Geldrop-Mierlo

GEMEENTEBLAD

Officiële uitgave van de gemeente Geldrop-Mierlo

Nr. 100121

8 maart

2023

Privacyprotocol gegevensdeling bestuurlijke aanpak ondermijnende criminaliteit Geldrop-Mierlo 2023

Het college van burgemeester en wethouders van Geldrop-Mierlo en de burgemeester van Geldrop-Mierlo, 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);

Overwegende dat van gemeenten meer verwacht wordt in de aanpak van georganiseerde ondermijnende criminaliteit regionaal, 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 noodzakelijk vereiste.

BESLUIT:
Vast te stellen:

Artikel 1 Definities

In dit protocol wordt verstaan onder:

AVG	Algemene verordening gegevensverwerking.
Ondermijning	Er is geen exacte definitie van ondermijning te geven. Globaal betekent het de vermenging van de onderwereld met en in de bovenwereld, de sluipende bedreiging van de integriteit van het openbaar bestuur, overheidsambtenaren en bedrijfsleven, bedreigde bestuurders en ambtenaren, afpersingspraktijken, de innesteling van criminele fenomenen in buurten en woonwijken of het ontstaan van 'vrijplaatsen'. Criminelen hebben de 'bovenwereld' nodig voor het faciliteren van hun criminele activiteiten. Het is een maatschappelijk probleem waar de gemeente mee te maken heeft. In bijlage 2 is uitgewerkt wat verstaan wordt onder ondermijnende activiteiten.
Signaal	Een signaal is een aanwijzing of meerdere aanwijzingen dat bepaalde gedragingen en/of situaties mogelijk verband zouden kunnen houden met (verschijningsvormen van) georganiseerde criminaliteit. Of dat zich een handhavingsknelpunt voordoet of dat bepaalde gedragingen en of situaties mogelijk relevant zijn voor de toepassing van de Wet Bibob. Bijlage 2 bevat een nadere concretisering van wat een signaal kan inhouden.
Plan van aanpak/ Interventies	Door een gemeentelijk onderdeel of in gezamenlijkheid van gemeentelijke onderdelen schrijven van een plan ten behoeve van uitvoering van de wettelijke instrumenten om ondermijning te stoppen, te verstoren of te verminderen. Vanaf fase 3 of 4 van het model kan de Taskforce-RIEC hierbij betrokken worden omdat de keuze gemaakt wordt om de casus integraal op te pakken met (ook) externe partners zoals de politie, het OM en de belastingdienst.
Lokaal informatie-overleg	Het lokaal informatieoverleg is het intern gemeentelijk overleg dat op een signaal kan volgen. Hierbij worden vaste contactpersonen van verschillende afdelingen binnen de gemeente betrokken. Een uitkomst kan zijn dat er een vervolgonderzoek komt. De informatiecoördinator bestuurlijke aanpak ondermijning voert de regie over het dit overleg en stelt vervolgens een plan van aanpak wordt op. Dit is de start van fase 4 van het proces.
Melders	Personen en organisaties die een melding doen/ een signaal afgeven van mogelijke ondermijning. Dit kan zowel een in- als externe melder zijn. Dit heeft ook betrekking op meldingen vanuit of naar de gemeenschappelijke regelingen.
Betrokkene	In dit protocol wordt hieronder verstaan een persoon waarop een signaal betrekking heeft of kan hebben. De identificeerbare natuurlijk persoon op wie de verwerkte en/of de te verwerken persoonsgegevens betrekking hebben.
Signalenregister	Een bestand waarin de signalen en de vervolgbehandeling van signalen worden vastgelegd.
Medewerker openbare orde en veiligheid	Medewerker belast met: De overall regie op en advisering over veiligheid en ondermijning.
Informatiecoördinator ondermijning	Heeft de regie op en zorg voor gezamenlijke acties/interventies ter voorkoming of beëindiging van ondermijning Deelt signalen, coördineert de signaalafhandeling, beheert het signalenregister en coördineert de gegevensuitwisseling en samenwerking met de Taskforce-RIEC.
Privacy adviseur	Functionaris belast met de advisering over privacy in de gemeente Geldrop-Mierlo
Functionaris gegevensbescherming	Functionaris als genoemd in hoofdstuk IV, afdeling 4 van de AVG. Deze functionaris is belast met het toezicht op de naleving van dit protocol

Handhavingsknelpunt zoals:
- Woonwagencentra: eigenaren woonwagens;
- Outlaw Motorcycle Gangs (OMG's): leden van OMG's;

– Huurders, bewoners; personen met ongebruikelijk bezit of personen van wie de levensstijl niet past bij het bekende inkomen;
– Harddrugs of een specifieke branche zoals de autobranche, kappers of wellnessdiensten.

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 ondermijnende criminaliteit: duurzaam terugdringen
Onze taak in de gemeente Geldrop-Mierlo is om onze inwoners, organisaties en hun integriteit te beschermen tegen ondermijnende invloeden. Op deze manier dringen we ondermijnende criminaliteit duurzaam terug. Door zicht te hebben op ondermijnende invloeden, kunnen we inzetten daar waar de ondermijnende keten het beste verstoord kan worden. Het doel van deze aanpak is om binnen de gemeente Geldrop-Mierlo door middel van samenwerking:
a. Ondermijnende criminaliteit te signaleren en te analyseren;
b. Te voorkomen dat de gemeente ondermijnende activiteiten onbewust faciliteert;
c. Vroegtijdig te kunnen signaleren en interveniëren door middel van een bestuurlijke aanpak;
d. Onrechtmatigheden en maatschappelijke bedreigingen veroorzaakt door criminele activiteiten te voorkomen.

Het gaat bij deze aanpak om personen/netwerken die binnen Geldrop-Mierlo actief zijn in illegale en of onrechtmatige activiteiten waarbij het doel is:
a. Het zo impactrijk mogelijk aanpakken van ondermijnende criminaliteit en ondermijnende invloeden. Deze aanpak draagt bij aan de leefbaarheid en veiligheid en is gericht op het bereiken van een zo groot mogelijk maatschappelijk effect.
b. Ondermijnende criminaliteit te signaleren en analyseren waardoor een goede gemeentelijke informatiepolitie ontstaat welke bijdraagt aan de voorfase van de Taskforce-RIEC samenwerking en ook bijdraagt aan een weerbare overheid. Hiermee minimaliseren we de kans dat we als gemeente (on)bewust ondermijnende criminaliteit faciliteren.

