

PRIVACY PROTOCOL BESTUURLIJKE AANPAK ONDERMIJNING Gemeente Son en Breugel 2024

Het college van burgemeester en wethouders van Son en Breugel en de burgemeester van Son en Breugel, ieder voor zover het zijn bevoegdheden betreft;

Gelet op het bepaalde in de Algemene verordening gegevensbescherming (hierna: AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG);

De burgemeester is o.a. conform artikel 172 Gemeentewet belast met de handhaving van de openbare orde, waaronder de aanpak van ondermijning. Gezien er van gemeenten steeds meer verwacht wordt in de aanpak van georganiseerde ondermijnende criminaliteit op regionaal niveau –in het kader van de Taskforce-RIEC samenwerking - alsook lokaal in het kader van de eigen taakuitvoering (niet-faciliteren van criminaliteit), is dit Protocol ondersteunend in de aanpak van de georganiseerde ondermijnende criminaliteit. Voor een effectieve aanpak van deze ondermijnende activiteiten (en mogelijk georganiseerde criminaliteit) is een geïntegreerde bestuurlijke aanpak binnen de gemeente een vereiste. Om onder andere het intern delen van informatie op een juridisch correcte wijze uit te voeren, is dit Privacy Protocol opgesteld.

BESLUIT:

Vast te stellen het **Privacy Protocol bestuurlijke aanpak ondermijning gemeente Son en Breugel 2024**

Artikel 1. Definities

In dit Protocol wordt verstaan onder:

AVG	Algemene Verordening Gegevensbescherming
Signaal	Een aanwijzing of meerdere aanwijzingen dat bepaalde gedragingen en/of situaties mogelijk verband zouden kunnen houden met (verschijningsvormen van) georganiseerde ondermijnende criminaliteit dan wel dat zich bepaalde gedragingen en of situaties voordoen die mogelijk relevant zijn voor de toepassing van de Wet Bibob. Bijlage 2 bevat een nadere concretisering van wat een signaal kan inhouden.
Signaalregister	Een bestand waarin de signalen en de vervolgbehandeling van signalen worden vastgelegd.
Betrokkene	De identificeerbare natuurlijk persoon op wie de verwerkte en/of te verwerken persoonsgegevens betrekking hebben.
Functionaris	Functionaris, als genoemd in art. 37 t/m 39 van de AVG, belast met het toezicht op naleving van de AVG en van andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens, waaronder dit Protocol.
Handavingsknelpunt	Complexe casuïstiek of thema's waarbij een integrale aanpak vereist is, zoals: • Illegale activiteiten op woonwagencentra's; • Outlaw Motorcycle Gangs (OMG's); • Personen met ongebruikelijk bezit of personen van wie de levensstijl niet past bij het bekende inkomen; • Deelen of produceren van harddrugs of criminaliteit/witwassen in een specifieke branche zoals de automotive, transport en logistiek, kappers of horeca.
Lokaal Informatie Overleg (LIO)	Het LIO is het intern gemeentelijk overleg waarin domein overstijgende informatie over een signaal met elkaar gedeeld kan worden. Hierbij worden vaste functionarissen van verschillende afdelingen binnen de gemeente betrokken. De informatiecoördinator bestuurlijke aanpak ondermijning voert de regie over het overleg.
Melders	Personen en organisaties die een melding doen/een signaal afgeven waarbij mogelijk sprake is van ondermijning. Dit kan zowel een in- als externe melder zijn. Dit heeft ook betrekking op meldingen vanuit of naar de gemeenschappelijke regelingen.
Medewerker Bestuurlijke Aanpak (MBA) / Informatiecoördinator	Medewerker belast met: De overall regie op en advisering over ondermijning; De regie op en zorg voor gezamenlijke acties/interventies ter voorkoming of beëindiging van ondermijning; Het delen van signalen, coördineren van signaalfhandeling, beheer van het signaalregister en de coördinatie van gegevensuitwisseling en samenwerking met het RIEC.
Plan van aanpak Interventies	Een plan opgesteld door een gemeentelijk onderdeel of in gezamenlijkheid van gemeentelijke onderdelen ten behoeve van de uitvoering van wettelijke instrumenten om ondermijning te doen voorkomen, stoppen, verstoren, of verminderen.
Privacy Officer (PO)	Een functionaris die verantwoordelijk is voor advisering over en begeleiding van de uitvoering van maatregelen om de privacy van betrokkenen te waarborgen bij de verwerking van persoonsgegevens door gemeente Son en Breugel.
Functionaris Gegevensbescherming (FG)	Een functionaris als genoemd in hoofdstuk IV, afdeling 4 van de AVG. Deze functionaris is belast met het toezicht op de naleving van dit Protocol.
Organisatieonderdeel	Een afdeling, team of (een of meerdere) functionaris(en) van de gemeente.

