaal gokken/heling/underground banking)

- a. Ontvanger/begunstigde uitkering vanuit de gemeente
- b. Ontvanger/begunstigde subsidie vanuit de gemeente
- c. Andersoortige begunstigende beschikking vanuit de gemeente

- d. Een tussenpersoon/gemachtigde met betrekking tot zorg
- e. Pandeigenaar
- f. Betrokkene

Overig

- a. Overige facilitators die ondermijnende of criminele activiteiten mogelijk maken en/of (on)bewust in stand houden;
- b. En/of personen die een rol spelen bij een regionaal thema of een handhavingsknelpunt zoals:
 - Opiumwet gerelateerde signalen
 - Thema's uit het RVP, IVP of UVP of actieplannen gericht op de aanpak van ondermijning.

Stap 2: het signaal voldoet aan één of meer van de volgende kenmerken.

- 1. Aantasting van instituten die zich richten op legale perspectieven en de werking van het samenlevingssysteem borgen en sturen
- 2. Aantasting van de gezagspositie van bestuur, politie en/of andere overheidsorganen
- 3. Aantasting of latente c.q. mogelijke aantasting van de openbare orde en veiligheid
- 4. Ontwrichting of latente c.q. mogelijke ontwrichting van de maatschappelijke, politieke en/of economische structuren
- 5. Onrechtmatigheden, maatschappelijke bedreigingen en/of georganiseerde criminaliteit

Bijlage 2: Toelichting privacy checks

In **fase 1** wordt in het kader van privacy check 1 bepaald of en zo ja welke gemeentelijke bronnen naar aanleiding van het concrete signaal kunnen worden geraadpleegd.

In ieder geval dienen de navolgende bronnen te worden geraadpleegd, afhankelijk van de inhoud van het signaal, om het signaal überhaupt te kunnen duiden.

- BRP (inwoners van een adres waarover gemeld wordt)
- KvK (inschrijvingen t.a.v. een adres of bedrijf waarover gemeld wordt)
- Kadaster (eigendom van onroerend goed waarover gemeld wordt).
- RDW (tenaamgestelde van een voertuig waarover gemeld wordt).
- Zaaksysteem
- Open bronnen op internet
- Sociale-media/kranten.

In **fase 2** (privacy check 2) en **fase 5** (privacy check 3) stelt de informatie coördinator vast:

- Welke verzamelde gegevens met de relevante, bij het signaal betrokkenen (gemeentelijke onderdelen of daarbuiten) mogen worden gedeeld ten behoeve van de vaststelling van de verdere aanpak (privacy check 2); en
- Welke binnengemeentelijke gegevensuitwisseling nodig is voor het verwezenlijken van die aanpak en of dat toelaatbaar is (privacy check 3).

De vraag welke binnengemeentelijke gegevensdeling is toegestaan moet steeds worden beantwoord aan de hand van de specifieke wettelijke regeling die op de betreffende gemeentelijke informatie van toepassing is. Dat is nog niet zo eenvoudig: niet alleen zijn op de verschillende soorten gemeentelijke bronnen verschillende wettelijke regelingen van toepassing, ook is iedere casus anders en zal daarom steeds een op het geval toegespitste afweging moeten worden gemaakt. Er is dan ook niet één simpel antwoord te geven op de vraag wie, wanneer, welke informatie binnen de gemeente mag delen ter bestrijding van ondermijning.

Gegevens-uitvraag Participatiewet (Pw); werk en inkomen

De Participatiewet-functionaris heeft geen (of in uitzonderlijke gevallen hooguit zeer beperkt) mogelijkheden om gegevens uit de Participatiewet te delen voor het doel en aanpak van ondermijning. Dit vanwege de geheimhoudingsbepaling in artikel 65 Participatiewet, welke op hen van toepassing is.

Vanwege deze strikte geheimhoudings- en doelbindingsbepaling in deze specifieke (materie/sectorale) wet, komt men ook niet toe aan de verenigbaarheidstoets als bedoeld in art. 6, lid 4, AVG).

De wetgever heeft namelijk zelf al duidelijkheid gegeven, door de geheimhoudingsbepaling in de wet op te nemen. Verstrekking uit de participatiewet kan alleen als de betrokkene schriftelijke toestemming heeft gegeven.

