VAN AETSVELD
verandermanagement, projectmanagement

Rapport

Een verwerkingsproces

voor de aanpak van ondermijning

in opdracht van
Gemeente Rheden
Petra van den Berg

datum
20 december 2018
referentie
18-391-002-v1.2
status
Definitief

gemeente Rheden

Documentbeheer

Versiebeheer

versie	status	wijzigingen	auteur	datum
0.8	Concept	Opzet in basis Word bestand	Mark Albers	Vanaf juni 2018
0.9	Concept	In template, Gegevensbeschermingseffect-beoordeling en hoofdstructuur opgezet	Mark Albers	22 oktober 2018
0.99	Concept	Verwerking reviewcommentaar	Mark Albers	19 november 2018
1.0	Definitief	Verwerken van opmerkingen FG n.a.v. review Taalcontrole	Mark Albers	29 november 2018
1.1	Definitief	Verwerking opmerkingen FG en opdrachtgever; aanpassing titel en aanvullen schema verwerkingsgrondslagen	Mark Albers	17 december 2018
1.2	Definitief	Taalcorrecties, specifiekere duiding grondslagen, term PIA vervangen voor Gegevensbeschermingseffectbeoordeling en verschuiving burgemeestersbevoegdheden van paragraaf 6.2 naar hoofdstuk 14	Mark Albers	20 december 2018

Reviews

naam	organisatie	functie
Aaf Groenewoud Cora Westhoff Ellen Pouw Elles van Orden Esther Barink-Nijenhuis Ingrid Pellegrom Jenine Hingstman Jeroen Wieland Julie Roselle Margriet Loeven Marit de Ridder Mirjam Nabbe Natascha v.d. Wijngaard Moiko Zeldenthuis	Gemeente Rheden	Ondermijiningsteam
Margriet van Kempen	Politie	Operationeel Expert Ondermijning

naam	organisatie	functie
Roel Daams	RIEC Oost Nederland	Accountmanager
Joey van Haassen Viresh Jagesser	Anti-Fraud Company	Accountmanager
Dominique van Woensel Laura de Vries	Cuccibu Gemeente Rheden	Privacy functionaris Functionaris Gegevensverwerking

Distributie

Naam	organisatie	Functie
0.9	Gemeente Rheden	Reviewers
0.9	Gemeente Rheden	Opdrachtgever
0.99	Gemeente Rheden	FG
1.0	Gemeente Rheden	Opdrachtgever
1.1	Gemeente Rheden	Opdrachtgever
1.2	Gemeente Rheden	Opdrachtgever

Inhoudsopgave

1 INLEIDING 7

1.1 Doel van dit document 7
1.2 Leeswijzer 7
1.3 Achtergrond 8
1.4 Beschikbare bijlagen 8

2 MANAGEMENTSAMENVATTING 9

3 CONTEXT 11

3.1 Werkproces in hoofdlijnen 12
3.2 Processtappen *Van Ondermijningssignaal naar actie* 13
3.2.1 Signalen ontvangen en verwerken 13
3.2.2 Analyse en plan van aanpak 14
3.2.3 Van plan van aanpak naar resultaat 16

4 RISICO'S EN MAATREGELEN – PRIVACY IMPACT ANALYSE 17

4.1 Signalen komen van eigen medewerkers 17
4.2 Signalen bevatten persoonsgegevens 17
4.3 Signalen anoniem verwerken 18
4.4 Toegang tot persoonsgegevens beperken 18
4.5 Niet ieder signaal leidt tot actie 19
4.6 Van signaal naar actie in een ander systeem 19
4.7 Logging zaaksysteem alleen op verwerkingsactiviteiten 19
4.8 Inzien van gegevens uit gemeentelijke systemen beperken 19
4.9 Gegevens van vermoeden uitwerken met het ondermijningsteam 20
4.10 Gegevens delen met partners 20
4.11 Gegevens beperkt overdragen 21
4.12 Medewerkers beschermen 21
4.13 Verwerking in zaaksysteem 22
4.14 Verwerking gegevens door ODRA 22
4.15 Reactie op review door FG 22

5 AANBEVOLEN MAATREGELEN 24

5.1 Aanwijzen functionarissen 24
5.2 Bewustwording ondermijning 24
5.3 Integriteitsdilemma's bespreekbaar maken 24
5.4 Uitbestede diensten betrekken 24
5.5 Politiek en bestuurlijk draagvlak 25
5.6 Auditcyclus opzetten 25

6 UITWERKING PROCESSTAP 1: MELDING VAN EEN VERMOEDEN VAN ONDERMIJNING 26

6.1 Hoe komen de signalen binnen? 26
6.1.1 Ingezette middelen - Mailadres ondermijning@rheden.nl 26
6.1.2 Ingezette middelen – App "Meld een vermoeden" 26
6.1.3 Ingezette middelen – Mondelinge of schriftelijke meldingen 27
6.2 Verwerkingsgrondslag 28
6.3 Verwerker 28
6.4 Wie kan er bij deze gegevens? 28

7 UITWERKING PROCESSTAP 2: ANALYSE VAN DE MELDING 30

7.1 Verwerkingsgrondslag 30

8 UITWERKING PROCESSTAP 3: KEUZEMOMENT - BESLUIT TOT NADER UITWERKEN 31

8.1 Wie neemt het besluit? 31
8.2 Verwerkingsgrondslag 31

9 UITWERKING PROCESSTAP 4: NADERE ANALYSE TEGEN INTERNE EN EXTERNE BRONNEN 32

9.1 Externe partners betrekken 34
9.2 Vastlegging 35
9.3 Verwerkingsgrondslag 36
9.4 Wie doet de analyse? 36
9.5 Autorisatie en opschoning 36

10 UITWERKING PROCESSTAP 5: ADVIES AANPAK OP SIGNAAL 37

10.1 Doel van het ondermijningsoverleg 37
10.2 Verwerkingsgrondslag 39

11 UITWERKING PROCESSTAP 6: BESLISSEN EN TOEWIJZEN 40

12 UITWERKING PROCESSTAP 7: ACTIE DOOR DE PARTIJ AAN WIE HET SIGNAAL IS TOEGEWEZEN 41

13 UITWERKING PROCESSTAP 8: EVALUATIE 42

14 BIJLAGE: GRONDSLAGEN 43

14.1 Thema's Integraal Veiligheidsplan 2017 – 2020 gemeente Rheden 45
14.2 RIEC thema's 48

1 Inleiding

1.1 Doel van dit document

De gemeente Rheden heeft in april 2018 aan Van Aetsveld gevraagd om ervoor te zorgen dat de procesgang van signaal tot actie compliant is aan de Algemene Verordening Gegevensverwerking. Dat wil zeggen dat op een correcte, zorgvuldige en transparante wijze met persoonsgegevens wordt omgegaan.

Daarbij ligt de focus op twee doelgroepen die signalen melden:

1. De medewerkers van de gemeente zelf; voor wie de gemeente vanuit haar bedrijfsvoering verantwoordelijk is;
2. Uitvoerende organisaties die in opdracht of onder regie van de gemeente taken uitvoeren.

De focus ligt daarbij op de verwerking van signalen die betrekking hebben op de wettelijke taken van de gemeente en die gemeld worden vanuit de aanpak van ondermijning. Het betreft een bestaande aanpak, waar in 2017 door de aanschaf van de app *Meld een Vermoeden* een nieuwe impuls aan is gegeven.

De opdracht was:
Werk de procesgang uit, zodat voldaan wordt aan de AVG en wettelijke verplichtingen, voor het analyseren van signalen op het gebied van Openbare Orde en Veiligheid of betreffende potentiele ondermijning die leiden tot:

1. Monodisciplinaire actie vanuit de eigen organisatie van de gemeente;
2. Multidisciplinaire actie vanuit de eigen organisatie van de gemeente;
3. Multidisciplinaire actie samen met externe partijen die taken uitvoeren voor de gemeente. Denk daarbij aan *De connectie* voor de inning van gemeentelijke belastingen en ODRA voor het uitvoeren van de omgevingswet en de partner uit de sociale gebiedsteams (die activiteiten uitvoert via detachering in dienst van gemeente).

1.2 Leeswijzer

Hoofdstuk 3 van dit document beschrijft de context en, in hoofdlijnen, *De aanpak van ondermijningssignaal tot actie*. Daarin is een drietal schema's opgenomen waarin de verschillende stappen zijn aangegeven.

Hoofdstuk 4 gaat in op de risico's en de voorgestelde maatregelen. Daarmee geeft het inzicht in de manier waarop wordt voldaan aan de uitgangspunten van de Algemene Verordening Gegevensverwerking. Als uitgangspunt is daarbij Privacy by design gehanteerd. In iedere stap wordt gewogen welke persoonsgegevens noodzakelijk zijn om te komen tot een adequate uitvoering. Uiteindelijk is het aan de verantwoordelijken binnen de gemeente Rheden om te bepalen welke risico's aanvaardbaar zijn, gezien de doelstelling: het aanpakken van ondermijning.

In de hoofdstukken 5 tot en met 12 staan de processtappen nader uitgewerkt.

Als bijlagen zijn stukken beschikbaar waarin de privacy impact analyse is opgenomen en aangegeven wordt hoe een dossier in het zaaksysteem eruit gaat zien.

1.3 Achtergrond

De gemeente Rheden pakt al jaren signalen van ondermijning van medewerkers en burgers op. Daarvoor wordt een mailadres gebruikt, waar de melder zijn of haar melding kan doen. Het werkproces om van melding naar actie te komen is jaren gebaseerd geweest op samenwerken binnen de gemeentelijke diensten.

Eind 2017, begin 2018 is besloten dat meldingen behalve via de mail ook via de app *Meld een vermoeden* gedaan kunnen worden. Die app werkt op mobiele telefoons, helpt bij het correct samenstellen van een melding en stuurt de gegevens vervolgens door naar een centraal punt. Het werken met een app vraagt onder meer om IT-activiteiten.

Daarbij werd duidelijk dat het proces van melden tot afhandelen tegen het licht van de Algemene Verordening Gegevensverwerking (AVG) gehouden moet worden. Deze AVG vervangt de Wet bescherming persoonsgegevens en wordt vanaf 25 mei 2018 gehandhaafd.

1.4 Beschikbare bijlagen

Naast de in dit document opgenomen bijlage is een aantal documenten opgesteld waaraan gerefereerd wordt in dit document of in de besluitvorming rond dit document:

Documentnaam	Inhoud
PIA proces van ondermijningssignaal naar actie v04	Gegevensbeschermingseffectbeoordeling (zoals bedoelt in Artikel 35 van de AVG)
Verwerkersovereenkomst app Meld een vermoeden	Verwerkersovereenkomst met Anti-Fraud
2018 10 31 Informatierapport van signaal naar actie	Opzet signaaldossier in zaaksysteem
2018-11-25_Rapportage advies DPIA ondermijningsapp.pdf	Reactie FG op procesdocument en Gegevensbeschermingseffectbeoordeling
2018 11 29 Reactie op FG-stuk DPIA	Respons gedeeld met FG op voorgaand stuk.