Ondermijning

Er is geen exacte definitie van ondermijning te geven. Globaal betekent het de vermindering van de onderwereld met de bovenwereld, de sluipende bedreiging van de integriteit van het openbaar bestuur, overheidsambtenaren en bedrijfsleven, bedreigde bestuurders en ambtenaren, afpersingspraktijken, de instelling van criminele fenomenen in buurten en woonwijken. Criminelen hebben de 'bovenwereld' nodig voor het bewerkstelligen van hun criminele activiteiten. Het zijn de maatschappelijke gevolgen van georganiseerde criminaliteit waarin de gemeente een gezamenlijke verantwoordelijkheid heeft. In bijlage 2 is uitgewerkt wat verstaan wordt onder ondermijnende activiteiten.

UAVG

Uitvoeringswet Algemene verordening gegevensbescherming

Waar in dit Protocol termen worden gebruikt die overeenstemmen met definities uit artikel 4 AVG wordt aan deze termen de betekenis van de definities uit de AVG toegekend.

Artikel 2. Doel bestuurlijke aanpak ondermijning: duurzaam terugdringen

Onze taak in de gemeente Son en Breugel is om onze inwoners, organisaties en hun integriteit te beschermen tegen ondermijnende invloeden. Door zicht te krijgen op ondermijnende invloeden, kan ingezet worden op de schakel waar de ondermijnende keten het beste verstoord kan worden. Het doel van deze aanpak is om binnen de gemeente Son en Breugel door middel van samenwerking:

- a. Ondermijnende criminaliteit te signaleren en te analyseren;
- b. Te voorkomen dat de gemeente ondermijnende activiteiten (on)bewust faciliteert;
- c. Vroegtijdig te kunnen signaleren en interveniëren door middel van een bestuurlijke- en eventueel integrale aanpak;
- d. Onrechtmatigheden en maatschappelijke bedreigingen door criminele activiteiten preventief te voorkomen en repressief aan te pakken.

Op deze manier dringen we ondermijnende criminaliteit structureel en duurzaam terug. Deze aanpak richt zich op personen, bedrijven en netwerken die binnen Son en Breugel actief zijn in ondermijnende-, illegale- en/of onrechtmatige activiteiten. De aanpak draagt bij aan de leefbaarheid en veiligheid van Son en Breugel en verhoogt de weerbaarheid voor zowel de samenleving als de overheid. Tevens wordt hiermee de kans op het (on)bewust faciliteren van ondermijnende criminaliteit gereduceerd.

Artikel 3. 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 Son en Breugel bij deze aanpak zijn/haar persoonsgegevens verwerkt en met welk doel dat gebeurt.

Artikel 4. Doel van de gegevensverwerking

Het doel van de verwerking van persoonsgegevens die deel uitmaken van een of meerdere signalen is:

1. Te voorkomen dat organisatieonderdelen bij de uitvoering van gemeentelijke taken (onbewust) ondermijning faciliteren;
2. De organisatieonderdelen in staat stellen bij de uitvoering van hun taken, waar nodig, bestuursrechtelijke instrumenten in te zetten voor het bestrijden van ondermijning binnen hun eigen vakgebied c.q. team;
3. Organisatieonderdelen door de MBA bij te laten staan en te laten adviseren bij het bereiken van de doelen als genoemd in lid 1 en lid 2 van dit artikel.

Artikel 5. Verwerkingsverantwoordelijke

1. Het College van Burgemeester en Wethouders van de gemeente Son en Breugel is verwerkingsverantwoordelijke voor verwerkingen van persoonsgegevens die plaatsvinden binnen de gemeente en waarvoor zij als verwerkingsverantwoordelijke zijn aangemerkt in het Register van verwerkingsactiviteiten Son en Breugel.
2. Het College van Burgemeester en Wethouders van de gemeente Son en Breugel is verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens die plaatsvinden in het kader van de registratie van en afhandeling van signalen.