Ten aanzien van algemene inkomensgegevens zouden eventueel de benodigde gegevens kunnen worden verschaft vanuit de Basisregistratie Inkomen (BRI).

Artikel 43c lid 1 onder m van de UAWB heft de geheimhoudingsplicht uit de belastingwetgeving op voor de gemeente als er sprake is van informatiedeling in een RIEC-samenwerkingsverband.

Artikel 67 AWR (geheimhoudingsplicht)

Het is eenieder verboden hetgeen hem uit of in verband met enige werkzaamheid bij de uitvoering van de belastingwet over de persoon of zaken van een ander blijkt of wordt meegedeeld, verder bekend te maken dan noodzakelijk is voor de uitvoering van de belastingwet of voor de invordering van enige rijksbelasting als bedoeld in de Invorderingswet 1990 (geheimhoudingsplicht).

Artikel 43c lid m UAWR.

De geheimhoudingsplicht, bedoeld in artikel 67, eerste lid, van de wet, artikel 67, eerste lid, van de Invorderingswet 1990 en artikel 10, eerste lid, van de Registratiewet 1970, geldt niet voor verstrekking aan de hierna genoemde bestuursorganen voor zover het betreft de hierna genoemde gegevens ten behoeve van de hierna genoemde publiekrechtelijke taak:

m. Gemeenten, provincies, de politie, de officier van justitie, de Minister van Sociale Zaken en Werkgelegenheid, de Koninklijke marechaussee, de Inspectie SZW, de Sociale verzekeringsbank of het Uitvoeringsinstituut werknemersverzekeringen: gegevens die nodig zijn om de samenwerking in het kader van de integrale toepassing en handhaving van overheidsregelingen effectief en efficiënt te laten verlopen voor zover een convenant is gesloten met deze bestuursorganen;

N.B. Gegevens betreffende gemeentelijke belasting vallen niet onder deze doorbreking van de geheimhoudingsplicht. Ten aanzien van deze gegevens is een afzonderlijk collegebesluit noodzakelijk.

Gegevens-uitvraag Wmo

Ook voor de uitvoering van de Wmo geldt een strikte geheimhoudingsplicht (artikel 5.3.3. Wmo 2015) en strikte doelbinding. De Wmo 2015 kent geen bepaling om gegevens te delen ten behoeve van de bestrijding van ondermijning.

Alleen met toestemming van de betrokkene of dienst wettelijke vertegenwoordiger kunnen inlichtingen, dan wel inzage in of afschrift van de bescheiden aan derden worden verstrekt. Voor de toezichthoudende ambtenaren geldt een afgeleide geheimhoudingsplicht (artikel 6.1, lid 3, Wmo 2015). De toezichthoudende ambtenaar mag alleen (bijzondere) persoonsgegevens verstrekken voor zover dat overeenkomt met het bepaalde in artikel 5.2.4., lid 3, Wmo 2015. Ondermijning valt daar niet onder.

Gegevens-uitvraag Jeugdwet

Gegevens die in de Verwijsindex Risicjongere (VIR) worden verwerkt mogen in beginsel niet aan een ondermijningsteam worden verstrekt t.b.v. de aanpak van ondermijning.

De VIR kent een strikte doelbinding die is bepaald in artikel 7.1.2.1., lid 3 en artikel 7.1.4.4. Jeugdwet.

De VIR mag namelijk alleen gebruikt worden om jeugdigen tijdige passende hulp zorg of bijsturing te verlenen om bedreigingen naar een veilige en gezonde ontwikkeling te voorkomen. De VIR is uitsluitend bedoeld om meldingsbevoegden in staat te stellen kennis te nemen van de meldingen.

Ook op gegevens uit een jeugdossier van de jeugdhulpverlener en de "gemeentelijke" gegevens ter uitvoering van de Jeugdwet kunnen in beginsel niet aan het Team veiligheid worden verstrekt. Dit kan alleen indien de jeugdige of met het gezag belaste ouder schriftelijke toestemming heeft gegeven, of sprake is van een conflict van plichten of zwaarwegend belang. Deze belangenafweging is altijd te maken door de jeugdhulpverlener /jeugdconsulent.