Artikel 3. Doel van protocol
De bestuurlijke aanpak van ondermijnende criminaliteit dient met inachtneming van wet- en regelgeving op het gebied van privacy- en gegevensbescherming plaats te vinden. Dit protocol heeft als doel de benodigde waarborgen daarvoor te bieden en verantwoording daarover af te leggen (conform het advies van de Raad van State d.d. 20 maart 2019). Daarom is dit protocol in fases ingericht, zodat de gegevensverwerking beperkt wordt tot dat wat noodzakelijk is voor het doel waarvoor de gegevens worden verwerkt. Dit protocol biedt een betrokkene inzicht in de wijze waarop de gemeente Geldrop-Mierlo bij deze aanpak 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 de taken (ongewild) meewerken aan ondermijning.
2. Organisatieonderdelen in staat te 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 informatiecoördinator ondermijning 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 en de burgemeester van de gemeente Geldrop-Mierlo zijn ieder voor zich verwerkingsverantwoordelijke voor verwerkingen van de persoonsgegevens die plaatsvinden binnen de gemeente en waarvoor zij als verwerkings-verantwoordelijke zijn aangemerkt in de wet- en regelgeving.
2. De burgemeester en het college van burgemeester en wethouders van de gemeente Geldrop-Mierlo zijn gezamenlijk verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens die plaatsvindt in het kader van de registratie en afhandeling van signalen.

Artikel 6. De privacy adviseur
1. De privacy adviseur adviseert de verwerkingsverantwoordelijke over:
   a. De inhoud van dit privacyprotocol 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 informatiecoördinator stemt af met privacy adviseur. De privacy adviseur stemt zo nodig het advies als bedoeld in lid 1 sub b van dit artikel af met de functionaris gegevensbescherming.

Artikel 7. Grondslag voor de verwerking

De grondslag voor de verwerking van (persoonsgegevens die deel uitmaken van) signalen is dat de gegevensverwerking noodzakelijk is voor de goede uitvoering van de gemeentelijke taken van de gezamenlijke verwerkingsverantwoordelijken. Namelijk het voorkomen dat de verwerkingsverantwoordelijken ongewild meewerken aan ondermijning of het bestrijden van ondermijning met bestuursrechtelijke instrumenten. In de toelichting is opgenomen welke persoonsgegevens worden verstrekt, voor elk doel, aan wie en welke grondslag er is om deze gegevens te verstrekken.

Artikel 8. Categorieën van betrokkenen en de verwerkte persoonsgegevens

1. Van een melder wordt in het signalenregister alleen geregistreerd de voornaam of voorletter en achternaam en de voor communicatie benodigde gegevens, 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, genoemd in bijlage 2 ‘Categorieën personen als onderdeel van de checklist beoordelen signalen Ondermijning’ worden in verschillende fases de gegevens verwerkt zoals genoemd in de fases bij bijlage 1 ‘categorieën van verwerkte gegevens’ behorend bij dit protocol.
3. De in bijlage 1 bedoelde categorieën van persoonsgegevens worden gebruikt voor:
   a. de afhandeling van een signaal;
   b. het (mono- of multidisciplinair) oppakken van een signaal binnen de eigen kaders door de gemeentelijke vakafdelingen of -teams;
   c. de verdere aanpak van ondermijning onder regie van de teammanager leefbaarheid en veiligheid.
   d. Het verstrekken van een signaal binnen het Taskforce-RIEC-samenwerkingsverband.

Artikel 9. Categorieën van ontvangers

1. Voor zover noodzakelijk voor de genoemde doelen, kunnen door de informatiecoördinator gegevens uit het signalenregister worden verstrekt aan:
   a. gemeentelijke organisatieonderdelen ten behoeve van;
      i. signaalverrijking of het opstellen van een plan van aanpak door de informatiecoördinator,
      ii. de voorkoming en bestrijding van ondermijning bij de uitvoering van hun wettelijke taak, of;

   b. aan een of meerdere partners die deelnemen aan de RIEC-samenwerking.

2. Voor zover noodzakelijk voor genoemde doelen, kunnen organisatieonderdelen gegevens uit de onder hun verantwoordelijkheid tot stand gekomen gegevensverwerkingen verstrekken aan de informatiecoördinator.
3. De informatiecoördinator 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 de databestanden

1. De Teammanager Leefbaarheid en Veiligheid van de gemeente Geldrop-Mierlo is verantwoordelijk voor het beheer van het signalenregister. Hij draagt zorg voor het dagelijks beheer van het signalenregister waaronder de beveiliging van de persoonsgegevens, de informatieverstrekking aan betrokkenen 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 informatiecoördinator alsook de afhandeling van de door betrokkene uitgeoefende rechten.
3. Uitsluitend de informatiecoördinator, diens plaatsvervanger en de medewerkers openbare orde en veiligheid hebben toegang tot het signalenregister.

Artikel 11. Beveiliging van persoonsgegevens

De beheerder draagt zorg voor en het management is verantwoordelijk 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 (BIO). Hiertoe behoren in ieder geval:

- Vastgesteld beveiligingsbeleid dat ook is geïmplementeerd;

- Fysieke maatregelen voor toegangsbeveiliging inclusief organisatorische controle;
- Logische toegangscontrole (wachtwoord, 2 FA of pincode).

Artikel 12. Bewaartermijn en verwijdering

1. De gegevens in het signalenregister worden bewaard:
   a. Gedurende een jaar in een niet-actieve 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 resulteert;

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 gegevens worden verwijderd binnen één maand na beëindiging van de bewaartermijn. De informatiecoördinator ziet toe op de naleving van de bewaartermijnen.
4. De bewaartermijn voor gegevens over ondermijning die organisatieonderdelen verwerken in het kader van de uitvoering van taken is gelijk aan de termijnen die voor die taken gelden volgens de in de archiefwet vastgelegde selectielijsten.

Artikel 13. Informatieplicht

1. De informatieverplichting aan betrokkene zoals bedoeld in artikel 14 van de AVG kan 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 regen 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 informatiecoördinator legt de motivatie voor het niet voldoen aan de informatieplicht op grond van lid 1 van dit artikel schriftelijk vast en legt vast wanneer zij verwacht dat betrokkene wel geïnformeerd kan worden, alsook van welke omstandigheden dit afhankelijk is, hoe periodiek wordt getoetst of deze omstandigheden nog aanwezig zijn en hoe/of wanneer betrokkene geïnformeerd zal worden.

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 1en 2 van dit artikel, alsmede het bezwaar als bedoeld onder 3 kunnen worden ingediend bij de verwerkingsverantwoordelijke. Deze neemt binnen één maand een besluit 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 toesturen over zijn rechten en de mogelijkheden deze uit te oefenen.
7. Het bovenvermelde kan buiten toepassing worden gelaten voor zover dit noodzakelijk is in het belang 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,;
   e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen of;
   f. de openbare veiligheid.

Artikel 15 Bijlagen
De bij dit protocol gevoegde bijlagen maken deel uit van dit protocol.

Artikel 16. 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 de verwerkingsverantwoordelijken vastgesteld worden.

Artikel 17. Datum inwerkingtreding
Dit protocol treedt in werking op de dag na bekendmaking ervan.