Artikel 6. De Privacy Officer

1. De Privacy Officer adviseert de verwerkingsverantwoordelijke over:
 - a. De inhoud van het onderhavig privacy Protocol en haar bijlagen;
 - b. De uitwisseling van gegevens als bedoeld in artikel 7 van dit Protocol, in die gevallen dat niet eenduidig is vast te stellen of de gegevensuitwisseling rechtmatig kan plaatsvinden.

2. De MBA stemt af met de Privacy Officer. De Privacy Officer stemt zo nodig het advies als bedoeld in lid 1 van dit artikel af met de functionaris gegevensbescherming.

Artikel 7. 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 (artikel 6 lid 1 onder e AVG). De wettelijke onderbouwing hiervoor is terug te vinden in onder andere de hieronder genoemde (niet uitputtend) artikelen. Per casus vinden privacy checks plaats om te bepalen of de verwerking noodzakelijk is en of er wordt voldaan aan subsidiariteit en proportionaliteit. Het gaat om de volgende bepalingen in de Gemeentewet:

- Artikel 151 d (Wet aanpak woonoverlast)
- Artikel 170 lid 2 (Bestuurlijke integriteit)
- Artikel 172 (Handhaving openbare orde)
- Artikel 172a en b (Gebiedsverboden, groepsverboden, meldplicht bij verstoren openbare orde)
- Artikel 174a (Het sluiten van een woning wegens verstoren openbare orde)
- Artikel 174b (Aanwijzen veiligheidsrisicogebied)
- Artikel 175 (Noodbevel)
- Artikel 176 (Noodverordening)

Daarnaast heeft de burgemeester meer specifieke bevoegdheden op grond van onder andere de volgende wetten:

- Artikel 13b Opiumwet (Sluiten woning wegens aantreffen middelen op lijst I/II Opiumwet)
- Wet tijdelijk huisverbod (Opleggen van een huisverbod bij (dreiging van) huiselijk geweld)
- Wet Bibob (Integriteitsbeoordeling bij een vergunningaanvraag, subsidieverstreking, aangaan overeenkomst of vastgoedtransactie)

Het kan voorkomen dat politie informatie wordt betrokken bij het bespreken van casuïstiek. De Wet politiegegevens (hierna: Wpg) regelt de verwerking van politiegegevens. Politiegegevens zijn persoonsgegevens die worden verwerkt in het kader van de uitoefening van de politietaken (artikel 1, sub a, Wpg). De Wpg voorziet naast bepalingen over de verwerking van gegevens binnen de politie, ook in bepalingen over de verstrekking van politiegegevens aan anderen buiten de politie, waaronder aan gezagdragers. Onder gezagdragers vallen ingevolge artikel 16, lid 1, sub b, Wpg ook burgemeesters.

Artikel 8. Categorieën van betrokkenen en de verwerkte persoonsgegevens

1. Van een melder worden uitsluitend in het bestand geregistreerd de voornaam of voorletter en achternaam, en de voor communicatie benodigde gegevens, te weten een emailadres en/of telefoonnummer, voor zover die in het signaal zijn opgenomen. Deze gegevens worden verwerkt ten behoeve van communicatie tussen teams binnen de gemeente.
2. Van de personen over wie wordt gemeld (betrokkene), genoemd in Bijlage 2 'Categorieën personen als onderdeel van de checklist beoordelen signalen Ondernijning' worden in verschillende fases de gegevens verwerkt zoals genoemd in de Bijlage 1 'categorieën van verwerkte gegevens' en Bijlage 1.1 'Vervolgfases' behorend bij dit Protocol.
3. De in bijlage 1 bedoelde categorieën van persoonsgegevens worden gebruikt voor:
 - afhandeling van het signaal of;
 - het (mono- of multidisciplinair) oppakken van het signaal binnen de eigen kaders door de gemeentelijke vak afdelingen of -teams en/of;
 - de verdere aanpak van ondernijning onder regie van de MBA en/of ;
 - het verstrekken van het signaal binnen het Taskforce-RIEC-samenwerkingsverband.