Gegevens-uitvraag Wet Structuur uitvoeringsorganisaties werk en inkomen (Wet Suwi)

Hoewel de bestrijding van ondermijning in het verlengde kan liggen van bestrijding van sociale zekerheidsfraude, liggen de strikte geheimhoudingsplicht en doelbinding in de weg om persoonsgegevens uit te wisselen met het Team veiligheid.

Eenieder die bij uitvoering van de Wet Suwi beschikking krijgt over gegevens geldt eveneens een strikte geheimhoudingsplicht. Die gegevens mogen niet verder bekend worden gemaakt dan voor de uitvoering van de Wet Suwi noodzakelijk is dan op welk grond van de Wet Suwi is voorgeschreven of toegestaan. Deze geheimhoudingsplicht geldt niet als de gegevensverstrekking wettelijk is verplicht, de betrokkene geen bezwaar tegen de verstrekking heeft gemaakt, of de gegevens niet herleidbaar zijn tot de betrokken persoon of er sprake is van een conflict van plichten. Dan moet sprake zijn van een levensgevaar of een ernstig strafbaar feit.

Conclusie voor deelname toezichthouders uit het Sociaal Domein aan het LIO

Bovenstaande betekent voor de toezichthouders die in het Sociaal Domein opereren alleen aan het LIO zouden kunnen deelnemen om informatie voor de eigen taken te kunnen ophalen. Het is hen niet toegestaan om informatie in het LIO te verstrekken.

Informatie inbrengen kan alleen:

- ✓ Toezichthouders Pw: schriftelijke toestemming betrokkene of geanonimiseerd worden gedeeld.
- ✓ Toezichthouders Wmo 2015: schriftelijke toestemming betrokkene of wettelijke vertegenwoordiger of sprake van een onderzoek naar een zeer ernstig strafbaar feit.
- ✓ Toezichthouders Jeugdwet: alleen informatie uit de jeugdossier en gemeentelijke gegevens indien sprake is van schriftelijke toestemming of sprake van conflict van plichten/zwaarwegend belang van de jeugdhulpverlener/jeugdconsulent.
- ✓ Toezichthouders Wet Suwi: schriftelijke toestemming betrokkene, geanonimiseerd of conflict van plichten bij levensgevaar of ernstig strafbaar feit.

Privacy check 1:

Privacy check 1 vormt de belangrijkste privacy-beoordeling en vindt plaats in het kader van de hit/no hit-analyse (start van fase 2). Per geval moet de regisseur ondermijning (eventueel in samenspraak met andere medewerkers van het Team veiligheid en/of de privacy-officer) voor zichzelf altijd de volgende vragen stellen:

A. Wat is de wettelijke basis voor het primaire gebruik?

Allereerst wordt bepaald welke gegevens nodig zijn voor het onderzoek naar een signaal. Op basis daarvan wordt vastgesteld op basis van welke gemeentelijke taak deze gegevens aanvankelijk zijn verkregen (ook wel: het primaire gebruik van de gegevens).

Deze taak zal steeds een wettelijke basis hebben, bijvoorbeeld in de Gemeentewet of een andere sectorale wet. De wettelijke regeling op basis waarvan gegevens aanvankelijk zijn verkregen, is in sterke mate bepalend voor de vraag of gegevens (ook) kunnen worden gebruikt voor de bestrijding van ondermijning.

Zo kan die wettelijke regeling een geheimhoudingsbepaling bevatten die het (verdere) gebruik van gegevens beperkt of anderszins regelen of en zo ja, in hoeverre de gegevens voor bepaalde doeleinden of taken mogen worden gebruikt.

B. Is bestrijding van ondermijning verenigbaar met het oorspronkelijk doel waarvoor de gegevens zijn verzameld?

In aanvulling daarop geldt dat het gebruik van gegevens ter bestrijding van ondermijning een toelaatbare verdere verwerking moet zijn.