Artikel 18. Citeertitel
Dit protocol kan worden aangehaald als: "Privacyprotocol gegevensdeling bestuurlijke aanpak ondermijnende criminaliteit Geldrop-Mierlo 2023"

Geldrop, datum

BURGEMEESTER EN WETHOUDERS VAN GELDROP-MIERLO

De secretaris
N. Scheltens

De burgemeester
J.C.J. van Bree

BIJLAGE 1: bij artikel 6 privacyprotocol categorieën persoonsgegevens

Van de personen over wie wordt gemeld, kunnen onderstaande gegevens, afhankelijk van de inhoud van de melding/signaal in de verschillende fases worden verwerkt en geregistreerd in het bestand.

Fase 1 Ontvangst en intake van het signaal
In fase 1 van het privacyprotocol zijn dit de volgende gegevens:

1. De (anonieme) melding c.q. het ontvangen signaal en de daarin van betrokkene opgenomen persoonsgegevens zoals naam, adres.
2. Of er sprake is van ondermijning zoals bedoeld in bijlage 2:
   e. eventuele aanwijzingen voor ondermijning uit de eerste weging van het onderzoek,
   f. het eventuele vervolg dat aan het onderzoek wordt gegeven,
   g. het thema van ondermijning dat van toepassing is op het signaal (bijv. synthetische drugs cocaïne, hennep, mensenhandel, fraude of witwassen),
3. Gegevens over mogelijke betrokkenheid van de betrokkene als eigenaar, directeur, bestuurder van een bedrijf of andere rechtspersoon, afkomstig uit het Handelsregister.
4. Gegevens over mogelijke eigendomsrechten van de betrokkene uit het 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 het privacyprotocol 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 intrekkingsbesluiten, waarmee betrokkene in relatie kan worden gebracht.
4. Informatie uit systemen van uitkeringen, hulpmiddelen WMO, zorgbudget (PGB) van werk en inkomen (gesloten bron). Bijv. Is er wel/niet een uitkering verstrekt? en of er andere bronnen van inkomsten zijn en zo ja welke soort uitkering? (geen volledige SUWI-net gegevens en niet de hoogte van andere uitkeringen zoals bijv. WAO- of WW-uitkering). Ook kan - zo nodig - andere informatie over een uitkeringsaanvraag relevant zijn, dit bespreken en eventueel in samenwerking met sociale recherche laten verstrekken.
5. Informatie uit systemen van toezicht en handhaving over opgelegde dwangsommen, bestuursdwang of andere handhavingsaanschrijvingen.
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 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 (straatinformatie) bekend bij interne functionarissen
10. Informatie van de leerplichtambtenaar over het betreffende adres of de persoon/gezin (is wel wel/niet sprake van schoolverzuim?).

Fase 3 hit/no hit en bepalen vervolgaanpak
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 informatiecoördinator en levert gegevens die de informatiecoördinator 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 buitenkantinformatie 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 informatiecoördinator, 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 informatiecoördinator waarin interne informatie met elkaar gedeeld wordt.
b. Een 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 van casus tot integrale Taskforce-RIEC casus.

BIJLAGE 2 bij artikel 6 Categorieën personen als onderdeel van de checklist beoordelen signalen ondermijning

Inhoud checklist
Deze checklist bestaat uit twee onderdelen.
1. Een overzicht van criminele (en niet-criminele) activiteiten en de rol van personen die daarin (al dan niet bewust) betrokken kunnen zijn;
2. Kenmerken van ondermijnende criminaliteit.

Aan de hand van deze checklist beoordeelt de informatiecoördinator of een signaal betrekking kan hebben op ondermijning. De beoordeling bestaat uit twee stappen.
1. Welke rol vervult een persoon die in een signaal wordt genoemd en kan die persoon in diens rol in relatie worden gebracht tot de vermeende criminele activiteit;
2. Voldoet het signaal ook aan de kenmerken van ondermijnende criminaliteit

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

Categorieën van personen:
De informatiecoördinator 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.

Algemeen ondermijnende activiteiten
En/of personen die een rol spelen bij een regionaal thema of een handhavingsknelpunt zoals:
- Autobedrijven;
- Outlaw Motorcycle Gangs (OMG's): leden van OMG's;
- Woonwagencentra: eigenaren woonwagens, huurders, bewoners;
- Aanpak in het buitengebied;
- Personen met ongebruikelijk bezit;
- Harddrugs.
- Overige faciliteerders die ondermijnende of criminele activiteiten mogelijk maken en/of (on)bewust in stand houden;

Mensenhandel, -smokkel en uitbuiting (o.a. illegale prostitutie)
- Huis/pandeigenaar
- Verhuurder
- Huurder
- Eigenaar (illegale) seksinrichting
- Eigenaar (illegale) massagesalon
- Illegaal werkende prostituee (d.w.z. zonder vergunning)
- Bewaking
- Kassier
- Financier

Georganiseerde hennepteelt/drugs(-handel)
- Huis/pandeigenaar
- Verhuurder
- Huurder
- Tussenpersoon (verhuurmakelaar, evt. andere vormen)
- Transporteur
- Electromonteur
- Financier

Fraude in de vastgoedsector
- Huis/pandeigenaar
- Verhuurder
- Huurder
- Tussenpersoon (verhuurmakelaar, andere vormen)
- Stichting, vereniging of andere ondernemingsvorm (of bestuurders hiervan)
- Notaris
- Financier

Misbruik in de vastgoedsector

- Huis/pandeigenaar
- Verhuurder
- Huurder
- Tussenpersoon (verhuurmakelaar, andere vormen)
- 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)
- Ontvanger/begunstigde uitkering vanuit de gemeente
- Ontvanger/begunstigde subsidie vanuit de gemeente
- Andersoortige begunstigende beschikking of vergunningen vanuit de gemeente
- Een tussenpersoon/gemachtigde met betrekking tot zorg
- Pandeigenaar
- Huurder
- Verhuurder
- Financier

Openbare inrichtingen
- Pandeigenaar
- Verhuurder
- Huurder/pachter
- Exploitant
- Beheerder/leidinggevende
- Tussenpersoon
- Geldschieters

Kenmerken van ondermijnende criminaliteit
Voor de bepaling of sprake kan zijn van ondermijnende criminaliteit bekijkt de informatiecoördinator 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. ontwrichting 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 onderstaande locatie-, persoons- en/of bedrijfsgebonden indicatoren binnen het grondgebied van de gemeente Geldrop-Mierlo;
- 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.

TOELICHTING PRIVACYPROTOL GEGEVENSDELING BESTUURLIJKE AANPAK ONDERMIJNENDE CRIMINALITEIT GELDROP-MIERLO 2023

1. Overwegingen
De gemeente, politie en andere ketenpartners werken samen bij de integrale aanpak van complexe veiligheidsvraagstukken, waaronder (georganiseerde) criminaliteitsbestrijding. Om criminaliteit zo effectief mogelijk te kunnen bestrijden is het nodig en noodzakelijk dat gemeenten, politie en andere partijen zoals het OM en de Belastingdienst informatie met elkaar delen en de onderlinge uitwisseling goed geregeld hebben.