Artikel 9. Categorieën van ontvangers

1. Voor zover noodzakelijk voor de genoemde doelen, kunnen door de MBA gegevens worden verstrekt aan:
 - a. gemeentelijke organisatieonderdelen ten behoeve van
 - i. signaalverrijking of het opstellen van een plan van aanpak door de MBA;
 - ii. de voorkoming en bestrijding van ondernijning bij de uitvoering van hun wettelijke taak, of;
 - b. aan een of meerdere partners die deelnemen aan de Taskforce-RIEC-samenwerking.
2. Voor zover noodzakelijk voor genoemde doelen, kunnen organisatieonderdelen gegevens uit de onder hun verantwoordelijkheid tot stand gekomen gegevensverwerkingen verstrekken aan de MBA.
3. De MBA en de organisatieonderdelen toetsen de noodzaak tot verstrekking als bedoeld in lid 1 respectievelijk lid 2 van dit artikel aan de hand van de criteria als genoemd in bijlage 1. De uitslag van de toets wordt vastgelegd in het signaaldocument.

Artikel 10. Beheer en toegang tot het bestand

1. De MBA van de gemeente Son en Breugel is verantwoordelijk voor het beheer van het signalen register. De MBA draagt zorg voor het dagelijks beheer van het bestand, waaronder de beveiliging van de persoonsgegevens, de informatieverstrekking aan betrokkene en de afhandeling van de door betrokkene uitgeoefende rechten, het bewaken van de bewaartermijnen en het vernietigen van de gegevens na het verstrijken van de bewaartermijn.
2. Het feitelijk beheer van de verwerking van persoonsgegevens en feitelijke naleving van de informatieplicht is opgedragen aan de MBA alsook de afhandeling van de door betrokkene uitgeoefende rechten.
3. Uitsluitend de MBA, diens plaatsvervanger en de eventueel administratief ondersteuner hebben toegang tot het signalenregister.

Artikel 11. Beveiliging van persoonsgegevens

De beheerder draagt zorg voor passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, gebaseerd op de Baseline informatiebeveiliging Overheid (B10).

Hiertoe behoren in ieder geval:

- Vastgesteld beveiligingsbeleid dat ook is geïmplementeerd, en;
- Fysieke maatregelen voor toegangsbeveiliging inclusief organisatorische controle, en;
- Logische toegangscontrole (zoals wachtwoord, 2 FA en pincode).

Artikel 12. Bewaartermijn en verwijdering

1. De gegevens in het signalenregister worden bewaard:
 - a. Gedurende een jaar in een inactieve omgeving indien fase 1 en/of 2 van het Protocol niet tot verdere aanpak van het signaal leiden;
 - b. Gedurende 2 maanden na de laatste verwerking in een actieve omgeving indien een signaal in een gemeentelijk casusoverleg (fase 4) resulteert.
2. Bij heropening van een inactief signaal kunnen de bewaarde persoonsgegevens vanuit het oude signaal worden geraadpleegd dan wel verwerkt en is het Protocol van toepassing op het nieuwe signaal.
3. De gegevens worden verwijderd binnen één maand na beëindiging van de bewaartermijn. De MBA ziet toe op de naleving van de bewaartermijnen.
4. De bewaartermijn voor gegevens over ondermijning die de organisatieonderdelen verwerken in het kader van de uitvoering van taken is gelijk aan de bewaartermijnen die gelden volgens de in de archiefwet vastgelegde selectielijsten.

Artikel 13. Informatieplicht

1. De informatieverplichting zoals bedoeld in artikel 14 van de AVG is niet van toepassing op de verwerking van persoonsgegevens van betrokkene in het bestand, omdat het achterwege laten van het informeren van betrokkene noodzakelijk is ter waarborging van:
 - a. de nationale veiligheid;
 - b. de voorkoming, het onderzoek, de 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.
2. De organisatieonderdelen voldoen aan de informatieverplichting zoals bedoeld in artikel 14 AVG overeenkomstig de informatieverplichting die van toepassing zijn op de reguliere uitvoeringspraktijk.

Artikel 14. Rechten van betrokkenen

1. Een betrokkene heeft het recht op inzage 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 in verband met zijn bijzondere persoonlijke omstandigheden het recht bezwaar te maken tegen de verwerking van zijn persoonsgegevens.

4. De verzoeken als bedoeld in de leden 1 en 2 van dit artikel, alsmede het bezwaar als bedoeld in lid 3 kunnen worden ingediend bij de verwerkingsverantwoordelijke. Deze reageert binnen één maand op de verzoeken of het bezwaar genoemd in dit artikel.
5. Op de schriftelijke besluiten die de verantwoordelijke neemt op verzoeken op grond van de leden 2, 3 en 4 van dit artikel 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.