2 Managementsamenvatting

De gemeente Rheden vervult een groot aantal wettelijke taken. Een belangrijk deel daarvan betreft het inzetten van collectieve middelen. Vanuit haar rol dient zij toe te zien op de correcte inzet van die middelen. Misbruik van voorzieningen als subsidies of uitkeringen benadeelt immers het collectief.

In het geval van ondermijning is er sprake van het stelselmatig misbruik maken van voorzieningen, bijvoorbeeld om criminele gelden wit te wassen of om persoonlijk voordeel te genieten. De gemeente Rheden voert een actief beleid om ondermijning aan te pakken. Als één van de ondertekenaars van het Pact van Ellecom heeft de gemeente zich verbonden aan de aanpak van ondermijning.

Het proces start met als een ambtenaar van de gemeente een signaal invoert in de app *Meld een vermoeden*. Met het formaliseren van dit werkproces moeten alle ambtenaren van de gemeente signalen kunnen melden in de app. Zo'n signaal wordt door de adviseurs integrale veiligheid geanalyseerd. Als er aanleiding is om dit signaal verder uit te werken, wordt een signaaldossier aangemaakt in het zaaksysteem. Het signaal wordt als een pdf-document geëxporteerd en toegevoegd aan het signaaldossier. Daarmee start de verwerking binnen de gemeentelijke systemen.

Bij iedere stap die wordt gezet, beoordelen de adviseurs integrale veiligheid of er voldoende aanleiding is om vervolg in te zetten. Daarbij staat het uiteindelijke doel wat bereikt moet worden; rechtsherstel centraal.

In gevallen die passen binnen de thema's van de werkingssfeer van het RIEC, kan tevens een beroep gedaan worden op de partners binnen het RIEC. Nadat een gezamenlijke doelstelling is bepaald, wordt die toegewezen voor afhandeling. De partijen die nodig zijn om de doelstelling te realiseren ondernemen actie.

Bij het uitwerken van het proces is een aantal risico's naar voren gekomen. Die hebben vooral te maken met het gebruik van persoonsgegevens en de balans tussen het doel van het proces (voorkomen van misbruik van collectieve voorzieningen) en de daarbij ingezette bevoegdheden van de afdelingen en partners. De belangrijkste verschuiving ten opzichte van het bestaande werkproces is, dat besloten is om niet de

app, maar het zaaksysteem te gebruiken voor de dossiervorming. Daarmee verwerkt de gemeente Rheden de informatie in een bestaand gemeentelijk systeem.

De Functionaris gegevensverwerking van de gemeente heeft een review gedaan van dit document en de uitgevoerde Gegevensbeschermingseffectbeoordeling. Daaruit is een aantal aandachtspunten gekomen. De inhoudelijke opmerkingen zijn verwerkt.

Risico's die over blijven hebben te maken met:

- Het nog niet afgerond hebben van een Gegevensbeschermingseffect-beoordeling op het zaaksysteem; dat is een gemeente-breed gebruikt systeem. De FG geeft terecht aan dat daar aandacht aan besteed moet worden. Het proces aanpak ondermijning is slechts een van de gebruikers. Het verdient aanbeveling dit gemeente-breed op te pakken en tot afronding van dat traject eventuele risico's te accepteren;
- Het kabinet Rutte III heeft de aanpak van ondermijning tot een van haar speerpunten gemaakt. De komende jaren zal dat leiden tot een aantal aanpassingen van bestaande wetten en mogelijk het introduceren van nieuwe wetgeving. Dat betekent dat de grondslagen geactualiseerd moeten blijven. Dat kan meegenomen in de evaluatie die als laatste stap in het proces is opgenomen;
- Momenteel wordt de functie van privacy-aanspreekpunt ingericht. Controle en toezicht op het proces ligt bij deze functie (-kolom). Daarom is het van belang de privacy-organisatie snel ingericht te krijgen.

3 Context

De gemeente Rheden vervult een groot aantal wettelijke taken. Een belangrijk deel daarvan betreft het inzetten van collectieve middelen. Vanuit haar rol dient zij toe te zien op de correcte inzet van die middelen. Misbruik van voorzieningen als vergunningen, subsidies of uitkeringen benadeelt immers het collectief.

In het geval van ondermijning is er sprake van het stelselmatig misbruik maken van voorzieningen, bijvoorbeeld om criminele gelden wit te wassen of om persoonlijk voordeel te genieten. De gemeente Rheden voert een actief beleid om ondermijning aan te pakken. Als één van de ondertekenaars van het Pact van Ellecom heeft de gemeente zich verbonden aan de aanpak van ondermijning.

De nota 'Integrale veiligheid Rheden 2017-2020: Samen Rheden nog veiliger maken' benoemt ondermijning als een speerpunt. En het coalitieakkoord 2018-2022 'Rheden geeft Energie' geeft zelfs expliciet aan, dat de gemeente bij de aanpak van ondermijning moet samenwerken met het publiek en private partijen:

> *We zorgen dat signalen van vermoedens van ondermijning door inwoners, ondernemers en medewerkers van de gemeente veilig en laagdrempelig gedaan kunnen worden. We werken samen met private en publieke partijen, zoals inwoners, brancheorganisaties en onze veiligheidspartners om samen weerbaarder te zijn. Een optimale benutting van onze basisregistratiesystemen is een voorwaarde. We toetsen ruimtelijke ontwikkelplannen aan mogelijke effecten op veiligheid en leefbaarheid.*

Bij ondermijning is het vaak niet direct zichtbaar van welke specifieke regeling of wettelijke taak misbruik gemaakt wordt. Daarom is het essentieel, dat signalen van ondermijning geanalyseerd worden alvorens tot actie over te gaan. Tijdens die analyse moet zichtbaar worden of en waar misbruik gemaakt wordt van collectieve voorzieningen. Die analyse biedt de mogelijkheid om met een minimale impact op de persoonlijke levenssfeer richting te geven aan eventuele vervolgstappen.

Door vaste keuzemomenten in te bouwen bepalen we of de informatie uit eerdere stappen voldoende basis vormt voor vervolgacties. Daarnaast kunnen we expliciet rekening houden met de wettelijke bevoegdheden van de betrokken interne en externe partners. Door samen op te trekken, kan doorgepakt worden door de juiste speler of door de juiste spelers, die integraal in staat zijn om de ondermijning aan te pakken. De gemeente Rheden wil natuurlijk dat haar buitenruimte "schoon heel en veilig is".

3.1 Werkproces in hoofdlijnen

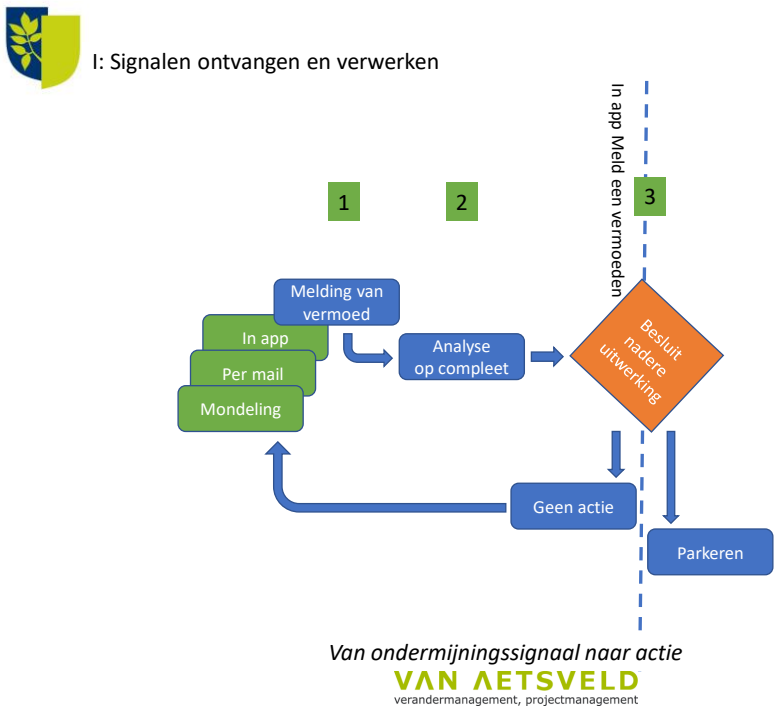
Het werkproces *Van ondermijningssignaal naar actie* ondersteunt het adequaat uitvoeren van de verschillende stappen om te komen tot legitieme acties. Daarbij onderkennen we drie fasen:

I. Signalen ontvangen en verwerken
In deze fase gaat het om het ontvangen van meldingen vanuit de eigen organisatie, via de app *Meld een vermoeden*, mail, schriftelijk of mondeling;

II. Analyse en plan van aanpak
In deze fase toetsen we het signaal tegen interne informatie om te kijken of we het signaal op moeten pakken. Vervolgens bepalen we de doelstelling van de aanpak met betrokken (interne en externe) partners. Als de doelstelling verbonden is aan de thema's die zijn vastgelegd in RIEC-verband, schakelen we de expertise van het RIEC in bij het opstellen van doelstelling en plan van aanpak.

III. Van plan van aanpak naar resultaat
Deze fase omvat de uiteindelijke uitvoering van het plan van aanpak om de doelstelling te behalen. Uiteindelijk gaat het erom, dat we concrete resultaten behalen. Deze fase wordt afgesloten met een evaluatie.

3.2 Processtappen *Van Ondermijningssignaal naar actie*



3.2.1 Signalen ontvangen en verwerken

- Melding van een vermoeden van ondermijning

  Een melding vormt een signaal dat werkt als trigger voor het starten van het proces. De melders maken gebruik van de app *Meld een vermoeden* en kunnen eventueel anoniem melden. Dat betekent, dat de melder zelf geen naam hoeft op te geven bij het doen van een melding. De melding zelf zal natuurlijk wel persoonsgegevens bevatten. Melders zijn in principe alle medewerkers van de gemeente, momenteel beperkt tot de boa's.