In het kader van de uitvoering van haar taken beschikt de gemeente over veel informatie, dat van belang kan zijn voor de criminaliteitsbestrijding. Een deel van die informatie kan en mag de gemeente gebruiken voor de veiligheidsvraagstukken.

Maar er zijn ook veel databronnen aanwezig die verbonden zijn aan specifieke doeleinden/taakvelden en die, onder andere vanwege privacywetgeving, niet zonder meer gedeeld mogen worden ten gunste van doeleinden op andere taakvelden, waaronder criminaliteitsbestrijding.

Het dilemma is duidelijk: Aan de ene kant heeft de gemeente Geldrop-Mierlo (ook volgens de Raad van State[1]) de taak en ook diverse wettelijke mogelijkheden (denk onder meer aan de wet Bibob) om mee te werken aan de bestrijding en voorkoming van (ondermijnende) criminaliteit en wil ze voorkomen (ongewild) bij te dragen aan de ondermijnende effecten daarvan. Aan de andere kant wil het gemeentebestuur van Geldrop-Mierlo dat haar burgers er ook op kunnen vertrouwen dat zij hun privacy beschermt en de regels naleeft die daarvoor in de wet zijn opgenomen.
Om uit dit dilemma te komen is belangenafweging en besluitvorming van bestuurlijk en ambtelijk verantwoordelijken nodig. Dit protocol heeft als doel bestuur en management een kader te bieden voor de afweging van deze soms tegenstrijdige belangen en daarover besluiten te nemen.

2. Doel en uitgangspunten van dit protocol

Doel
De gemeente Geldrop-Mierlo heeft een medewerker aangewezen die de informatiepositie van ondermijnende criminaliteit coördineert en die de organisatie ondersteunt bij het voorkomen en bestrijden van ondermijning. Informatieverwerking over personen en organisaties is voor de doeltreffendheid van het werk van de informatiecoördinator van cruciaal belang.
Deze informatiecoördinator ontvangt signalen over vermoedens van ondermijnende activiteiten uit zijn professionele netwerk, vanuit burgers, maatschappelijke organisaties, bedrijven, politie en andere overheidsorganisaties.

Daarnaast kan de informatiecoördinator signalen genereren door databestanden zoals bijvoorbeeld BRP en BAG te vergelijken en de resultaten hiervan te analyseren. Als daar aanleiding voor is, is het noodzakelijk deze informatie en resultaten te delen met organisatieonderdelen die mogelijk (onbewust) betrokken zijn (geraakt) bij ondermijning of dit door hun handelen (onbewust) faciliteren.

Zowel het generen en verwerken van signalen als de uitwisseling van informatie, waaronder persoonsgegevens tussen de informatiecoördinator en de andere organisatieonderdelen in het kader van de aanpak van ondermijning dient met inachtneming van wet- en regelgeving op het gebied van privacy plaats te vinden.

De privacybescherming bij het genereren van signalen door bestandsvergelijking en data-analyse zal de gemeente waarborgen door op het gebruik van de bronnen en de toe te passen algoritmes een data protection impact assessment (DPIA) te laten uitvoeren en de privacy- en beveiligingsrisico's die dit oplevert met toepasselijke maatregelen te mitigeren[2]. De informatiecoördinator maakt telkens een zorgvuldige belangenafweging waarbij de technische mogelijkheden worden afgewogen tegen de noodzaak om bepaalde informatie te verzamelen. De informatieverzameling moet een doel hebben in het voorkomen, verstoren of tegengaan van ondermijning.

De uitwisseling van data en dan met name van persoonsgegevens tussen de informatiecoördinator en de uitvoeringsorganisatie/ afdelingen binnen de gemeentelijke organisatie (Geldrop-Mierlo en Dienst Dommelvallei) stuit in een aantal gevallen op de grenzen van de wettelijke mogelijkheden. In het bijzonder betreft dit de wetgeving op het gebied van het sociaal domein (Participatiewet, WMO, Jeugdwet). Dat blijkt ook uit de "Handleiding binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondermijning" die Minister van Veiligheid en Justitie in februari 2020 heeft gepubliceerd.
Hierbij wordt ook de 'wet aanpak meervoudige problematiek sociaal domein' (Wams) betrokken op het moment dat deze in werking treedt. Deze wet voorziet in wettelijke taken voor onderzoek, planvorming en coördinatie bij meervoudige problematiek in het sociaal domein. Deze wettelijke taken vormen de grondslag voor de uitvoering van voor die wettelijke taken noodzakelijke verwerking en uitwisseling van persoonsgegevens.

1) Uit Advies Raad van State van 20 maart 2019: "Het mag duidelijk zijn dat ook de bestuurlijke aanpak van ondermijning tot de taak van de gemeente behoort. ..... 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".
2) Let op: Daarmee ontstaat geen generaal pardon op de toepassing van dit instrumentarium. De gemeente zal in haar privacybeleid moeten opnemen dat bij bestandsvergelijkingen met nieuwe bronnen en/ of nieuwe analysemethodes er steeds opnieuw een DPIA uitgevoerd moet worden. Ook van belang om van tijd tot tijd aan de hand van criteria van proportionaliteit en subsidiariteit het gebruik van de vergelijkingen en analyse te evalueren.

Ondanks dat de ruimte voor gegevensuitwisseling vanuit sommige taakvelden zeer beperkt is of ontbreekt, is de noodzaak tot gegevensuitwisseling soms zeer urgent. De gemeente Geldrop-Mierlo heeft in dat soort gevallen toch de behoefte om over te gaan tot het delen van informatie, maar wil door middel van dit privacyprotocol de benodigde waarborgen inbouwen die eventuele risico's voor de privacybescherming tot een minimum beperken.

De uitgangspunten van dit privacyprotocol zijn:

- De organisatie is primair verantwoordelijk voor het *voorkomen* van ondermijnende criminaliteit Dat houdt in dat zij ervoor zorgt dat alle informatie vergaard wordt die nodig is om tot een rechtmatig besluit te komen over elke dienst of product die een burger of organisatie van haar vraagt. Een team maakt daarvoor gebruik van signalen die de informatiecoördinator spontaan of op verzoek aanlevert en verwerkt die signalen binnen de mogelijkheden van het wettelijk kader dat op de uitvoering van de werkzaamheden van een team van toepassing is. Wat voor soort informatie gedeeld wordt, bekijkt en beoordeelt de informatiecoördinator per casus.
- We voldoen aan de Algemene verordening gegevensbescherming (AVG) en overige privacyvoorschriften bij de uitwisseling van persoonsgegevens. Waar dit niet of niet volledig kan, besteden we bijzondere aandacht aan:
  - Toetsing aan het noodzakelijkheidscriterium: is er een noodzaak om gegevens uit te wisselen en weegt het belang van bescherming van de persoonlijke levenssfeer in concrete situaties op tegen het belang van de voorkoming en bestrijding van ondermijnende criminaliteit?
  - Toetsing aan eisen van proportionaliteit en subsidiariteit. We voorkomen bovenmatig gebruik van gegevens, door middel van fasering en per fase een afweging te maken van de noodzaak tot informatiede¬ling (zie hierna 2 Procesbeschrijving). Ook beoordelen we of we hetzelfde resultaat kunnen verkrijgen met een minder belastende manier voor de betrokkene.
  - Toetsing aan de eisen van transparantie: het zichtbaar en inzichtelijk maken met welk doel en op welke wijze (persoons)gegevens worden verwerkt door de gemeente Geldrop-Mierlo.