Artikel 15. Beperking van de informatieplicht en de rechten van de betrokkene

1. De informatieverplichting aan betrokkene zoals bedoeld in artikel 14 van de AVG en de rechten van de betrokkene, zoals bedoeld in artikel 13 en 14 van dit Protocol kunnen worden beperkt als dit noodzakelijk is ter waarborging van:
 - a. de nationale veiligheid;
 - b. de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen met inbegrip van de bescherming tegen en voorkoming van gevaren voor de openbare veiligheid;
 - 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;
 - e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen of;
 - f. de openbare veiligheid.
2. De MBA legt de motivatie voor het niet voldoen aan de informatieplicht op grond van lid 1 van dit artikel schriftelijk vast en legt vast wanneer naar verwachting betrokkene wel geïnformeerd kan worden, alsook van welke omstandigheden dit afhankelijk is, hoe periodiek wordt getoetst of deze omstandigheden nog aanwezig zijn en hoe de betrokkene geïnformeerd zal worden.

Artikel 16 Bijlagen

De bij dit Protocol gevoegde bijlagen maken deel uit van dit Protocol.

Artikel 17. Looptijd en evaluatie

Dit Protocol geldt voor 2 jaar, met stilzwijgende verlenging van telkens één jaar.

De verwerking van persoonsgegevens waarop dit Protocol van toepassing is, zal jaarlijks worden geëvalueerd. Eventuele wijzigingen zullen door Het College van Burgemeester en Wethouders (de verwerkingsverantwoordelijke) vastgesteld worden.

Artikel 18. Datum inwerkingtreding

Dit Protocol treedt in werking op de eerste dag na de datum van bekendmaking. Het Protocol van 22 november 2022 wordt tegelijkertijd ingetrokken.

Artikel 19. Citeertitel

Dit Protocol kan worden aangehaald als: "Privacy Protocol bestuurlijke aanpak ondermijning Son en Breugel 2024"

Aldus vastgesteld op 27 augustus 2024 door het college van burgemeester en wethouders van de gemeente Son en Breugel.

De secretaris, De burgemeester,

Jeroen Wesselink Suzanne Otters-Bruijnen

BIJLAGE 1: Categorieën van de verwerkte persoonsgegevens

Van de personen over wie wordt gemeld, kunnen onderstaande gegevens, afhankelijk van de inhoud van de melding of het signaal in de verschillende fases worden verwerkt en geregistreerd in het signaalregister. Borging vindt plaats door registratie van de te verwerken persoonsgegevens in het verwerkingsregister waardoor wordt voldaan aan de AVG-eisen.

Fase 1: Ontvangst en intake van het signaal

In fase 1 van de uitvoering van de bestuurlijke aanpak van ondermijning zijn dit de volgende gegevens:

1. De (anonieme) melding c.q. het ontvangen signaal en de daarin van melder en betrokkene opgenomen persoonsgegevens zoals naam, adres en contactgegevens.
2. Of er sprake is van ondermijning zoals bedoeld in bijlage 2:
 - a. eventuele aanwijzingen voor ondermijning uit de eerste weging van het onderzoek,
 - b. het eventuele vervolg dat aan het onderzoek wordt gegeven,
 - c. het thema van ondermijning dat van toepassing is op het signaal (bijv. hennep, mensenhandel, fraude of witwassen),
3. Gegevens over mogelijke betrokkenheid van de betrokkene als eigenaar, directeur, bestuurder van een bedrijf of ander rechtspersoon, afkomstig uit het KVK Handelsregister.
4. Gegevens over mogelijke eigendomsrechten van de betrokkene uit de openbare registers van het Kadaster.
5. De bestemming van het adres of locatie waarmee betrokkene in relatie wordt gebracht en de gebruiksmogelijkheden van het adres of de locatie, gebaseerd op het voor het gebied geldende bestemmingplan.
6. Informatie over betrokkene aangetroffen op het internet, zowel door betrokkene zelf als door derden geplaatst. Dit betreft alleen openbare informatie.
7. Informatie/bevindingen die voortvloeien uit de vergelijking van de feitelijke afmetingen van een object op de locatie of het adres waarmee betrokkene in relatie wordt gebracht met dezelfde gegevens op luchtfoto's van het object.