Van een toelaatbare verdere verwerking is sprake als het gebruik van de gegevens verenigbaar is met het doel waarvoor de gegevens aanvankelijk zijn verkregen. Daarbij moeten de volgende vragen worden beantwoord:

1. Wat is het doel van de wet en/of de wettelijke bepaling op basis waarvan de gegevens aanvankelijk zijn verkregen?
2. Is het bestrijden van ondermijning verenigbaar met dat primaire doel?
3. Wat is het kader waarin de persoonsgegevens zijn verzameld?
4. Wat is de aard van de verwerkte persoonsgegevens?
5. Wat zijn de mogelijke gevolgen voor de betrokkene?
6. Worden er passende waarborgen getroffen?²²

Van verenigbaarheid in de zin van de vragen 1 en 2 zal sneller sprake zijn als de wettelijke basis voor het primaire gebruik gerelateerd is aan het bestrijden van ondermijning, bijvoorbeeld een openbare orde bevoegdheid van de burgemeester. Dat wordt lastiger, maar is niet onmogelijk, als de wettelijke basis betrekking heeft op een geheel ander domein, zoals het sociaal domein.

Ondermijning heeft namelijk ook een zorgkant en het is vaak in het belang van een betrokkene of meerdere betrokkenen dat de gemeente uitvoering geeft aan die taak.

Bij de aanpak van ondermijning wordt niet alleen gedacht in termen van opsporing en vervolging.

De gemeente heeft een brede taakstelling die er in de meeste gevallen toe strekt dat zij moet zorgdragen voor een veilige en prettige leefomgeving. Ondermijning slaat aan de wortels van die beoogde veilige leefomgeving en persoonlijke belangen van kwetsbaren.

De regievoering op de aanpak van ondermijning met als gevolg een verdere verwerking van persoonsgegevens is breed. In het concrete geval wordt dit doel daarom gepreciseerd door het te vertalen naar de gemeentelijke wettelijke bevoegdheden die de gemeente ten behoeve van de aanpak van het signaal van ondermijning zou willen inzetten.

Het zal hierbij veelal gaan om wettelijke taken en gemeentelijke bevoegdheden die zien op openbare orde bevoegdheden en bevordering van de leefbaarheid.

Van belang hierbij is dat aan het voorzienbaarheids criterium wordt voldaan: een betrokkene moet kunnen voorzien dat de bedoelde gegevensverstrekking zou kunnen plaatsvinden.

Dit wordt transparant gecommuniceerd middels de privacyverklaring ondermijning op de website van de gemeente Maashorst.

Indien de regisseur ondermijning concludeert dat sprake is van onverenigbaarheid, kan het gebruik van de gegevens ter bestrijding van ondermijning toch toelaatbaar zijn als er een expliciete wettelijke grondslag voor dat gebruik is. De privacy-officer kan worden ingeschakeld om daarbij hulp te bieden.

Het model privacy-protocol van de VNG bevat voorbeelden van bovenstaande analyse met betrekking tot wetten op basis waarvan gegevens kunnen worden verkregen die vaak relevant zullen zijn voor het tegengaan van ondermijning door gemeenten (als gezegd zal het hierbij veelal gaan om wettelijke taken en bevoegdheden die toezien op openbare orde bevoegdheden en bevordering van de leefbaarheid)²³.

Voor de verwerking van bijzondere en strafrechtelijke persoonsgegevens geldt een bijzonder regime: die gegevens mogen in beginsel alléén worden verwerkt als uit de wet op basis waarvan die gegevens zijn verkregen blijkt dat dat – voor de in die wet genoemde doelen – mag.

Voor strafrechtelijke gegevens geldt nog een andere relevante uitzonderingsgrond: een gemeente zal die gegevens mogen verwerken als zij krachtens de Wet politiegegevens of Wet justitiële en strafvorderlijke gegevens zijn verkregen (zie voor een uitwerking van verstrekking op grond van de Wet politiegegevens²⁵).

C. Is het gebruik van de gegevens noodzakelijk en proportioneel en wordt aan het subsidiariteitsvereiste voldaan?

Gegevens mogen alleen worden gebruikt voor de bestrijding van ondermijning als dat gebruik noodzakelijk en proportioneel is en er geen minder ingrijpende middelen voorhanden zijn. Bij de vraag of een verstrekking noodzakelijk en proportioneel is, spelen onder meer de volgende omstandigheden een rol:

- De aard en ernst van een binnengekregen signaal. Bij aanwijzingen dat er ernstige feiten spelen, zal informatie eerder mogen worden gedeeld;
- De ernst van de inbreuk die op de persoonlijke levenssfeer van de betrokkene wordt gemaakt. Daarbij kan onder meer acht worden geslagen op:
 - De voorzienbaarheid van de (cumulerende) inbreuk die op de persoonlijke levenssfeer wordt gemaakt;
 - De vraag in hoeverre een compleet beeld van de betrokkene ontstaat;
 - In hoeverre een betrokkene negatieve gevolgen zal ondervinden van de gemaakte inbreuk;
 - De aard van de gegevens (hoe gevoeliger, hoe terughoudender ermee moet worden omgegaan);
 - Of een betrokkene zich effectief kan verweren tegen gemaakte inbreuken (bijv. rechtsbescherming).

In het kader van de vraag naar subsidiariteit moet bijvoorbeeld, als is vastgesteld dat sprake is van een verenigbare verdere verwerking of een expliciete wettelijke grondslag voor het gebruik, eerst een ‘hit/no hit’-check worden gedaan (met andere woorden: eerst nagaan dat er bepaalde informatie bij de gemeente berust), alvorens de informatie zelf kan worden geraadpleegd (wat is de informatie waarover de gemeente beschikt). In sommige gevallen kan de eerste vorm van informatie volstaan (subsidiariteit).

Privacy check 2 en 3: aanvullende waarborg

Als aanvullende waarborg is in dit protocol een tweede en derde privacy beoordelingsmoment. Privacy check 2 wordt door de informatie coördinator uitgevoerd voorafgaand aan het Lokaal Informatie Overleg (start fase 3).

Bij onduidelijkheden of vragen wordt de privacy-officer ingeschakeld. De regisseur ondermijning (eventueel in samenspraak met de privacy-officer stelt bij iedere casus vast of en zo ja welke verzamelde gegevens daadwerkelijk mogen worden gedeeld met de/het relevante, bij het signaal betrokkenen (gemeentelijke onderdelen of daarbuiten) ten behoeve van de verdere aanpak.

Met name de beoordeling van de *noodzaak* om informatie te delen, zal daarbij centraal staan. Het gaat dan niet alleen om de hoeveelheid gegevens, maar ook om de vraag of alle deelnemers de betreffende informatie nodig hebben.

Denkbaar is bijvoorbeeld dat een signaal op maar drie domeinen ziet en de informatie ten aanzien van dat signaal dus ook alleen aan de deelnemers vanuit die domeinen mag worden verstrekt (in plaats van aan alle domeinen die aan tafel zitten)

Zoals eerder aangegeven kan ook in fase 5 – bij het bepalen van het plan van aanpak voor een casus – een privacy check nodig zijn, om te bepalen of de verzamelde gegevens daadwerkelijk mogen worden gedeeld met relevante betrokkenen ten behoeve van de verdere aanpak en beoogde inzet van bevoegdheden. Daartoe zullen dezelfde vragen moeten worden gesteld als hierboven omschreven.

Bijlage 3: Algemene privacy waarborgen

Er is geen wet die gemeenten expliciet opdraagt tot een bestuurlijke aanpak van ondermijning en evenmin tot binnengemeentelijke gegevensdeling. Echter, de Raad van State oordeelt wel degelijk dat beide behoren tot een gemeentelijke taak³:

“Het mag duidelijk zijn dat ook de bestuurlijke aanpak van ondermijning tot de taak van de gemeente behoort. Vaak nestelt georganiseerde criminaliteit zich in lokale gemeenschappen. In de taak van gemeentelijke organen ligt besloten om georganiseerde criminaliteit niet ongemerkt en onbedoeld te faciliteren met subsidies, vergunningen of overheidsopdrachten. Daarnaast bestaat een samenhang met de taak van handhaving van de openbare orde in bredere zin en bevorderen van de leefbaarheid van (kwetsbare) wijken. De strafrechtelijke aanpak van ondermijning is een taak van politie en OM. De bestuurlijke aanpak is een taak van gemeenten, waarbij zowel het college van B&W als de burgemeester beschikken over bevoegdheden die uiterst effectief kunnen zijn bij het tegengaan van ondermijnende criminaliteit.”⁴

Bovenstaande uitspraak van de Raad van State waarborgt dat de gemeente op een rechtmatige en effectieve manier kan voldoen aan de binnengemeentelijke gegevensdeling. Daarnaast is er informatie beschikbaar vanuit het ‘Model privacy protocol’ over analyses naar de ruimte voor binnengemeentelijke gegevensuitwisseling in relevante wet- en regelgeving⁵.