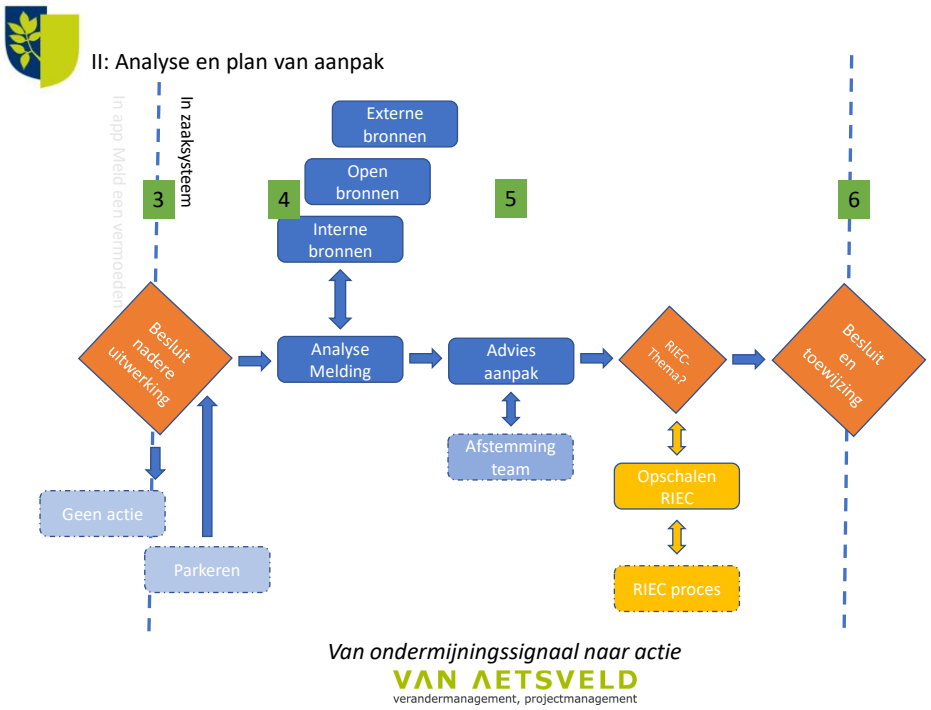
- Analyse van de melding

  De melding komt via het dashboard van *Meld een vermoeden* binnen bij de adviseurs Integrale Veiligheid en wordt bekeken op de inhoud van de melding zelf. Daarbij wordt gekeken of er genoeg gegevens beschikbaar zijn om mee aan de slag te gaan en of het een melding betreft die binnen de gemeentelijke verantwoordelijkheden ligt.

- Keuzemoment: besluit tot nader uitwerken

  De adviseurs integrale veiligheid evalueren of de melding reden is om er een nadere analyse van te maken. Dit leidt tot een vastgelegd besluit om te stoppen of door te gaan. Op kwartaalbasis wordt verantwoord welke besluiten zijn genomen. Bij stoppen blijft het signaal nog zes maanden bewaard in het dashboard van *Meld een vermoeden* ter onderbouwing van het besluit. Signalen worden verwijderd na de verantwoording twee kwartalen later.

3.2.2 Analyse en plan van aanpak



Van ondermijningssignaal naar actie
VAN AETSVELD
verandermanagement, projectmanagement

- Nadere analyse tegen interne en externe bronnen

  Bij het oppakken van de signalen waarmee wordt doorgegaan en het exporteren van deze gegevens vanuit *Meld een vermoeden* naar het zaaksysteem, volgt een raadpleging van verschillende bronnen. Daarbij wordt gekeken of er informatie is; dus alleen naar het feit dàt er informatie is. Dat zijn zowel systemen binnen de gemeente als open bronnen. Op basis van die analyse wordt gekeken of het ondermijningssignaal gecategoriseerd kan worden naar een specifieke soort misbruik. Er wordt een eerste doelstelling opgesteld op grond van de beschikbare informatie.

- Advies aanpak op signaal

  Samen met het lokale ondermijningsteam wordt het dossier besproken. Iedere deelnemer zorgt dat hij of zij weet wàt er aan informatie is. Daardoor kan inhoudelijk gekeken worden of de doelstelling vertaald kan worden naar een plan van aanpak.

- RIEC-thema?

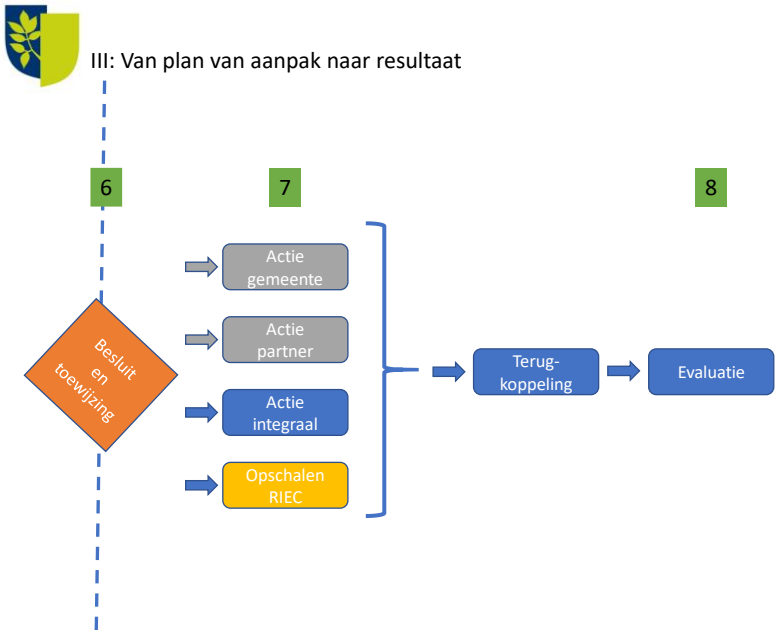
  Als de doelstelling gekoppeld kan worden aan één van de RIEC-thema's of handhavingsknelpunten, wordt het signaal ook doorgezet naar het RIEC en door de verantwoordelijke vanuit de adviseurs Integrale Veiligheid integraal besproken met de externe partners bij het RIEC; politie, Openbaar Ministerie, belastingdienst en eventueel andere door het RIEC geïnventariseerde belanghebbenden.

  Na de analyse volgt een advies over hoe om te gaan met dit signaal. Dat kan zijn:
  - Terzijde leggen;
  - Niet voldoende aanleiding om direct op te pakken, wel bewaken;
  - Monodisciplinair oppakken, door één afdeling of partner;
  - Multidisciplinair oppakken;
  - Opschalen naar integrale sturing via RIEC-lijnen.

- Beslissen en toewijzen

  In overleg tussen partijen wordt bepaald wie het vervolg op gaat pakken. Die toewijzing gebeurt op basis van de bevoegdheden die deze partij (of partijen) in gaat (-n) zetten. En die partij legt hierover verantwoording af aan de gemeente, zodat opvolging en voortgang bewaakt kunnen worden. Afhankelijk van de in te zetten bevoegdheden zullen signaal, informatie en analyse, of alleen het signaal of de (deel-) informatie gedeeld worden.

3.2.3 Van plan van aanpak naar resultaat



Van ondermijningssignaal naar actie
VAN AETSVELD
verandermanagement, projectmanagement

- Actie

  De partij aan wie het signaal is toegewezen, onderneemt vervolgens actie. Deze partij opereert op basis van zijn eigen bevoegdheden.

- Evaluatie

  De verantwoordelijke voor de analyse krijgt achteraf terugkoppeling, zodat lering getrokken kan worden uit de praktijk. Daarmee kan de analyse uit stap 2 en 4 worden verbeterd. Eventuele nieuwe inzichten in ondermijningsvormen worden in deze fase ook gebruikt om het bewustzijn van de medewerkers te verhogen, bijvoorbeeld door het houden van een casusbespreking of het aanvullen van materiaal waarop voorbeeldsignalen staan.

4 Risico's en maatregelen – privacy impact analyse

Dit hoofdstuk beschrijft de in het proces aangetroffen risico's op het gebied van persoonlijke gegevens. Waar mogelijk zijn maatregelen genomen om die risico's weg te nemen of te minimaliseren. Een Gegevensbeschermingseffectbeoordeling is beschikbaar op verzoek.

4.1 Signalen komen van eigen medewerkers

Een eerste filter op de signalen ligt bij de bron: de persoon die de gegevens invult. De app is alleen beschikbaar te stellen aan medewerkers die actief zijn voor de gemeente Rheden (met een @rheden mailadres). Daarmee beperken we de risico's op misbruik van meldingen. Van een ambtenaar van de gemeente mogen wij verwachten dat een melding ter zake is.

Een ambtenaar die een melding doet, ziet na het indienen zijn eigen melding niet meer. Daarmee voorkomen we dat ambtenaren die uit dienst gaan en de app nog actief hebben nog abusievelijk bij gemeentelijke informatie kunnen. Door de eerdere keuze om een beperking in de doelgroep te leggen door alleen boa's te autoriseren is het niet meer mogelijk om de app alleen beschikbaar te stellen in de secure mobile app-store van de Mobile Iron oplossing.

De risicobeperkende maatregel is hiermee het beperkt autoriseren van toegang tot *Meld een Vermoeden.*

4.2 Signalen bevatten persoonsgegevens

Alle signalen zijn herleidbaar naar (natuurlijke) personen. En daarmee vormen zij persoonsgegevens. Een signaal vormt de start van het proces. De traditionele kanalen, e-mail en mondeling of schriftelijk, leiden tot vastlegging in systemen die daar niet voor zijn ingericht. *Dat maakt beheer van de persoonsgegevens lastig of zelfs onmogelijk*. Als een collega een mail stuurt, staat dat bericht (hoogst waarschijnlijk) in zijn verstuurde berichten. En als blijkt dat de melding niet leidt tot vervolg –en deze daarmee vernietigd kan worden-, dan is dat bericht nog aanwezig.

Daarom is gekozen voor het vastleggen van alle meldingen in een centrale voorziening: de app *Meld een vermoeden.* Vanuit die app kan centraal beheer gevoerd worden over de gegevens. Oude en/of niet tot opvolging leidende meldingen worden geschoond in de app.

De risicobeperkende maatregel is hiermee om alle signaalgegevens alleen vast te leggen in *Meld een vermoeden* en daarmee centraal te beheren. Na besluitvorming wordt het nu gebruikte mail-meldadres afgesloten.

4.3 Signalen anoniem verwerken

Gezien de gevoeligheid van het thema ondermijning is ervoor gekozen om het mogelijk te maken om via de app *Meld een vermoeden* anoniem te melden. Dat betekent dat de gegevens van de melder ontbreken. Daarmee beschermen we de persoonlijke levenssfeer van de melder. We voorkomen immers dat herleidbaar is wie het betreffende signaal heeft afgegeven. Dat beschermt de melder tegen pressie vanuit de ondermijners.

De inhoud van de melding is natuurlijk niet anoniem; daarin moet een adres of persoon opgenomen worden.

De risicobeperkende maatregel is het mogelijk maken van anoniem melden.