Fase 2: Zwaarte van het signaal bepalen

In fase 2 van de uitvoering van de bestuurlijke aanpak van ondermijning kunnen in aanvulling op gegevens uit fase 1 onderstaande gegevens worden verwerkt, afhankelijk van de melding en of relevante casusinformatie:

1. Basisgegevens over een locatie of adres en een daarop gebouwd object uit de Basisregistratie Adressen en Gebouwen (BAG);
2. Naam, adres van betrokkene zoals ingeschreven in de Basisregistratie personen (BRP) en gegevens over de aanduiding of een adres waarmee betrokkene in relatie wordt gebracht wel/niet in onderzoek staat en mogelijke andere signalen van de BRP-controleur;
3. Informatie over vergunningaanvragen, inhoudelijke behandeling, verleende vergunningen en eventuele intrekingsbesluiten, waarmee betrokkene in relatie kan worden gebracht;
4. Inkomensgegevens uit systemen van uitkeringen, hulpmiddelen WMO, zorgbudget (PGB) van werk en inkomen (gesloten bron). Bijv. Is er wel/niet een uitkering aangevraagd en/of verstrekt (uitkeringsinformatie)? Zijn er andere bronnen van inkomsten en zo ja welke soort? (geen volledige SUWI-net gegevens en niet de hoogte van andere uitkeringen zoals bijv. WAO- of WW-uitkering);
5. Informatie uit systemen van de vak afdeling Toezicht en Handhaving over opgelegde dwangsommen, bestuursdwang of andere handhavingstrajecten;
6. Informatie uit systemen van Toezicht en Handhaving over uitgevoerde controles;
7. Informatie uit systemen over andersoortige beschikkingen zoals APV-zaken (bv Alcoholwet (gesloten bron));
8. Informatie uit systemen van de vak afdeling Veiligheid, zoals eerder ontvangen bestuurlijke rapportages van partners of bekende informatie uit het RIECIS-systeem over het pand, adres of de betrokken persoon in het kader van het vaststellen van de classificatie recidive (gesloten bron);
9. Informatie (straat informatie) bekend bij interne functionarissen;
10. Informatie van de leerplichtambtenaar over het betreffende adres of de persoon/gezin (is er wel/niet sprake van schoolverzuim?).

BIJLAGE 1.1: Vervolgfases

Fase 3: hit/no hit

Als er in een (bron)bestand van een gemeentelijke afdeling gegevens over een persoon of organisatie die in het signaal voorkomen bekend zijn, geeft de afdeling dit aan bij de MBA en levert gegevens die de MBA nodig heeft om te beoordelen of deze gegevens het signaal bevestigen of versterken. Indien dit het geval blijkt te zijn dan is er een 'hit'. Dit betreft zogeheten 'dat' informatie en geen 'wat' informatie. Voor afdelingen die werkzaam zijn in het sociaal domein houdt dit in dat zij slechts de zogenaamde buitenkant informatie verschaffen, te weten het feit dat een persoon bekend is bijvoorbeeld als cliënt. De inhoud van het dossier (de wat-informatie) blijft echter gesloten voor de MBA, omdat de sociaal domeinwetgeving (Participatiewet, WMO, Jeugdwet) geheimhoudingsverplichtingen kent, waardoor verstrekking van persoonsgegevens niet is toegestaan buiten een in de wet genoemde kring van personen en instanties.

Fase 4: vervolgaanpak

Als duidelijk is dat er sprake is van een 'hit' en er meer informatie moet worden verzameld dan zijn er verschillende acties mogelijk te weten:

- a. Lokaal informatie-overleg beleggen door de MBA waarin interne informatie met elkaar gedeeld wordt;
- b. Een bestuurlijke en/of integrale controle laten uitvoeren door een BOA/Toezichthouder of het Dommelstroom Interventie Team;
- c. Het delen van informatie met Taskforce-RIEC-partner(s), verrijking door Taskforce-RIEC en bestempelen tot integrale Taskforce-RIEC casus.

BIJLAGE 2 Categorieën personen/bedrijven als onderdeel van de checklist beoordelen signalen Ondernijning

Deze checklist bestaat uit twee onderdelen:

1. Een overzicht van criminele (en niet-criminele) activiteiten en de rol van personen of bedrijven die daarin (al dan niet bewust) betrokken kunnen zijn;
2. Kenmerken van ondernijnende criminaliteit.