- Het delen van signalen met de informatiecoördinator gebeurt alleen in het kader van de bestrijding van ondermijnende criminaliteit en als onderdeel van gecoördineerde interventies c.q. aanpak, zo nodig in samenwerking met externe partners van de Taskforce-TASKFORCE-RIEC. Vanzelfsprekend zal een verstrekker van een signaal wel steeds moeten vaststellen of die verstrekking in lijn is met de privacyregelgeving en indien daar twijfel over bestaat daarin de afstemming te zoeken met de privacy-adviseur van de gemeente Geldrop-Mierlo.

Op deze wijze worden alleen de strikt noodzakelijke gegevens ten behoeve van data-analyse, signaalverwerking en -verrijking en concrete acties c.q. interventies gedeeld en benut en op een manier die het minst belastend is voor betrokkenen.

3. Privacy dilemma's

Ondermijnende criminaliteit nestelt zich in de haarvaten van onze samenleving. Om daar effectief tegen op te treden is een goede informatiepositie van de overheid cruciaal. Gemeenten hebben in de aanpak van georganiseerde criminaliteit een belangrijke rol en lopen aan tegen het feit dat veel informatie die zij zelf bezitten, niet gedeeld en gebruikt mag worden binnen de eigen gemeente (tussen interne afdelingen). De reden daarvan is dat achter verschillende taken veelal specifieke sectorale wetgeving ligt met een geheimhoudingsplicht.

Het delen van informatie is nodig om te beoordelen of een actie nodig is, zo ja welke actie en welk team of welke (keten)partner die actie het beste kan uitvoeren. De keuze om een interventie te plegen kan pas worden gemaakt na het leggen van een complete informatiepuzzel. Om een vuist te kunnen maken tegen ondermijnende criminaliteit is een goede informatiepositie daarom essentieel.

Informatiedeling, het verrijken van ingekomen signalen en anonieme meldingen en informatie uit verschillende interne afdelingen is nodig voor een ontkokerde, effectieve en integrale aanpak van ondermijnende criminaliteit en daadkrachtige fraudebestrijding.

Als de gemeente de informatie waarover zij beschikt niet of niet goed kan benutten binnen de aanpak van ondermijning, werkt dit ook door naar het niet goed kunnen deelnemen in het Taskforce-RIEC samenwerkingsverband. Sterker nog: het staat haaks op de gedachte achter het Taskforce-RIEC convenant waarbij partners samen komen tot de integrale aanpak van ondermijningscasussen. Dit gebeurt onder andere door het delen van gegevens.

Als de interne informatie-uitwisseling niet optimaal is, dan kan de gemeente vanuit haar ondermijningsaanpak geen goede inschatting maken of er actie nodig is, of dat de casus naar de Taskforce-RIEC moeten worden gebracht zodat informatiedeling met externe partners kan plaatsvinden of dat zij zelfstandig direct kan ingrijpen c.q. handhaven op grond van de beschikbare en bestaande bestuursrechtelijke instrumenten.

Alhoewel de nood hoog is en er hoge maatschappelijke en politieke verwachtingen zijn ten aanzien van het ingrijpen door het gemeentebestuur, heeft de wetgever het gemeentebestuur niet voorzien van een wettelijke grondslag voor dit ingrijpen. Als geen grondslag kan worden aangewezen, is er vanuit privacy oogpunt geen basis voor het verwerken van persoonsgegevens door de gemeente voor onderzoek naar activiteiten van ondermijning en georganiseerde criminaliteit. De aanpak van ondermijning houdt namelijk in het verwerken van persoonsgegevens voor een ander doel dan waarvoor deze gegevens oorspronkelijk zijn verzameld. Informatie wordt verzameld vanuit verschillende taken en bevoegdheden, om het vervolgens voor een nieuw doel te gebruiken. Dat nieuwe doel, vaststellen van ondermijning, is nog niet wettelijk vastgelegd. Dit is in de praktijk het grootste knelpunt. Dit protocol heeft als doel handvatten te bieden hoe om te gaan met dit knelpunt.

4. Noodzaak reglement: De gemeente kan niet wachten op wetgeving
Het is duidelijk dat door het geschetste dilemma informatie-uitwisseling uiterst moeizaam of zelfs helemaal niet tot stand komt. Om misverstanden te voorkomen, wordt opgemerkt dat dit niet aan medewerkers kan worden toegerekend. Zij volgen immers de op hen van toepassing zijnde (privacy)-voorschriften.

Het gaat hier ook niet om een bevoegdheidsverdelingsvraagstuk. Dit is ook nooit een vraagstuk geweest want bij een integrale gemeentelijke aanpak hoort dat iedere afdeling/team gebruik maakt van haar eigen bevoegdheden en haar eigen instrumentarium.

Vanuit het taakveld ondermijning is het zeker niet de bedoeling om hier afbreuk aan te doen. Het gaat er uitsluitend om informatie die al binnen de gemeente aanwezig is, met elkaar te delen voor een goede uitvoering van onze bestuursrechtelijke bevoegdheden en -instrumenten.

Er is wetgeving voor gegevensdeling voor samenwerkingsverbanden (Wet gegevensverwerking samenwerkingsverbanden). De vraag is of deze wet het dilemma opgelost heeft en toepasbaar is binnen een gemeente. Daarnaast ligt er het al eerdergenoemde advies van de Raad van State, die stelt dat er al veel mogelijk is als het gaat om het delen van gegevens in het kader van de aanpak van georganiseerde misdaad. De uitwerking van die mogelijkheden laat vervolgens op zich wachten. De gemeente kan echter door het ontwikkelen van een werkproces met bijbehorende formats beter afwegen waarom gegevensuitwisseling in sommige gevallen toch noodzakelijk is.