Momenteel is er slechts een tiental gebruikers. Door het vergroten van het aantal gebruikers van de app naar alle ambtenaren van de gemeente, bereiken we dat meldingen daadwerkelijk anoniem gedaan kunnen worden. Daarmee beschermen we de persoonlijke levenssfeer van de meldende ambtenaar.

4.4 Toegang tot persoonsgegevens beperken

Signalen worden ingevuld in de app *Meld een vermoeden.* Daarmee staan alle persoonsgegevens in die omgeving. Niet iedereen mag zomaar toegang hebben tot deze gegevens.

De app wordt afgenomen als een Cloud-service. Met de verwerker wordt een verwerkingsovereenkomst afgesloten parallel aan de besluitvorming over het proces. Het beheer van gebruikersaccounts ligt bij de gemeente Rheden. De adviseurs Integrale Veiligheid beheren deze accounts. Naast hen kan alleen één systeembeheerder van de leverancier bij de informatie in de database. Zelfs de melder kan niet bij zijn melding na indienen. Alleen de adviseurs Integrale Veiligheid moeten vanwege hun functie bij alle meldingen kunnen.

In *Meld een vermoeden* wordt gelogd welke gebruiker welke verwerkingsacties op gegevens uitvoert. Deze logging is via (het technisch) beheer beschikbaar. Daarmee biedt deze voorziening de garantie dat inzichtelijk is wie, welke persoonsgegevens heeft verwerkt. Er is gekozen voor een halfjaarlijkse controle van deze gegevens door het privacy-aanspreekpunt van de adviseurs Integrale Veiligheid.

De risicobeperkende maatregel is het beperken van de toegang tot het systeem, loggen van de handelingen van de medewerkers en de halfjaarlijkse controle daarop.

4.5 Niet ieder signaal leidt tot actie

Niet ieder signaal is valide of geeft aanleiding tot directe actie. Daarom worden de signalen op regelmatige basis opgeschoond. Registraties die niet leiden tot opvolging worden zes maanden na het indienen van het signaal verwijderd.

De risicobeperkende maatregel is het zesmaandelijks opschonen van de signalen met persoonsgegevens.

4.6 Van signaal naar actie in een ander systeem

Als een signaal wordt opgepakt, dan volgt een raadpleging van gemeentelijke systemen. De adviseurs Integrale Veiligheid kunnen deze raadpleging doen met dit doel. Daarbij wordt een verdergaande inbreuk gedaan op de persoonlijke levenssfeer van degene op wie de melding betrekking heeft (de betrokkene). Daarom is besloten om de verwerking van de vervolgacties in het zaaksysteem GreenValley van de gemeente Rheden in te richten. Hierdoor worden de gegevens "in eigen huis" verwerkt.

De risicobeperkende maatregel is het beperken van de gegevens die bij de leverancier van *Meld een vermoeden* zijn opgeslagen.

4.7 Logging zaaksysteem alleen op verwerkingsactiviteiten

Door het gebruik van GreenValley introduceren we een nieuw risico. Dit systeem logt verwerkingsacties die een medewerker van de gemeente doet, zoals toevoegen, verwijderen en aanpassen. Helaas logt het systeem niet wie welke gegevens inziet.

Dat betekent dat de toegang tot de ondermijningssignaaldossiers beperkt moet worden. Alleen adviseurs Integrale Veiligheid krijgen toegang tot de dossiers voor de verwerking van de signalen in het zaaksysteem. Vanwege functiescheiding is het noodzakelijk dat er een specifieke collega wordt aangewezen die voor een specifiek signaal de diverse systemen van de gemeente raadpleegt of er informatie over een signaal te vinden is.

De risicobeperkende maatregel is het beperkt autoriseren van toegang tot de signaaldossiers en het controleren of die autorisaties actueel zijn.

4.8 Inzien van gegevens uit gemeentelijke systemen beperken

Om te bepalen of een signaal aanleiding geeft om opgepakt te worden, is het van belang om in de diverse systemen van de gemeente te controleren of er informatie aanwezig is. Dat kan op twee manieren:

1. Door een medewerker van iedere afdeling te vragen om te kijken in die systemen of er iets bekend is. Daarbij wordt het signaal met persoonsgegevens gedeeld met de betreffende collega's van de afdelingen van

de gemeente. Zij moeten immers in hun eigen systemen kijken of er informatie te vinden is. Daarmee worden persoonsgegevens op basis van een eerste vermoeden gedeeld. Dat vermoeden kan onterecht zijn.
2. Door adviseurs Integrale Veiligheid de autorisatie te geven om te kijken of er informatie te vinden is in de systemen van de verschillende afdelingen (nagaan dát er informatie te vinden is). Daarmee krijgt een adviseur Integrale Veiligheid toegang tot de verschillende systemen met een beperkte mogelijkheid om te kijken of er iets geregistreerd staat.

Gezien de fase waarin het signaal wordt opgepakt, is gekozen voor de tweede optie. Daarmee wordt een eerste filter gelegd, waarbij een signaal alsnog terzijde gelegd kan worden.

De risicobeperkende maatregel is het autoriseren van een adviseur Integrale Veiligheid op de verschillende systemen om te zien of er informatie beschikbaar is (dàt er gegevens zijn).

4.9 Gegevens van vermoeden uitwerken met het ondermijningsteam

Als blijkt dat er gegevens rond een signaal beschikbaar zijn in de gemeentelijke systemen, dan volgt een inhoudelijke slag. Daarbij wordt gekeken wàt er bekend is. In deze fase is ervoor gekozen om de leden van het ondermijningsteam deze actie uit te laten voeren. Zij kunnen op basis van hun autorisaties inzage krijgen in de gegevens zelf en weten wie van hun collega's eventueel aanvullende informatie kan verstrekken.

Hierbij is ervoor gekozen om eerst in de gemeentelijke context te kijken of bepaald kan worden welk thema van ondermijning het betreft. Om dat beeld op te bouwen is het niet nodig de onderliggende gegevens daadwerkelijk te delen. Wel worden in het gemeentelijk ondermijningsoverleg inzichten gedeeld op basis van die gegevens. Die informatie wordt gebruikt om een doelstelling te formuleren.

De risicobeperkende maatregel is het beperken van de verwerkingsactiviteiten tot de leden van het ondermijningsteam. En bij het behandelen van het signaal niet de geregistreerde gegevens te delen, maar de inzichten te bespreken.

Een tweede risicobeperkende maatregel is hiermee het beperken van delen van gegevens tot binnen de gemeente. De overige spelers als politie en andere (RIEC-) partners ontvangen in deze fase nog geen gegevens.

4.10 Gegevens delen met partners

De informatie vanuit de gemeentelijke systemen leidt tot een doelstelling. Pas als die doelstelling te koppelen is aan die van partners, wordt informatie met hen gedeeld.

Dat kan bijvoorbeeld zijn bij een vermoedelijke koppeling aan de RIEC-thema's. In dat geval wordt informatie gedeeld met die partners om een integraal beeld te krijgen.

De risicobeperkende maatregel is, om pas als er aanleiding is op basis van de doelstelling, gegevens met externe partners te delen.

4.11 Gegevens beperkt overdragen

De gegevens die zijn gebruikt voor het opstellen van de doelstelling kunnen alleen gedeeld worden met partners, als de gemeente die gegevens ook mag verstrekken. De doelstelling van een actie is bepalend voor de in te zetten partners en bevoegdheden. Op basis van die bevoegdheden kunnen de partners aangeven welke informatie zij op welke wijze nodig hebben om tot actie te komen. Denk hierbij aan het vorderen van informatie door justitie voor een strafrechtelijke vervolgstap.

De risicobeperkende maatregel is dat informatie alleen gedeeld wordt als dat kan op basis van de bevoegdheden van de betreffende partner.

4.12 Medewerkers beschermen

Gezien de hiervoor genoemde risico's is het van groot belang, dat de medewerkers van de gemeente die signalen oppakken zelf ook beschermd worden. Zij gaan immers om met persoonsgegevens. De impact van hun handelen op de persoonlijke levenssfeer van de betrokkene kan immer groot zijn. Dat kan zorgen voor een reactie. Dat vraagt om ondersteuning in hun weerbaarheid, zodat zij hun publieke taak veilig uit kunnen voeren. Dat betekent dat zij ook specifieke ondersteuning binnen de organisatie nodig hebben om te zorgen dat zij hun werk kunnen doen. En dat vraagt om zowel politieke als ambtelijke steun.

Gezien de kwetsbaarheid van de informatie is het wenselijk dat alle bij ondermijningsdossiers betrokken collega's op regelmatige basis gescreend worden en dat zij specifiek aangewezen worden om dit werk te doen. Het bieden van een veilige omgeving vraagt ook om het bespreekbaar maken van dilemma's die zich voordoen.

De gemeente is momenteel bezig met de benoeming van een privacy-aanspreekpunt per team. Deze persoon zal in principe als eerste aanspreekpunt functioneren voor het team en daarmee controles uitvoeren. Indien hierbij vervolgens problemen worden geconstateerd, zal deze persoon dit in het Privacy Team aangeven en zal óf de Privacy Officer van de Gemeente Rheden (voor uitvoerende taken) óf de Functionaris Gegevensbescherming (algemeen toezicht & advies) dit verder oppakken.

De risicobeperkende maatregel is het specifiek aanstellen van medewerkers om ondermijningsdossiers op te pakken en hen te voorzien van ondersteuning daarbij.

Een aanvullende risicobeperkende maatregel is het feit dat politiek en bestuurlijk de prioriteit van het aanpakken van ondermijning op de hier gedocumenteerde wijze wordt gevoeld en onderschreven.

4.13 Verwerking in zaaksysteem

Met GreenValley is (nog) geen Verwerkersovereenkomst (VO) gesloten. Wel bestaat een Bewerkersovereenkomst uit 2016 op basis van Wbp. De gemeente is bezig om deze te laten omzetten naar een model VO. Er zijn risico's verbonden aan het gebruik van het zaaksysteem. Er loopt momenteel een project om de autorisaties in het systeem te verbeteren en enkele veiligheidsrisico's uit te bannen.

De risicobeperkende maatregel is het sluiten van de verwerkingsovereenkomst. Deze actie raakt de hele gemeentelijke organisatie die gebruik maakt van GreenValley en daarmee alle gebruikers van het zaaksysteem. Vanuit de adviseurs integrale veiligheid zullen deze ontwikkelingen gevolgd worden. Dit risico is bekend en wordt gedragen door de gemeente.

4.14 Verwerking gegevens door ODRA

Momenteel is niet inzichtelijk hoe de verwerking van gegevens door ODRA verloopt. Vanuit het kader van de naleving van de AVG wordt dit traject onderzocht. Dit risico geldt gemeentebreed en wordt daarmee geaccepteerd.