Bij het opstellen van het werkproces is rekening gehouden met de basisregels voor de binnengemeentelijke gegevensdeling.

De rechtsgrond (of grondslag) voor de binnengemeentelijke gegevensdeling:

- Artikel 6, lid 1, onder c AVG (noodzakelijk om wettelijke verplichting na te komen), of
- Artikel 6, lid 1 onder e AVG (noodzakelijk voor de vervulling van een taak van algemeen belang of openbaar gezag)

Verwerk uitsluitend gegevens die noodzakelijk zijn om de taak goed te kunnen uitvoeren (ofwel: data-minimalisatie). Dit hangt af van het doel van de verwerking.

- Zorg ervoor dat, vóórdat gegevens worden verwerkt, het doel daarvan welbepaald, uitdrukkelijk omschreven en gerechtvaardigd is, ofwel: bepaal vooraf wat je doet en waarom en wees concreet.
- Zowel de gegevensverstrekker (verwerking) als de ontvanger (verdere verwerking) moeten een rechtsgrond hebben voor de verwerking van de gegevens.
- Voor zover sprake is van ‘verder verwerken’ moet de verstrekking verenigbaar zijn met het doel waarvoor de bron de gegevens verzameld heeft.
- Er kan ook sprake zijn van schijnbare onverenigbaarheid terwijl toch verwerking en verdere verwerking mogelijk is.

Art 6, lid 4 AVG.

Wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld niet berust op toestemming van de betrokkene of op een Unierechtelijke bepaling of een lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, lid 1, bedoelde doelstellingen houdt de verwerkingsverantwoordelijke bij de beoordeling van de vraag of de verwerking voor een ander doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld onder meer rekening met:

- a) Ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking;
- b) Het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;
- c) De aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt, overeenkomstig artikel 9 AVG, en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt, overeenkomstig artikel 10 AVG;
- d) De mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;
- e) Het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

Naast het in acht nemen van bovenstaande basisregels wordt er middels de volgende punten voldaan aan algemene privacy waarborgen op het gebied van persoonsgegevens:

3) Uit: Kamerstukken II 2018/19, 35000 VI, nr. 2, p. 14 en Voorlichting van de Raad van State van 20 maart 2019: De rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning”

4) <https://www.raadvanstate.nl/@113263/w16-18-0272-ii-vo/>

5) <https://www.rijksoverheid.nl/documenten/rapporten/2020/02/20/tk-bijlage-model-privacy-protocol-binnengemeentelijke-gegevensdeling>, p. 31-89.

1: (verwerkings-)verantwoordelijke

In de meest voorkomende gevallen is de Burgemeester van de gemeente Maashorst de (verwerking)verantwoordelijke.

2: grondslag van verwerking

De verwerking is noodzakelijk 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 (artikel 6, lid 1, onder e, AVG). Het zal daarbij veelal gaan om wettelijke taken en bevoegdheden die zien op de openbare orde bevoegdheden en bevordering van de leefbaarheid.

3: de verwerkte persoonsgegevens

1. Van de melders wordt uitsluitend de in het signaal opgenomen persoonsgegevens verwerkt ten behoeve van communicatie met de melder, zoals naam, voornamen, telefoonnummer, e-mailadres, afdeling.
2. Van de personen over wie wordt gemeld, worden gegevens verwerkt zoals benoemd in het werkproces dat is vastgelegd in het eerder beschreven protocol (hoofdstuk 2).
3. De in het tweede lid bedoelde persoonsgegevens worden gebruikt voor:
 - Afhandeling van het signaal
 - Het (mono- of multidisciplinair) oppakken van het signaal binnen de eigen kaders door de gemeentelijke onderdelen of;
 - De verdere aanpak van ondermijning onder regie van Team veiligheid (eventueel in samenwerking met gemeentelijke onderdelen en de politie) of;
 - Het verstrekken van het signaal binnen het RIEC-samenwerkingsverband.