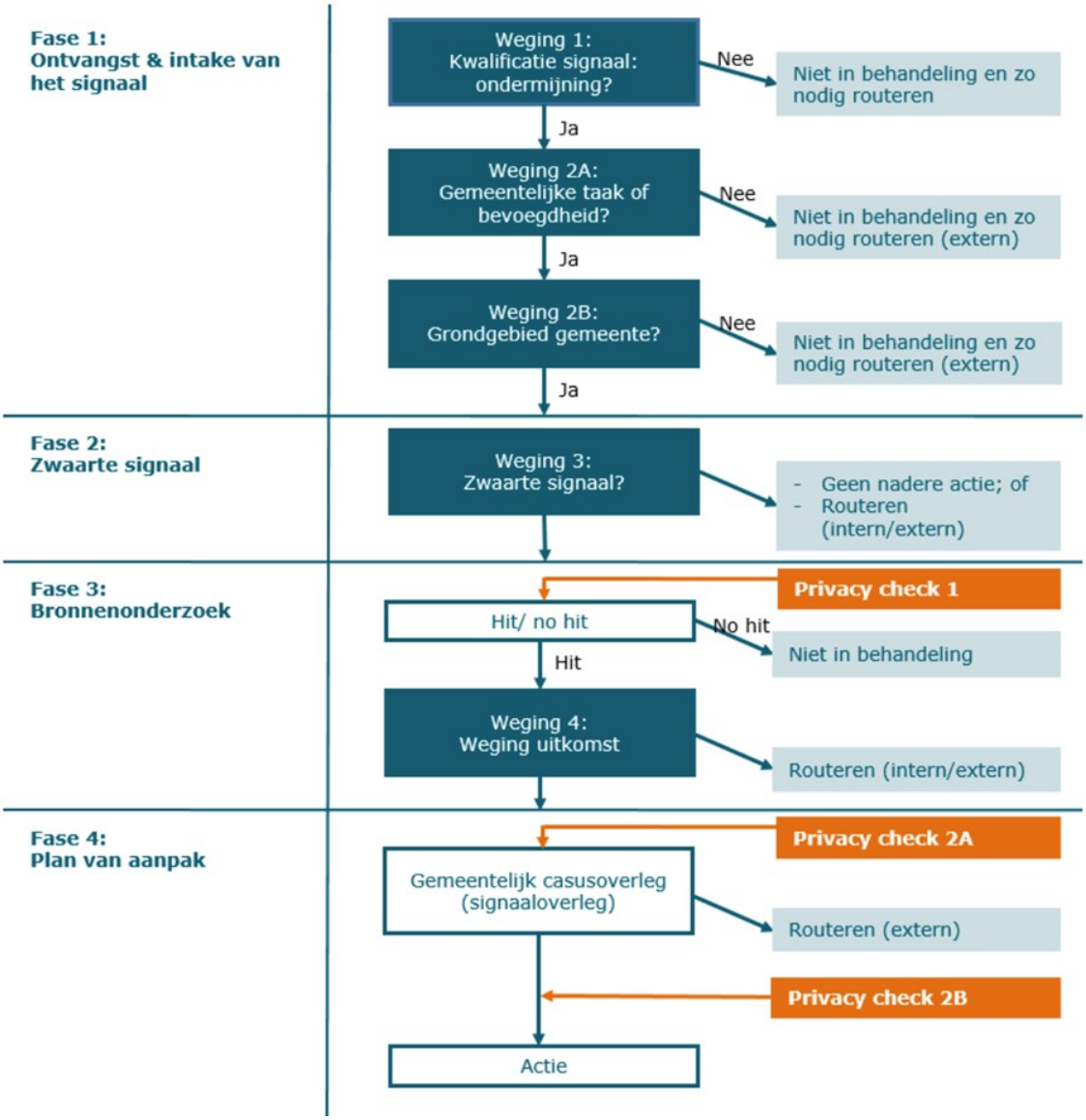
De georganiseerde criminaliteit wacht daar niet op en de gemeente kan het zich niet permitteren om in de tussentijd stil te zitten. Daarom is het noodzakelijk om vooruitlopend op (toekomstige) regels, voor de gemeente Geldrop-Mierlo een protocol op te stellen voor het delen van informatie in die situaties dat de wetgever er niet in heeft voorzien. Dat biedt bestuur en management een afwegingskader en verschaft medewerkers duidelijkheid over wat zij in welke gevallen kunnen delen met het taakveld ondermijning.

5. Inhoud protocol
Een procesbeschrijving, waarin de fasen worden beschreven die signalen doorlopen die de informatiecoördinator ontvangt of zelf heeft ontwikkeld door bestandsvergelijking en informatie-analyses, maakt onderdeel uit van dit protocol. In elke fase wordt een afweging gemaakt over het doorgaan naar de vervolgfase of beëindiging van de signaalverwerking, om onnodige uitwisseling en verwerking van persoonsgegevens te voorkomen.

De condities waaronder persoonsgegevens kunnen worden verwerkt, de registratie en uitwisseling van gegevens en de rechten van de betrokken personen, zijn vastgelegd in het privacyprotocol.

Evaluatie
Het protocol zal tweejaarlijks worden geëvalueerd. Het protocol kan bijvoorbeeld worden aangepast als werkprocessen of wet- en regelgeving wijzigen of als er sprake is van nieuwe verschijningsvormen van ondermijning.

6. Procesbeschrijving
Procesfases van belang voor dit protocol
In deze procesbeschrijving draait het om het verwerken van signalen en het aanpakken van signalen van ondermijnende activiteiten. Het proces verloopt met het oog op proportionaliteit en subsidiariteit in vier fases. De informatiecoördinator waarborgt dat de verschillende fases ook op juiste wijze worden gevolgd. Hiervoor wordt nog een werkproces en format ontwikkeld dat handvatten geeft om hier in de praktijk vorm aan te geven.
Hieronder worden de verschillende fasen toegelicht. Daarbij geldt dat de beoordeling van een binnengekomen signaal het startpunt van het protocol vormt. Het verwerken en registreren van de signalen is op zichzelf al een verwerking van persoonsgegevens die opgenomen dient te worden in het register van verwerkingen van de gemeente Geldrop-Mierlo.