Aan de hand van deze checklist beoordeelt de MBA of een signaal betrekking kan hebben op ondernijning. De beoordeling bestaat uit twee stappen:

1. Welke rol vervult een persoon of bedrijf die in een signaal wordt genoemd en kan die persoon of bedrijf in diens rol in relatie worden gebracht tot de vermeende criminele activiteit?;
2. Voldoet het signaal aan de kenmerken van ondernijnende criminaliteit?

De inhoud van de checklist is afhankelijk van maatschappelijke ontwikkelingen en kan derhalve niet als limitatief worden beschouwd.

Categorieën van personen:

De MBA registreert persoonsgegevens van personen die in hun hoedanigheid, als beschreven in de onderstaande lijst, mogelijk betrokken kunnen zijn bij de omschreven criminele activiteit.

Omschrijving van de (criminele) activiteiten en rollen van daarbij (al dan niet bewust) betrokken personen of bedrijven

Algemeen ondernijnende activiteiten:

- a. Faciliteerders die ondernijnende of criminele activiteiten mogelijk maken en/of (on)bewust in stand houden;
- b. Personen of bedrijven die een rol spelen bij een regionaal thema, kwetsbare branche/doelgroep of een handhavingsknelpunt zoals:
 - Autobedrijven
 - Transport en Logistiek
 - Outlaw Motorcycle Gangs (OMG's): leden van OMG's
 - Woonwagenlocaties: eigenaren woonwagens, huurders, bewoners
 - Aanpak in het buitengebied
 - Personen met ongebruikelijk bezit
 - Hard- en softdrugs

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

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Bewoner
- e. Eigenaar (illegale) seksinrichting
- f. Eigenaar (illegale) massagesalon
- g. Illegaal werkende prostituee (d.w.z. zonder vergunning)
- h. Exploitant en beheerder van een vergunde seksinrichting
- i. Bewaking
- j. Kassier
- k. Financier

Georganiseerde hennepcultuur/drugs(-handel)

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Bewoner
- e. Tussenpersoon (verhuurmakelaar, evt. andere vormen)
- f. Transporteur
- g. Electromonteur
- h. Financier

Fraude 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. Notaris
- g. Financier

Misbruik in de vastgoedsector

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

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 of vergunningen vanuit de gemeente
- d. Een tussenpersoon/gemachtigde met betrekking tot zorg
- e. Pandeigenaar
- f. Huurder
- g. Verhuurder
- h. Bewoner
- i. Financier

Openbare inrichtingen

- a. Pandeigenaar
- b. Verhuurder
- c. Huurder/pachter
- d. Exploitant
- e. Beheerder/leidinggevende
- f. Tussenpersoon
- g. Geldschietters

Kenmerken van ondermijnende criminaliteit

Voor de bepaling of sprake kan zijn van ondermijnende criminaliteit bekijkt de MBA of het signaal een van de onderstaande kenmerken bevat:

- Aantasting van instituten die zich richten op legale perspectieven en de werking van het samenlevingssysteem borgen en sturen;
- Aantasting van de gezagspositie van het bestuur, politie of andere overheidsorganen;
- Aantasting of mogelijke aantasting van de openbare orde en veiligheid;
- Aantasting of mogelijke aantasting c.q. ontwijking van de maatschappelijke, politieke of economische structuren;
- Onrechtmatigheden/overtredingen;
- Maatschappelijke bedreigingen en/of mogelijke georganiseerde criminaliteit;
- Vermoeden van strafbare feiten;
- Vermoeden van boetewaardig gedrag (bestuurlijke boete);
- Hinder of overlast door overschrijding van de normen, regels of het niet naleven daarvan;
- Aantasting van de veiligheid en leefbaarheid in de wijk door (vermoedens) van ondermijnende activiteiten;
- Er is sprake van een van de bovenstaande locatie-, persoons- en/of bedrijfsgebonden indicatoren binnen het grondgebied van de gemeente Son en Breugel;
- Gelegenheidsstructuren (of criminaliteit bevorderende condities) in de maatschappelijke omgeving, fysieke omgevingskenmerken, sociale relaties of netwerken of in de zakelijke omgeving;
- Vermoedens van het bewust of onbewust faciliteren van ondermijnende criminaliteit.