De risicobeperkende maatregel is het accepteren van de status quo en het volgen van de stappen die hierop gezet worden.

4.15 Reactie op review door FG

De FG heeft dit procesdocument en de Gegevensbeschermingseffectbeoordeling uitgebreid beoordeeld. Dat heeft op een aantal punten geleid tot nadere aanscherping van beide stukken. Daarvoor onze dank!

In grote lijnen:

- De grondslagen voor verwerking zijn aangevuld met de artikelen in de aangegeven wettelijke grondslagen zijn nader geduid;
- De FG signaleert en adviseert dat rond het zaaksysteem, o.a. op gebied van logging nog gewerkt moet worden aan AVG-compliance. Die constatering onderschrijven we. Het betreft een gemeente-brede aanbeveling die we van harte ondersteunen. Omdat we slechts een van de vele gebruikers zijn van dat systeem, is het niet mogelijk dat binnen de scope van dit traject op te lossen;
- De gegevensuitwisseling tussen de verschillende systemen en met externe partners is nader expliciet gemaakt. Er wordt gebruik gemaakt van pdf-export en -import om de gegevens over te dragen;

- Voor de in 2017 aangeschafte app Meld een vermoeden wordt een verwerkingsovereenkomst afgesloten parallel aan de besluitvorming;
- Op verzoek van de FG is aangegeven vanaf wanneer de bewaartermijnen in gaan;
- De FG doet een aantal uitspraken over het wel of niet wenselijk zijn van anoniem melden. Dat aspect zien wij niet als een zaak die raakt aan de persoonlijke levenssfeer, anders dan dat we die van ambtenaren -en die mogelijk onder druk worden gezet door ondermijnende burgers- die melden willen beschermen. Daarmee laten we deze discussie over aan organisatie en politie;
- Het overleg over de gegevens betreft geen gegevensverwerking in de zin van de AVG. De reden van overleg is juist om inzichten vanuit de betrokken afdelingen af te stemmen, zodat bepaald kan worden of er aanleiding is voor vervolgactie en zo ja, met wel doel de vervolgstap wordt gezet.

5 Aanbevolen maatregelen

Zoals in het voorgaande hoofdstuk is aangegeven, zijn er nog verschillende zaken die aanvullend aan de procesbeschrijving geregeld kunnen of moeten worden.

5.1 Aanwijzen functionarissen

Als eerste het aanwijzen van de adviseurs Integrale Veiligheid zodat zij geformaliseerd hun rol in dit proces uit kunnen voeren. Zij voeren de regie en raadplegen informatie. De vier adviseurs Integrale Veiligheid vormen daarmee een cruciale schakel in de aanpak van ondermijning. Dat maakt hen ook kwetsbaar. Door hen specifiek aan te wijzen voor deze rol, kunnen zij beter beschermd hun werk doen.

5.2 Bewustwording ondermijning

De tweede aanbeveling heeft te maken met het verhogen van de kwaliteit van meldingen. Het verdient aanbeveling om te zorgen dat alle medewerkers die de app gaan gebruiken, zich bewust zijn van wat Ondermijning betekent. Daartoe moeten zij een toelichting en instructie krijgen over het gebruik van de app.

5.3 Integriteitsdilemma's bespreekbaar maken

Het verdient aanbeveling om in navolging van de gemeente Tilburg te zorgen dat bestuurlijk of operationele dilemma's rond de aanpak van signalen besproken kunnen worden. In die gemeente is een dilemmatafel ingericht. Vraagstukken kunnen daar ingebracht worden om duiding te krijgen over hoe om te gaan met de gesignaleerde dilemma's.

In Tilburg worden de signalen vertrouwelijk besproken met een afdelingshoofd, de gemeentesecretaris en betrokken collega (`s). In geval van politieke gevoeligheid wordt er tevens voor gekozen om een wethouder uit te nodigen. Het is van groot belang dat dilemma's achter gesloten deuren en vertrouwelijk kunnen worden besproken.

5.4 Uitbestede diensten betrekken

Het verdient aanbeveling om afspraken te maken met De Connectie, ODRA en wellicht ook de omgevingsdienst Gelderland Midden. Deze spelers voeren gemandateerde of gedelegeerde activiteiten uit voor de gemeente. Dat betekent dat zij in hun dagelijks werk gewoon gemeentelijke taken uitvoeren. Daarmee moeten zij aansluiten bij het ondermijningsteam om ook eventuele vervolgacties op te pakken. En meldingen kunnen doen in de app *Meld een vermoeden.*

5.5 Politiek en bestuurlijk draagvlak

Politiek en bestuurlijk is de aanpak van ondermijning geprioriteerd. Daarom is het van groot belang dat de politiek en het bestuur de werkwijze van het ondermijningsteam onderschrijven. Ook als er in de maatschappij consequenties gevoeld worden, moet er doorgepakt worden.

5.6 Auditcyclus opzetten

Door het inregelen van een auditcyclus kan grip gehouden worden op de risico's uit hoofdstuk 4. Wellicht is het mogelijk om aan te sluiten op bestaande controles. Naast de reguliere bewaking van toegang tot de verschillende systemen, dient twee keer per jaar de autorisatie gecontroleerd te worden. Een privacy-aanspreekpunt kan deze controles uitvoeren en daarover rapporteren aan de verantwoordelijke lijnfunctionaris, de burgemeester in verband met inzet van bevoegdheden, en het Privacy Team/de Functionaris Gegevensverwerking.

6 Uitwerking processtap 1: Melding van een vermoeden van ondermijning

In deze stap meldt een medewerker van de gemeente (of mogelijk een van haar partners) een vermoeden van ondermijning. Doel van de melding is om vermoedelijk ondermijnende activiteiten te voorkomen of te stoppen. Een melding moet een aantal inhoudelijke elementen bevatten om opgepakt te kunnen worden in het verwerkings-proces. De informatie waarop een melding wordt gebaseerd kan uit de tweede hand zijn (ik heb gehoord dat.., het gerucht gaat…).

De melder geeft door:
- een locatie (adres);
- soort vermoeden;
- omschrijving van het vermoeden;
- indien mogelijk beeldmateriaal (foto);
- of het een vermoeden is of een concrete constatering.

(Mogelijke) persoonsgegevens in de melding zijn *de naam* van de melder (tenzij anoniem), *de locatie* (het adres), eventuele *verwijzingen naar personen* in de mogelijke omschrijving en *het beeldmateriaal*.

6.1 Hoe komen de signalen binnen?

Signalen komen via verschillende middelen binnen. Hieronder een uitwerking met voor- en nadelen van de verschillende middelen.

6.1.1 Ingezette middelen - Mailadres ondermijning@rheden.nl

Binnen de gemeente Rheden wordt al langer gebruik gemaakt van meldingen via een mailadres (ondermijning@rheden.nl). Daarbij staat het de melder vrij om alles wat hij of zij relevant vindt te melden in het vrije format van een mailbericht.

Risico van incomplete informatie

Door het ontbreken van structuur in een mailbericht is het lastig om van de vermoedens te bepalen welke aangeleverde gegevens persoonsgegevens zijn. Daarnaast is het niet mogelijk om anoniem te melden.

Opschonen lastig tot onmogelijk

Beheer van deze mailberichten is lastig: kopieën kunnen immers ook aanwezig zijn bij de inzender van het verstuurde bericht en bij eventuele anderen met wie het bericht gedeeld is. Verwijderen van persoonsgegevens is daarbij lastig.

6.1.2 Ingezette middelen – App "Meld een vermoeden"

Om het melden gemakkelijker te maken is de app "*Meld een vermoeden*" aangeschaft. Hiervoor is in 2017 een aanbestedingsprocedure doorlopen. Deze app wordt geleverd door de Anti-Fraud Company. Binnen de app kan gestructureerd gemeld worden. Dat

maakt het mogelijk om bijvoorbeeld de categorieën vermoedens op te nemen waarop de gemeente actie kan ondernemen.

Categoriseren van meldingen

In de app kunnen categorieën opgenomen worden. Dat maakt het mogelijk een melder te helpen bepalen wat hij wil melden. En die categorieën kunnen direct gekoppeld zijn aan het wettelijk mandaat dat de gemeente heeft. Denk aan de gemeentelijke bevoegdheden op het gebied van overbewoning in het kader van BRP-controles, uitkeringsfraude en andere vormen van misbruik. Daarnaast kunnen de categorieën vanuit het RIEC-convenant worden opgenomen. Denk daarbij aan mensenhandel, drugs (-handel en -productie), witwassen, fraudevormen, outlaw motorbendes en andere vastgestelde thema's.

Anoniem melden

De app voorziet in de mogelijkheid om anoniem te melden. Momenteel gebruiken alleen de bijzondere opsporingsambtenaren (boa's) de app. Omdat we in dat geval te maken hebben met een kleine doelgroep is al snel te herleiden wie gemeld heeft. Dat betekent dat anonimiteit vraagt om een groot/groter aantal gebruikers.

Als het aantal gebruikers te klein is, kan immers (mogelijk) terug geredeneerd worden wie de melding heeft gedaan. Het rapporteren van eventuele vervolgacties is bij een anonieme melding natuurlijk niet mogelijk. Met het formaliseren van dit werkproces is het de bedoeling dat iedere medewerker van (of medewerker die taken uitvoert namens) de gemeente Rheden toegang heeft tot de app en kan melden.

Opschonen en loggen

De app op een mobiele telefoon zet gegevens in een centrale omgeving. Die omgeving staat in een datacenter dat als Cloud-service haar diensten levert. Alle handelingen die gedaan worden op dat systeem, worden gelogd. De leverancier Anti -Fraud Company kan deze logging inzien en -indien gewenst of noodzakelijk- beschikbaar stellen aan de gemeente Rheden. Hiermee is inzichtelijk wie welke verwerkingen heeft gedaan op de beschikbare data.

De app voorziet in de mogelijkheid om gegevens weg te gooien. Op basis van vastgestelde uitgangspunten kunnen meldingen verwijderd worden. Daarmee wordt voorkomen dat persoonsgegevens onnodig bewaard blijven.

6.1.3 Ingezette middelen – Mondelinge of schriftelijke meldingen

Naast mail en app komen ook signalen mondeling binnen. De afspraak is, dat die door de ontvangende medewerker ingevoerd worden in de app. Daarmee ontstaat een centraal overzicht van alle meldingen in de app *Meld een vermoeden*.

Schriftelijke informatie kan gescand worden om aan het dossier in het zaaksysteem toegevoegd te worden.