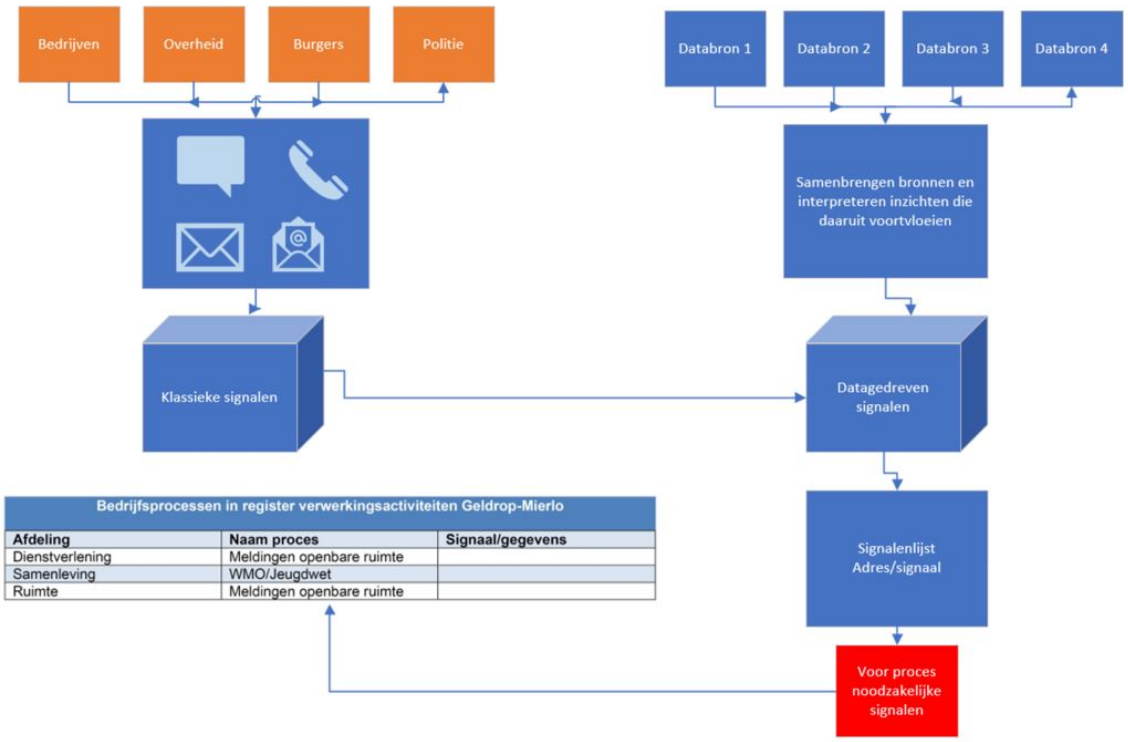
Figuur 1: Procesfasen, ontleend aan Model privacy protocol ministerie van justitie en veiligheid

Het doel van deze gefaseerde aanpak is om per fase een afweging te kunnen maken of er een noodzaak is om persoonsgegevens te verwerken, welke gegevens dat zijn en of dat leidt tot vervolgfasen (triages).

Signalen van binnen en buiten de organisatie of als resultaat data-analyse.
Een signaal is binnen het kader van dit protocol een aanwijzing of meerdere aanwijzingen dat bepaalde gedragingen en/of situaties mogelijk verband zouden kunnen houden met verschijningsvormen van georganiseerde criminaliteit dan wel dat zich een handhavingsknelpunt (bijvoorbeeld op een bedrijventerrein) voordoet dan wel dat bepaalde gedragingen en of situaties mogelijk relevant zijn voor de toepassing van de Wet Bibob. Bijlage 2 van het privacyprotocol bestuurlijke aanpak ondermijning bevat een nadere concretisering van wat een signaal kan inhouden.

Signalen kunnen afkomstig zijn van burgers en professionals of voortvloeien uit resultaten van data-analyse. Zie ook figuur 2.

Figuur 2: Klassieke en datagedreven signaalverwerking



Fase 1 Ontvangst, intake en registratie signaal
Fase 1 heeft betrekking op het beoordelen van signalen van criminele activiteiten, onrechtmatigheden en maatschappelijke dreigingen. Een signaal kan op verschillende manieren binnenkomen zoals per mail, MOR- of MMA-melding. Ook kan naar signalen worden gezocht door middel van data-analyse.

Voor de beoordeling van een signaal is van belang te weten wat het signaal inhoudt en of het betrekking heeft op ondermijning. Dat betreft de **eerste weging**. Een signaal wordt bij de intake beoordeeld op grond van een aantal kenmerken en indicatoren, die zijn weergegeven in bijlage 2 van het privacyprotocol bestuurlijke aanpak ondermijning. Er dient tenminste sprake te zijn van één van de indicatoren en/of categorieën van personen.

De informatiecoördinator registreert elk signaal in een overzicht. Dit overzicht bevat de inhoud van het signaal, de naam van de persoon op wie het signaal betrekking heeft en het resultaat van een eerste onderzoek van de informatiecoördinator.

Voordat het signaal verder in behandeling/onderzoek wordt genomen, beoordeelt de informatiecoördinator of het signaal betrekking heeft
a. op een taak of bevoegdheid van de gemeente en niet op een taak of bevoegdheid van een andere instantie (**Weging 2A**)
b. op het grondgebied van de gemeente (**Weging 2B**). De volgende vragen moeten daarbij achtereenvolgend worden beantwoord:
    a. Gaat het om een object of een subject?
    b. In het geval van een object: is het object binnen de gemeentegrenzen gelegen (dan wel is er anderszins een link met de gemeente)?
    c. In het geval van een subject: is het subject woonachtig binnen de gemeentegrenzen (dan wel is er anderszins een link met de gemeente)?

Deze vragen beantwoordt de informatiecoördinator door een of meerdere signalen te vergelijken met informatie uit openbare bronnen zoals het Handelsregister (bij de Kamer van Koophandel), het eigendommenregister (bij het Kadaster), publicaties (al dan niet op internet) en bekende informatie binnen het vakgebied Ondermijning.

Na dit eerste onderzoek volgt een eerste beslismoment:
- het signaal leidt niet tot verder onderzoek en blijft bewaard gedurende één jaar na het beslismoment en wordt daarna binnen 1 maand vernietigd, of
- het onderzoek geeft aanleiding om het signaal verder in behandeling/onderzoek te nemen.

Verder in behandeling nemen kan inhouden dat de informatiecoördinator het signaal:
a) naar de politie stuurt met behulp van een proces-verbaal van bevindingen dat door een buitengewoon opsporingsambtenaar wordt gemaakt omdat het signaal betrekking heeft op opsporingstaken van de politie bijvoorbeeld het vermoeden van een hennepkwekerij, aanwijzingen van dealen, heling of prostitutie.
b) naar de bevoegde toezichthouders van een andere gemeentelijk afdeling of team stuurt, die vervolgens het signaal vertaalt naar concrete acties of verder onderzoek uitvoert binnen het kader van de eigen wettelijke taken en bevoegdheden. Bijvoorbeeld bij vermoeden van uitkeringsfraude gaat er een signaal naar Senzer en fraudesignalen op het gebied van WMO en Jeugd worden doorgezet naar de afdeling Samenleving.
c) voor vervolgbehandeling doorzet naar fase 2.

De behandelaars onder a. en b. koppelen het resultaat van hun handelen terug naar de informatiecoördinator. De informatiecoördinator noteert dat resultaat in het signalenregister. Dat resultaat kan luiden:
– proces beëindigd;
– proces wordt voortgezet door (de toezichthouders van) de afdelingen en eventueel in samenwerking met welke partij.

Als het proces wordt voortgezet, koppelt de behandelaar het eindresultaat terug aan het eind van het proces. Voortzetting van het proces kan ook tot gevolg hebben dat de behandelaar de informatiecoördinator adviseert tot opschaling. Het signaal wordt bewaard tot één jaar na het moment waarop het eindresultaat is geregistreerd en daarna binnen één maand verwijderd.