4: categorieën van ontvangers

Voor zover noodzakelijk voor de in hoofdstuk 1.2 genoemde doelen, kunnen gegevens (signaal en aanvullingen uit open bronnen) worden:

- a. Verstrekt aan gemeentelijke onderdelen of de politie ten behoeve van een plan van aanpak, voor zover zij die behoeven voor de uitvoering van hun wettelijke taak of;
- b. Verstrekt aan het RIEC-OB voor het binnen het RIEC-samenwerkingsverband ingebrachte en aangenomen casus.

5: beheer (technische en organisatorische waarborgen).

1. Het college van B&W van de gemeente Maashorst respectievelijk de burgemeester van de gemeente Maashorst (ieder voor zover het zijn bevoegdheid betreft) zijn beheerder. Zij dragen zorg voor het dagelijks beheer van de verwerking, waaronder de beveiliging van de persoonsgegevens, de informatieverstrekking, aan betrokkene en de afhandeling van de door betrokkene uitgeoefende rechten.
2. Het feitelijk beheer van de verwerking van persoonsgegevens en feitelijke naleving van de informatieplicht is opgedragen aan een door organisatie daartoe aangewezen persoon, behorende tot zijn organisatie. Slechts de regisseur, het VIK en andere medewerkers van Team veiligheid hebben toegang tot de bijbehorende bestanden.

De regisseur ondermijning is adviserend voor de uitvoering en de lijnverantwoordelijkheid ligt bij de teamleider van Team veiligheid.

Artikel 6: beveiliging van persoonsgegevens

a. Binnengemeentelijke verwerking en uitwisseling van gegevens

De beheerder draagt zorg voor passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Hiertoe behoren in ieder geval:

Vastgesteld beveiligingsbeleid dat ook is geïmplementeerd en;

Fysieke maatregelen voor toegangsbeveiliging inclusief organisatorische controle. Zoals:

- Een proces voor controle op logging;
- Logische toegangscontrole (wachtwoord of pincode).

b. Uitwisseling van gegevens met externe partners

- Samenwerkingspartners van RIEC-convenant²⁷

Functiescheiding BOA

Buitengewoon opsporingsambtenaren (Boa's) hebben door hun taken en bevoegdheden in veel gevallen een dubbele functie. Een boa heeft namelijk naast opsporingsbevoegdheden bijna altijd ook bestuursrechtelijke toezichts- en handhavingstaken. Bij het verwerken van persoonsgegevens hebben zij daarom zowel te maken met de AVG als de Wet politiegegevens (Wpg).

Voor de BOA die zowel onder de Wpg als AVG valt is een afzonderlijke werkinstructie opgesteld.

In het kort komt het erop neer dat een BOA geen bevoegdheden heeft ten aanzien van de Opiumwet en de Jeugdwet. Hij onthoudt zich dan ook van de uitoefening van bevoegdheden op dat gebied. Wel heeft hij een signaleringsfunctie zoals elke gemeenteambtenaar die heeft en kan derhalve wel signalen van ondermijning en waarnemingen op dat gebied (Opiumwet en Jeugdwet) doen en rapporteren aan het Team veiligheid. Gegevens die hij verkrijgt vanuit zijn bevoegdheid als bijzonder opsporingsambtenaar vallen onder de WPG waar een gesloten regime geldt. De bijzonder opsporingsambtenaar onthoudt zich dan ook van het verstrekken van gegevens die onder de Wpg vallen aan het Team veiligheid.

Artikel 7: bewaartermijnen

1. De gegevens worden:
 - a. Gedurende een jaar in de database ondermijning bewaard indien fase 1 t/m 4 van het protocol niet tot verdere aanpak van het signaal leidt;
 - b. Gedurende vijf jaar in de databaseomgeving bewaard en vervolgens een jaar in een niet-actieve omgeving bewaard indien een signaal in fase 5 resulteert in de aanpak van het signaal.
2. Op basis van een nieuw signaal kunnen de bewaarde persoonsgegevens ten behoeve van het nieuwe signaal worden geraadpleegd dan wel verwerkt en is het protocol van toepassing op de nieuwe verwerking.
3. De opgenomen gegevens kunnen voor evaluatie dan wel statistische doeleinden in niet tot individuele personen herleidbare vorm bewaard blijven, zoals is bepaald in artikel 89, lid 1 AVG jo artikel 9, lid 2, AVG en artikel 24 UAVG.