6.2 Verwerkingsgrondslag

Op basis van het voorgaande geldt een verwerkingsgrondslag voor de persoonsgegevens is artikel 6.1.e AVG; de **noodzaak voor de vervulling van een taak van algemeen belang of uitoefening van het openbaar gezag.** We willen immers misbruik van collectieve voorzieningen voorkomen. Het Europees Verdrag van de Rechten van de Mens (EVRM) zegt daar in artikel 8 het volgende over:

Artikel 8 – Recht op eerbiediging van privé familie- en gezinsleven

1. Eenieder heeft het recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan *voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen*.

In hoofdstuk 14 zijn de grondslagen nader weergegeven. Wie mag er melden? Melden staat vrij aan *alle* ambtenaren van de gemeente Rheden (via de app *Meld een vermoeden)*. Als vertegenwoordigers van de gemeente horen en zien zij dagelijks zaken die van belang kunnen zijn bij de aanpak van ondermijning. Door melding zo laagdrempelig mogelijk te maken kunnen signalen snel en adequaat opgepakt worden. Melders kunnen in de app anoniem melden.

6.3 Verwerker

De verwerking van de gegevens wordt gedaan door Anti-Fraud Company. Zij bieden de app en een centrale locatie (een Cloud server) waar de gegevens opgeslagen worden. Omdat een deel van de opgeslagen gegevens persoonsgegevens betreft, moet met deze partij een verwerkingsovereenkomst gesloten worden.

6.4 Wie kan er bij deze gegevens?

De gegevens op de centrale locatie (een Cloud server) zijn alleen toegankelijk voor specifiek aangewezen adviseurs Integrale Veiligheid. De adviseurs Integrale Veiligheid beheren de autorisatie en zijn verantwoordelijk voor het muteren van autorisaties als medewerkers een andere functie krijgen.

Anti-Fraud Company logt alle verwerkingen op de Cloud-server. Daardoor is inzichtelijk te maken wie wanneer welke informatie heeft ingezien. In de verwerkingsovereenkomst wordt geregeld dat hierop op reguliere basis toezicht gehouden kan worden door een privacy-aanspreekpunt van de gemeente Rheden.

Dit privacy-aanspreekpunt moet door of namens de adviseurs Integrale Veiligheid aangewezen zijn en zelf geen inhoudelijke taak hebben in het proces. De functionaris rapporteert aan de burgemeester als verantwoordelijke voor veiligheid. Het voorstel is, dat deze controle halfjaarlijks wordt uitgevoerd. Die periode loopt parallel aan de opschoningsfrequentie, die dan tegelijkertijd gecontroleerd kan worden.

Binnen de gemeente loopt momenteel een traject rond de benoeming van privacy-aanspreekpunten per team. Deze personen zullen in principe als eerste aanspreekpunt functioneren voor een team en daarmee deze controle moeten uitvoeren. Indien hierbij vervolgens problemen worden geconstateerd, zullen deze personen dit in het Privacy Team aangeven en zal óf de Privacy Officer van de Gemeente Rheden (voor uitvoerende taken) óf de Functionaris Gegevensbescherming (algemeen toezicht & advies) dit verder oppakken.

Het privacy-aanspreekpunt controleert:

- wie er rechten heeft;
- of die rechten ook passen bij de vervulde functie;
- of de signalen zijn opgeschoond conform de bewaartermijnen;
- op basis van een steekproef welke informatie door wie verwerkt is en of dat legitiem is.

7 Uitwerking processtap 2: Analyse van de melding

De adviseurs Integrale Veiligheid krijgen een signaal als een melding binnen komt. Vervolgens wordt een specifieke adviseur gevraagd het signaal te valideren. Hiermee voorkomen we dat diverse medewerkers persoonsgegevens gaan beoordelen. Deze validatie betreft alleen de beoordeling van de gegevens die in het signaal zijn opgenomen.

Deze stap heeft als doel te zorgen dat alleen die meldingen worden opgepakt, die daadwerkelijk compleet zijn, zodat ze nader uitgewerkt kunnen worden. Als bijvoorbeeld de locatie ontbreekt, zal gekeken moeten worden of de omschrijving afdoende aanknopingspunten geeft om te bepalen waar wat speelt. Als de melding niet anoniem is gedaan, kan eventueel in deze fase contact gezocht worden met de melder om gegevens aangevuld of verhelderd te krijgen.

7.1 Verwerkingsgrondslag

De verwerkingsgrondslag ligt in lijn met die van processtap 1. De verwerking betreft een analyse op kwalitatieve gronden, zodat de juiste informatie de basis vormt voor de vervolgstappen. In principe wordt door de beoordelaar niets veranderd aan de informatie. De informatie blijft op de centrale omgeving van de app *Meld een vermoeden* van Anti-Fraud Company.

Gegevens worden op kwartaalbasis geëvalueerd. Na twee evaluaties (zes tot negen maanden na registratie) worden meldingen die niet zijn opgepakt verwijderd.

8 Uitwerking processtap 3: Keuzemoment - besluit tot nader uitwerken

Na het uitvoeren van stap 2 volgt een beslismoment. Daarin wordt bepaald of de melding nader wordt geanalyseerd of terzijde gelegd.

Als de melding compleet is, volgt de eerste inschatting of het een melding betreft die binnen de sfeer van de (brede) gemeentelijke verantwoordelijkheden valt. In dat geval wordt de melding opgepakt voor nadere analyse. Als dat niet het geval is, zal het signaal terzijde worden gelegd en mogelijk contact gezocht worden met de melder om deze te verwijzen naar een instantie die wel iets met de melding kan. Het delen van persoonsgegevens zonder grondslag is immers niet toegestaan. De melder zal daarom zelf actie moeten ondernemen om een melding bij de juiste partij te doen.

Het besluit wordt vastgelegd in de centrale omgeving (Cloud server) van Anti-Fraud Company.

8.1 Wie neemt het besluit?

De behandelaar van het signaal doet een voorstel aan een van de adviseurs Integrale Veiligheid. Op basis van het *vier ogenprincipe*[1] nemen zij het besluit.

8.2 Verwerkingsgrondslag

De verwerkingsgrondslag ligt in lijn met die van de processtappen 1 en 2. De verwerking betreft een besluit tot het wel of niet zetten van vervolgstappen. Het besluit wordt vastgelegd. Deze registratie betreft een procesgegeven en daarmee geen persoonsgegeven. De informatie blijft op de centrale omgeving van Anti-Fraud Company.

[1] Vier ogenprincipe betekent dat een collega die niet inhoudelijk bij de eerdere stappen betrokken is, wordt bijgepraat en geraadpleegd om vervolgens gezamenlijk een besluit te nemen. Dat vult een integriteitsprincipe in, omdat daarmee wordt voorkomen dat een medewerker eigenstandig besluiten neemt, waarbij de mogelijkheid bestaat dat die besluiten beïnvloed worden door het eigen referentiekader of invloeden van buiten.

9 Uitwerking processtap 4: Nadere analyse tegen interne en externe bronnen

De informatie (vermoedens) uit het signaal wordt **verrijkt met informatie uit de gemeentelijke systemen en open bronnen**. Doel daarvan is om een **completer beeld** te krijgen wat er zich op die locatie/het specifieke adres afspeelt. In eerste instantie wordt daarbij gekeken of er iets bekend is (DAT het adres of de persoon bekend is). Wát er in de systemen bekend is, wordt pas onderzocht door de betreffende afdeling die over die informatie beschikt.

Soort gegevens	Upgrade indien nodig met doel inzicht te krijgen in:	Geoview	Gegevensmakelaar	Kamer van koophandel	Zaaksysteem	Google, Facebook, Linked in …	MOR-meldingen	Kadaster
Adres	basisinformatie	X						
Bestemming	Beoordeling strijdig gebruik	X						
Eigendom pand	Inschatting soort pand (huur, koop) kan van belang zijn voor aanpak	X						
	Wie zijn nog meer betrokken bij eigendom pand							X
Bewoners	Basisinformatie	X						
	Soort huishouden (familie), kamerbewoning?		X					
	Migratiepatroon (onder de radar willen blijven)		X					
Bedrijven	Match bedrijf en bewoner?	X		X				
Contacten gemeente	Lopen er nog andere zaken binnen de gemeente, uitkeringen, handhavingszaken, betrokkenheid sociaal gebiedsteam, Bibob				X			
Algemene info open bronnen						X		
Meldingen	Inzicht in overlast of andere klachten						X	

De volgende bronnen worden bevraagd:

Bron	Zoekvraag	Toelichting
Greenvalley	Welke zaaktypen spelen er op het adres?	Inhoudelijk wordt de correspondentie niet ingezien. Doel is om te achterhalen bij welke afdelingen contextinformatie gehaald kan worden.
Makelaar	Wie woont op het adres? Hoe is de relatie tussen bewoners?	Opvallende zaken, bijvoorbeeld veel verhuizingen van een persoon tijd of mutaties op dat adres binnen korte tijd?
SQUIT	Zijn er bijzonderheden m.b.t. wabovergunningen of handhavingstrajecten	Kloppen de vergunningen? Is er sprake van afgesloten of lopende handhavingstrajecten?
Geoview	Wie is eigenaar van het perceel? Zijn er bedrijven geregistreerd op het adres? Bestemming van het pand?	Zijn deze gegevens in overeenstemming met het signaal?
KvK	Welke branche? Wie zijn eigenaren van het bedrijf?	Klopt dit met de bestemming van het pand?
VIS	Is er sprake van vergunningen bijzondere wetten?	Kloppen de vergunningen?
SuWI	Welke uitkeringen ontvangt iemand?	Uitvraag door betreffende lid van ondermijningsteam. Alleen delen indien relevant voor aanpak.
ODRA/ Connectie	Nog nader uit te werken bij aansluiting.	
Google	Wat voor informatie krijg je als je het adres, bedrijf of bewoners googelt?	Informatie uit open bron die mogelijk aanvullend kan zijn aan het signaal of kan helpen het signaal verder te duiden.

Daarbij wordt tevens onder de signalen op de Cloud server van *Meld een Vermoeden* gekeken of er in de voorafgaande zes maanden signalen binnen zijn gekomen op of rond dit adres. Het kan immers zijn dat de inhoud van de analyse het mogelijk maakt een andere interpretatie te hangen aan eerder ontvangen signalen. Daardoor kunnen eventueel eerder geparkeerde meldingen meegenomen worden in de nadere analyse.

Op basis van de bevraging van de eigen gemeentelijke bronnen ontstaat een eerste beeld van de context van de ondermijningscasus: wat kan er aan de hand zijn? Dat beeld vormt de doelbinding voor vervolgstappen om de informatie te verrijken. Dat kan aanleiding zijn om binnen de gemeente te schakelen met collega's van het gemeentelijk kernteam ondermijning om meer context te krijgen bij de analyse. Door gebruik te maken van het kernteam wordt voorkomen dat persoonsgegevens breed de organisatie in gaan. Het kernteam is specifiek aangewezen om dit soort activiteiten op te pakken.