Aan het einde van fase 1 is vastgesteld of het signaal:
- Betrekking heeft op ondermijning;
- Mogelijk aanleiding kan vormen voor inzet van een gemeentelijke taak of bevoegdheid (het zal hierbij veelal gaan om wettelijke taken en bevoegdheden die zien op openbare orde en bevordering van de leefbaarheid); én
- Betrekking heeft op een subject of object dat binnen de gemeente woont of is gevestigd.

Alleen als dat zo is, komt fase 2 in beeld.

Fase 2: Weging zwaarte signalen (derde weging)
Fase 2 start met een eerste nadere verkenning. De informatiecoördinator vraagt de relevante gemeentelijke afdelingen/teams na te gaan of er in relatie tot het signaal relevante informatie over een (rechts)persoon bekend is. Dit gaat in deze fase nog niet om zogeheten 'wat' informatie. Het gaat om óf er informatie beschikbaar is, niet welke informatie. Afdelingen/teams raadplegen hiervoor de bronnen waarover zij de beschikking hebben zoals BAG, BRP, informatie van vergunningverlening en toezicht- en handhaving. Daardoor ontstaat meer zicht op de inhoud en omvang van het signaal op basis waarvan de informatiecoördinator kan beoordelen of een vervolg (fase 3) nodig is.

Fase 3: Hit No Hit en beslissen vervolgaanpak
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 informatiecoördinator en levert gegevens die de informatiecoördinator 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'. Voor afdelingen die werkzaam zijn in het sociaal domein houdt dit in dat zij slechts de zogenaamde buitenkantinformatie 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 informatiecoördinator, 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.

Als er geen hit is na raadpleging van de gemeentelijke bronnen dan volgt verder geen actie, tenzij het oorspronkelijke signaal zo sterk is dat volgens de informatiecoördinator nader onderzoek nodig is. Volgt er definitief géén actie, dan wordt informatie die naar aanleiding van het signaal ontvangen is tijdelijk bewaard in de niet-actieve omgeving van het signalenregister. De verzamelde informatie leidt niet tot verder onderzoek en blijft bewaard gedurende één jaar na het beslismoment en wordt daarna binnen één maand vernietigd.

Bij een hit beslist de informatiecoördinator op basis van de beoordeling van de verzamelde informatie wat er verder met die informatie gaat gebeuren.

Fase 4 Vervolgaanpak
De volgende acties zijn mogelijk.

a. *Lokaal informatieoverleg*
Om een beter beeld te krijgen van alle digitale informatie uit gemeentelijke bronnen en -systemen plant de informatiecoördinator zo nodig een lokaal informatie-overleg in met interne, bij de casus betrokken, collega's om de casus te bespreken. Het doel is verdere beeldvorming, verrijking van het signaal en het beoordelen van concrete interventiemogelijkheden. Elke afdeling treedt, zo nodig, op conform eigen bevoegdheden en instrumentarium. De informatiecoördinator zorgt voor de overall-regie en planning. De informatiecoördinator zorgt voor verslaglegging en dat de gemaakte afspraken tijdens het overleg vastgelegd worden.

b. *Controle door de BOA/Toezichthouder*
De informatiecoördinator stuurt het signaal of de casus door naar de buitengewone opsporingsambtenaar en/of toezichthouder. Deze voert, zo nodig ondersteund door de lokale politie en andere partners, een flexcontrole[3] uit om overtredingen te constateren en vast te leggen zodat hier handhavend tegen kan worden opgetreden door de gemeente. De toezichthouder of BOA stemt de controleresultaten af met de handhavingsjurist en/of de afdeling vergunningverlening en koppelt terug naar de informatiecoördinator. De informatiecoördinator verwerkt het resultaat in het signalenregister.

c. *Delen met Taskforce-RIEC-partner(s), verrijking informatie door Taskforce-RIEC en Taskforce-RIEC aanpak*
Indien de informatiecoördinator vermoedt dat hij een ondermijningssignaal onderhanden heeft welke zich leent voor een bestuurlijk geïntegreerde aanpak onder het Taskforce-RIEC convenant, kan de informatiecoördinator de intell specialist van de Taskforce-RIEC consulteren. De intell specialist Taskforce-RIEC verzorgt de intake van het signaal. De intell specialist kan ook adviseren om het signaal op een andere wijze te routeren.

Indien de informatiecoördinator besluit het signaal te routeren voor een Taskforce-RIEC aanpak wordt het signaal via een signaaldocument aangeleverd bij de intell specialist. De agendeert het signaaldocument voor het ambtelijk voorbereidingsoverleg (AVO). Het signaaldocument wordt hiertoe geüpload in een fileshare map binnen het Taskforce-RIEC informatiesysteem (Taskforce-RIECIS). Dit betreft een beveiligde, afgeschermde digitale omgeving waartoe alleen de deelnemers aan het AVO-overleg toegang hebben.

In de informatiefase wordt het signaal, onder regie van de intell specialist van de Taskforce-RIEC, verrijkt met informatie van de samenwerkende partners. Dit is het moment waarop alle relevante gemeentelijke informatie wordt gedeeld binnen het Taskforce-RIEC samenwerkingsverband. Ook de andere partners delen alleen de informatie die voor een andere partner nodig is om tot de benodigde analyse en interventies te komen. Het Taskforce-RIEC -bureau voert de analyse uit. De informatie van de partners wordt gescheiden bewaard.

Op basis van het informatiebeeld wordt door de casusgroep een interventieadvies opgesteld. Dit interventieadvies bevat de aanleiding, een beknopt informatiebeeld, het beoogde doel en de voorgestelde interventies. Indien relevant worden meerdere scenario's beschreven.

De in fase 4 gebruikte begrippen

Gelegenheidsstructuren: een gelegenheid en/of een opeenstapeling van gelegenheden welke zich voordoen in de bestuurlijke, maatschappelijke en zakelijke omgeving die faciliterend werken voor het plegen van bestuursrechtelijk of strafrechtelijk of civielrechtelijk te sanctioneren gedragingen en waarin personen samenwerken die deze gedragingen faciliteren.

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

Integriteitsbeoordelingen: een onderzoek naar persoonlijke en karaktereigenschappen, van een individu met als doel te beoordelen dat de betrokkene eerlijk en oprecht is en niet omkoopbaar.

Privacy protocol Taskforce-RIEC: het Privacy protocol behorende tot en deel uitmakende van het Taskforce-RIEC convenant.

Lokaal informatieoverleg: overleg na de eerste weging van signaal van de desbetreffende gemeentelijke onderdelen die een hit op een signaal hebben.

3) Flexcontrole is een controle op een adres, waarbij afhankelijk van het signaal of de casus verschillende (in- en externe) partners deelnemen. De samenstelling is afhankelijk van de casuïstiek.

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

Plan van aanpak/ Interventies: door een gemeentelijk onderdeel of in gezamenlijkheid van gemeentelijke onderdelen schrijven van een plan ten behoeve van uitvoering van de zijnde wettelijke instrumenten om ondermijning te doen stoppen.