Artikel 8: rechten van betrokkenen

1. Een betrokkene heeft het recht om inzage te verzoeken in zijn gegevens en het gebruik daarvan door de gemeente.
2. De betrokkene kan de gemeente verzoeken de gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen, indien de gegevens feitelijk onjuist, onvolledig of niet ter zake dienend zijn voor het doel van de verwerking.
3. Een betrokkene heeft het recht verzet aan te tekenen in verband met zijn bijzondere persoonlijke omstandigheden.
4. De verzoeken als bedoeld in de leden 1 en 2 van dit artikel, alsmede het verzet als bedoeld onder 3 kunnen worden ingediend bij de beheerder. Deze reageert binnen vier weken op de verzoeken of het verzet genoemd in dit artikel.
5. Tegen een afwijzing van de verzoeken of het verzet kan de betrokkene bezwaar aantekenen.
6. De gemeente zal betrokkene op eerste verzoek nadere informatie toezenden over zijn rechten en de mogelijkheden deze uit te oefenen.
7. Het bovengemelde kan buiten toepassing worden gelaten voor zover dit noodzakelijk is in het belang van:
 - a. De veiligheid van de staat;
 - b. De voorkoming, opsporing en vervolging van strafbare feiten
 - c. Gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
 - d. Het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of
 - e. De bescherming van de betrokkene of van de rechten en vrijheden van anderen

Per geval vindt een afweging plaats. De betrokkene wordt nooit uit eigen beweging geïnformeerd. Hier wordt in algemene bewoordingen aandacht besteed in de privacyverklaring.

Artikel 9: informeren betrokkene

1. Indien een signaal, mono- of multidisciplinair door een onderdeel (onderdelen) van de gemeente wordt opgepakt, dan informeert het desbetreffende onderdeel (onderdelen) betrokkene conform wet- en regelgeving die van toepassing is op basis van de bij die taak behorende wet- en regelgeving.
2. Indien het signaal naar het RIEC-samenwerkingsverband wordt doorgezet dan geldt de procedure zoals deze is neergelegd in het privacy-protocol van het RIEC.
3. De verwerkingsverantwoordelijke laat op grond van art. 23 AVG jo artikel 41 UAVG informatieverstrekking achterwege voor zover dit noodzakelijk is in het belang van:
 - a. De nationale veiligheid, landsverdediging of openbare veiligheid.
 - b. De voorkoming, onderzoek, opsporing en vervolging van strafbare feiten, of tenuitvoerlegging van straffen.

- c. De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes.
- d. Voor gereglementeerde beroepenschendingen van de beroepscodes van gereglementeerde beroepen.
- e. Andere belangrijke doelstellingen van algemeen belang van Nederland of de Europese Unie.
- f. De bescherming van de onafhankelijkheid van rechters en rechterlijke procedures; en;
- g. Taken op het gebied van toezicht, inspectie of regelgeving op de hierboven genoemde gebieden, de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Uit oogpunt van transparantie is het uitgangspunt dat betrokkene zo snel en volledig mogelijk wordt geïnformeerd over het onderzoek dat naar hen wordt gedaan. Dat is echter niet altijd mogelijk en niet wenselijk, omdat het informeren het onderzoek kan schaden of onbedoeld het criminele netwerk blootlegt. Dan kan een beroep worden gedaan op één van de uitzonderingen, zoals genoemd in bovengenoemd artikel 9 lid 4, onder a en b.

In algemene zin wordt de betrokkene geïnformeerd over de mogelijkheid dat gegevens verder worden verwerkt ter bestrijding van ondermijning door middel van publicatie van dit protocol en de privacyverklaring van de gemeente Maashorst.

Na vaststelling zal het privacy protocol worden opgeslagen in het zaaksysteem van de gemeente Maashorst.

Indien werkprocessen of wet- en regelgeving worden aangepast en/of sprake is van nieuwe verschijningsvormen van ondermijning, kan dit van invloed zijn op de rechtmatigheid van de verwerkingen van persoonsgegevens. Dit kan leiden tot aanpassing van het privacy protocol (inclusief werkproces) ondermijning.