De vervolgstap wordt dus gezet samen met het gemeentelijk kernteam ondermijning.

Gemeentelijk kernteam ondermijning	
Adviseur Integrale Veiligheid	Bijzondere wetten, exploitatievergunningen, ondermijning, Wet Bibob
Sociale rechercheur	Onderzoeken uitkeringsfraude e.d.
Kwaliteitsmedewerker werk en inkomen en fraudepreventiemedewerkers van Werk en Inkomen	Uitkeringen
Sociaal gebiedsteam	Bijzonderheden vanuit zorg
Toezicht- en handhaving	Informatie vanuit waarnemingen surveillance, handhavingstrajecten APV, meldingen MOR
Wabo	Toezichthouder bouwen en milieu, handhavingstrajecten, vergunningen
Medewerker burgerzaken/publieksbureau	Adrescontrole, inschrijvingen BRP
ODRA	Nog niet aangesloten
Brandweer	Nog niet aangesloten
Belastingen (Connectie)	Nog niet aangesloten

Samen met het kernteam ondermijning wordt de analyse compleet gemaakt voor zover het de bestuurlijke informatie betreft uit de gemeente zelf. Daartoe doorzoeken de betrokken collega's de systemen van hun eigen afdeling. Centraal staat wát de informatie is die daarin besloten ligt. Door het gezamenlijk bespreken van de inzichten ontstaat een gemeenschappelijk beeld, zonder dat de inhoudelijke details gedeeld hoeven worden. Daarbij wordt gezamenlijk bepaald welk thema het betreft, welk doel gemeentelijk wordt nagestreefd en waar mogelijk een opzet gemaakt voor het plan van aanpak.

9.1 Externe partners betrekken

Als de analyse betrekking heeft op één van de thema's of handhavingsknelpunten van het RIEC, wordt de lijn naar het RIEC ingezet. Op basis van het *informatierapport gemeente* van het RIEC wordt een aanvraag naar het informatieplein van het RIEC

gedaan. Daarnaast zal vanuit de gemeente met in een brede ondermijningstafel met de RIEC-partners (in ieder geval Belastingdienst, Politie en Openbaar Ministerie) overlegd worden over de melding (bij hen bekend als RIEC-casus). Daarbij is de verantwoordelijke adviseur Integrale Veiligheid aanwezig om de casus in te brengen, toe te lichten en om de bestuurlijke lijn te verhelderen.

9.2 Vastlegging

Alle gegevens uit de analyse worden vastgelegd in het *zaaksysteem*. Het betreft een dossier van het zaaktype *anoniem*. Hierdoor wordt het niet gekoppeld aan het dossier van de betreffende burger, locatie of bedrijf. Daarmee voorkomen we dat gegevens uit dit dossier zomaar gedeeld worden met de betrokkene. Het dossiernummer van het zaaksysteem wordt bij de melding in de app *Meld een vermoeden* van Anti-Fraud Company opgenomen. Daarmee zorgen we er vanwege rapportagedoeleinden voor dat we signalen aan dossiers kunnen koppelen en inzichtelijk hebben of er opvolging gegeven is aan een signaal. In het zaaksysteem wordt opgenomen welke signalen zijn meegenomen in de analyse (n:1 relatie)

Het dossier in het zaaksysteem heeft de opsteller van de analyse als eigenaar. Anderen kunnen niet bij het dossier. Als een medewerker een andere functie krijgt, zijn de adviseurs Integrale Veiligheid verantwoordelijk voor de overdracht van de dossiers aan collega's.

Hierdoor zorgen we voor een vorm van functiescheiding binnen het team. Het zou immers zomaar kunnen zijn, dat de analyse uiteindelijk aanleiding is om vanuit de adviseurs Integrale Veiligheid actie te ondernemen. En dan dienen wettelijke bevoegdheden gerespecteerd te worden. In dat geval zal een collega het vervolg dus op moeten pakken en op eigen bevoegdheden een uitvoeringsdossier samenstellen.

Het zaaksysteem voorziet (nog) niet in volledige logging. Muteren en verwijderen is zichtbaar. Raadplegen (tonen van de informatie) is helaas niet te achterhalen. Daardoor kunnen we niet in alle gevallen vaststellen wie welke verwerkingen heeft gedaan. Dit betreft een beperking van het systeem onder GreenValley, dat voor alle gebruikte processen in GreenValley geldt.

De gegevens van het signaal uit *Meld een vermoeden* kunnen als pdf-bestand geïmporteerd worden, waardoor het dossier compleet is met de startinformatie. Door een juiste opbouw van de zaak kan eventueel in het systeem opgeslagen informatie bij verdere verwerking gedeeltelijk beschikbaar gesteld worden aan afdelingen binnen de gemeente die verantwoordelijk zijn voor of bijdragen aan het aanpakken van het signaal.

9.3 Verwerkingsgrondslag

Op basis van voorgaande informatie geldt een verwerkingsgrondslag voor de persoonsgegevens op basis van de noodzaak voor de vervulling van een taak van algemeen belang of uitoefening van het openbaar gezag. Indien de melding een van de thema's of handhavingsknelpunten van het RIEC betreft, geldt diezelfde basis. Via de lijn van integrale sturing op de benoemde thema's en handhavingsknelpunten kunnen de RIEC-partners informatie delen. Dat is beschreven (inclusief mandaten) in het RIEC-convenant. De basis van het RIEC-convenant ligt in het aanpakken van de georganiseerde criminaliteit en de uitwassen daarvan.

9.4 Wie doet de analyse?

Deze stap brengt een dilemma aan de orde. Als we zorgvuldig willen handelen, willen we zo snel mogelijk alle (mogelijk) betrokken (interne en mogelijk ook externe) partners bevragen. Dat kan echter alleen door het vermoeden met de diverse partners te delen. En daarmee worden persoonsgegevens op basis van een zachte aanleiding gedeeld.

Die insteek wordt door de gemeente Rheden als niet wenselijk beschouwd. Het alternatief is dat deze stap doorlopen wordt vanuit een *onderzoeksgerichte* vraagstelling. Dat betekent dat een adviseur Integrale Veiligheid het signaal oppakt en zelf de verschillende systemen bevraagt. Hierdoor zijn de persoonsgegevens bij één medewerker bekend en bouwt deze vanuit de bevraagde systemen een beeld op van de situatie. Daarmee voldoen we aan een zorgvuldigheidsbeginsel: persoonsgegeven zijn in dat geval alleen bekend bij die medewerker.

De medewerker zal vervolgens een beeld opbouwen van wie er betrokken moeten worden bij het oppakken van de zaak/het dossier. Die partijen wordt gevraagd aan te sluiten en via hun eigen bevoegdheden en autorisaties nadere informatie in te winnen. Die informatie (eigenlijk data) wordt niet inhoudelijk gedeeld; wel worden de inzichten besproken om gezamenlijk te komen tot een doelstelling en aanpak.

Als doelstelling en/of aanpak gekoppeld kunnen worden aan de RIEC-thema's, volgt een tweede uitvraag via de RIEC-lijn. Al deze informatie komt terug via de behandelend adviseur Integrale Veiligheid.

9.5 Autorisatie en opschoning

De keuze is daarom één medewerker het vermoeden te laten onderzoeken en daartoe te autoriseren voor de verschillende systemen. Dat betekent dat de activiteiten van die medewerker in die systemen gelogd moeten worden en dat er regulier (bij voorkeur halfjaarlijks) een audit moet plaatsvinden op het correct gebruik van deze autorisaties. De burgemeester onder wiens bevoegdheid wordt gewerkt, dient deze audit jaarlijks uit te laten voeren door een privacy-aanspreekpunt en daarover te laten verantwoorden in het veiligheidsjaarverslag.

10 Uitwerking processtap 5: Advies aanpak op signaal

Na de analyse volgt een advies hoe om te gaan met dit signaal. Daarbij wordt bepaald wat het doel is van de aanpak, waar mogelijk gekoppeld aan de ondermijnings-thematiek die aangepakt moet worden. Daarbij wordt ook bepaald welke partij of partijen het beste in staat zijn om in actie te komen.

De vervolgactie kan zijn:
1. Terzijde leggen;
2. Niet voldoende aanleiding op direct op te pakken, wel bewaken;
3. Monodisciplinair oppakken, door één afdeling of partner;
4. Multidisciplinair oppakken;
5. Opschalen naar integrale aanpak via RIEC-lijnen en integrale sturing.

In de gevallen 3 tot en met 5 moet het advies zodanig opgebouwd zijn, dat het het doel voor de vervolgactie omvat. Deze doelstelling is essentieel om tot besluitvorming over vervolg te komen. Bij een correcte formulering van de doelstelling is het mogelijk om persoonsgegevens uit de eerdere stappen over te dragen aan de partij(-en) die tot actie over moeten gaan.

Periodiek wordt een overleg georganiseerd met een lokaal ondermijningsteam. Daarin worden de bestuurlijke maatregelen besproken. Aanvullend vindt overleg plaats met de politie en de accountmanager RIEC. Dit is te vergelijken met het voormalige lokale RIEC-casustafeloverleg. We noemen dit *lokaal ondermijningsoverleg*.

Als een casus bestuurlijk is opgewerkt en vanuit politie en /of RIEC komen signalen dat andere partners aan willen sluiten, dan wordt een casus via de RIEC-lijn ingebracht naar het informatieplein. Hiermee loopt het proces van de opstart binnen de gemeente door naar de partners. Zie dit als lokaal starten en waar nodig bovenlokaal opschalen. Hiermee acteren we conform de Wassenaarnotitie (sturing over politie) waar het gaat over sturing van openbaar bestuur en openbaar ministerie op de politie. Die lijn loopt door van lokaal naar (intern-) nationaal.

10.1 Doel van het ondermijningsoverleg

Doel van dit lokale ondermijningsoverleg is te bepalen of het beeld compleet is, aanleiding geeft tot meer verrijking en of voor de concrete aanpak opgeschaald moet worden naar het RIEC. Dat gebeurt door het invullen van het RIEC-informatieformulier. De gemeentelijke regisseur maakt het formulier aan. De politie vult zijn/haar specifieke informatie via RIEC/IS in. Deze informatiedeling valt onder het RIEC-convenant.

<table>
<tr><th>Basisinformatie + contextinformatie + informatie van politie = resultaat A, B of C</th><th>Vervolgstap 1</th><th>Vervolgstap 2</th><th>Vervolgstap 3</th></tr>
<tr><td rowspan="5">A. Compleet beeld + sprake van ondermijning</td><td>Bepalen van de aanpak:</td><td>Toetsing in overleg team ondermijning</td><td></td></tr>
<tr><td rowspan="2">Alleen strafrechtelijk</td><td colspan="2">Opstarten strafrechtelijk proces</td></tr>
<tr><td>Verrijking door RIEC wenselijk</td><td>Invullen RIEC-formulier: afsluiten van de casus in de website</td></tr>
<tr><td rowspan="2">Alleen gemeentelijk proces</td><td colspan="2">Opstarten gemeentelijk proces</td></tr>
<tr><td>Verrijking door RIEC wenselijk</td><td>Invullen RIEC-formulier: afsluiten van de casus in de website</td></tr>
<tr><td>Integrale aanpak</td><td>Verrijking door RIEC wenselijk</td><td>Invullen RIEC-formulier: afsluiten van de casus in de website</td></tr>
<tr><td rowspan="2">B. Compleet beeld + geen sprake van ondermijning</td><td colspan="2" rowspan="2">Check of situatie voldoet aan alle gemeentelijke processen (brandveiligheid, vergunningen, bestemming)</td><td>Ja: afsluiten van de melding in het zaaksysteem en terugkoppeling aan de melder</td></tr>
<tr><td>Nee: betreffende gemeentelijk proces inzetten + terugkoppeling naar melder</td></tr>
<tr><td>C. Geen compleet beeld van de situatie</td><td colspan="2">Bespreking in overleg team ondermijning
- Plan van aanpak om beeld compleet te krijgen (bv. adrescontrole, brandweercontrole)
- Uitvoering van plan van aanpak</td><td>Resultaat = Terug naar A of B</td></tr>
</table>

Als er sprake is van opschalen, wordt het signaalformulier door de accountregisseur van het RIEC onder de aandacht gebracht van de RIEC-partners en geagendeerd voor bespreking in het Infoplein. In het Infoplein zijn vertegenwoordigd: de politie, het openbaar ministerie, de belastingdienst, de accountmanager van het RIEC en een vertegenwoordiger van de betreffende gemeente (de adviseur Integrale Veiligheid die het dossier onder handen heeft).

Op het Infoplein wordt het signaal beoordeeld op zowel proces als inhoud. Verder wordt ingeschat of het signaal in behandeling genomen kan worden voor een integrale aanpak door het Infoplein of lokaal of dat de strafrechtelijke aanpak de beste kaart in handen heeft en aanleiding geeft voor strafrechtelijk onderzoek. In dat geval wordt geadviseerd het dossier met doelstelling en plan van aanpak door te sturen naar de (integrale) stuurploeg.

10.2 Verwerkingsgrondslag

Het advies bevat een specifieke doelstelling voor de vervolgactie gebaseerd op een (set van wettelijke) bevoegdheid (-heden). Tevens wordt aangegeven welke partijen de vervolgstappen moeten zetten.

Bij het formuleren van die doelstelling is het niet noodzakelijk om alle opgevraagde en gebruikte persoonsgegevens te delen. Door selectief om te gaan met deze gegevens en het feit dat een doelbinding is geformuleerd, is voldoende basis aanwezig om de persoonsgegevens te delen. Deze gegevens worden immers gedeeld met als doel te besluiten over de aanpak.

11 Uitwerking processtap 6: Beslissen en toewijzen

In overleg tussen partijen wordt bepaald wie de vervolgactie op gaat pakken. Die toewijzing gebeurt op basis van de bevoegdheden die deze partij in gaat zetten. De partij of partijen moeten daarom instemmen met de doelstelling en het feit dat zij met hun bevoegdheden die doelstelling (moeten) kunnen bereiken.

Het besluit wordt gedocumenteerd. Gezien de eerder ingezette bevoegdheden is de burgemeester verantwoordelijk. Op reguliere basis (tweewekelijks) worden de dossiers besproken met de burgemeester. Dossiers die vragen om een integrale aanpak worden altijd inhoudelijk afgestemd met de burgemeester. Deze kan vanuit zijn verantwoordelijkheden (onder andere vanuit zijn gezagsrol naar de politie) dossiers begeleiden naar de (integrale) stuurploegen op lokaal, districtelijk of regionaal niveau.

Afhankelijk van de bevoegdheden van de afhandelende partij worden de eerder gebruikte gegevens uit signaal, signaal en analyse of alleen de doelstelling overgedragen of volgt een aangepaste verstrekking. Denk in dat laatste geval aan de aanpak door een afdeling binnen de gemeente, die de gegevens die uit hun systemen eerder zijn opgevraagd bij de analyse verstrekt krijgt.

De partij die de vervolgactie oppakt, legt hierover verantwoording af aan de gemeente, zodat opvolging en voortgang bewaakt kunnen worden. Bij voorkeur worden de dossiers die onder handen zijn kort besproken in het besluitvormingsoverleg. Daardoor ontstaat een duurzaam overzicht van het aantal casussen dat onder handen is en de status.

Al deze activiteiten worden bijgehouden in het zaaksysteem in het dossier. Hierdoor kan bij het overleg met de burgemeester te allen tijde een adequaat statusoverzicht van de onderhanden dossiers besproken worden. Ook als het inhoudelijk dossier zelf verwijderd is, blijft de procesinformatie beschikbaar. Daarmee voorkomen we dat we persoonsgegevens onder ons houden waar eigenlijk (alleen) behoefte is aan sturings- en inzicht (management-) informatie.

12 Uitwerking processtap 7: Actie door de partij aan wie het signaal is toegewezen

De partij of partijen aan wie de casus is toegewezen gaat/gaan aan de slag. Zij opereert op basis van zijn of haar eigen bevoegdheden.

De verwerking van de persoonsgegevens vindt plaats door de betreffende partij(-en) binnen haar eigen privacy-regime.

In het geval partijen integraal of multidisciplinair vervolgacties oppakken, dient de doelstelling zodanig geformuleerd te zijn, dat de partijen op basis van die doelstelling gegevens kunnen delen. De RIEC-thema's bieden hier handvatten voor. Door besluitvorming via de districtelijke of regionale stuurgroepen kunnen daarbij zelfs externe private of publieke partners aansluiten, die onder het RIEC-convenant persoonsinformatie mogen uitwisselen.

De gemeente Rheden ontvangt in deze fase alleen procesvoortgangsinformatie over de casus. Daarmee blijft er overzicht op de lopende en afgesloten trajecten binnen de gemeentegrenzen.

13 Uitwerking processtap 8: Evaluatie

Nadat een casus succesvol is afgerond, volgt een evaluatie. Deze evaluatie wordt opgesteld door een gecombineerd team, bestaande uit de adviseur Integrale Veiligheid die het signaal beoordeeld heeft en het team dat de actie uitgevoerd heeft. Hierdoor kan het proces van start tot en met einde besproken worden.

Alle betrokkenen hebben in eerdere fasen toegang gekregen tot de persoonsinformatie die in de casus gebruikt is. Het doel van de evaluatie is om lering te trekken uit het hele proces. Welke elementen van het signaal waren aanleiding om te komen tot aanpak? Welke nieuwe inzichten zijn naar voren gekomen tijdens de actie? Hoe kunnen we nieuwe inzichten vertalen naar de collega's die signalen geven? Welke partijen zijn nog meer betrokken bij de aanpak? Welke effecten heeft de actie gehad? Welke vervolgstappen zijn er nog nodig om het effect van de actie te versterken, denk bijvoorbeeld aan beleidswijzigingen?

Leereffecten worden periodiek besproken in een overleg georganiseerd met gemeentelijk ondermijningsteam, politie en de accountmanager RIEC. Dit lokaal ondermijningsoverleg dient onder meer om leereffecten beschikbaar te stellen aan de regio via het RIEC. Hierbij worden in principe geen persoonsgegevens gebruikt. Het betreft immers een procesevaluatie.

Na evaluatie kan de zaak in het zaaksysteem gesloten worden en na een bewaartermijn van zeven jaar na afsluiting dossier vernietigd.

14 Bijlage: Grondslagen

	Georganiseerde hennepteelt	Mensenhandel en –smokkel	Fraude & misbruik in de vastgoedsector	Witwassen	Milieucriminaliteit	Outlaw Motorclubs	Project Ongebruikelijk Bezit (POB)	Misstanden in de prostitutie	Vrijplaatsen	Zorgfraude	Shisha lounges
	RIEC thema's					Handhavingsknelpunten					
Art 172 gemeentewet – handhaving OOV	X	X	X	X	X	X	X	X	X	X	X
Art 170 lid 2 en 3 BM bevordert de integriteit van de gemeente	X	X	X	X	X	X	X	X	X	X	X
Politiewet artikel 11 – BM gezag over politie	x	x	x	x	x	x	x	x	x	x	X
Politiewet artikel 13 – driehoeksoverleg over lokale prioriteiten en criminaliteitsbestrijding	x	x	x	x	x	x	x	x			
Art 121 gemeentewet – Algemene Plaatselijke Verordening	x	x	x	x	x	x	x	x	x		X
Art 174a gemeentewet – situaties van overlast door criminaliteit rond woningen/ sluitingsbevoegdheid publiek toegankelijke gelegenheden (uit APV)	x	x	x				x	x	x		X
Art 13b Opiumwet – sluiting drugspanden	x			x	x		x		x		x
Wet Bibob – artikel 3 vermoedens van strafbare feiten of witwassen	x	x	x	x	x		x	x	x	x	
Abw hoofdstuk 5 – toezicht en handhavingsbevoegdheden	x	x	x	x	x	x	x	x	x	x	X

	Georganiseerde hennepteelt	Mensenhandel en –smokkel	Fraude & misbruik in de vastgoedsector	Witwassen	Milieucriminaliteit	Outlaw Motorclubs	Project Ongebruikelijk Bezit (POB)	Misstanden in de prostitutie	Vrijplaatsen	Zorgfraude	Shisha lounges
	RIEC thema's					**Handhavingsknelpunten**					
(bestuurlijke/herstel/straffende sancties) – met name informatie over 5:9											
art. 1.4 Wet basisregistratie personen (WBRP)	x	x	x	x	x	x	x	x		x	
art. 26 Paspoortwet		X		X			X	X	X	X	
Participatiewet; art. 67 voor verstrekking aan Belastingdienst									X	X	
artikel 220 t/m 229 Gemeentewet – gemeentelijke belastingen	X	X	X	X	X	X	X	X	X	X	X
Aanbestedingen/ art. 2.86 van de Aanbestedingswet en Wet Bibob art. 1 eerste lid onder c			X	X			X				
Vastgoedtransacties/ Wet Bibob art. 5 en art. 5a			X	X			X				
Wet SUWI artikel 62; verstrekking van UWV aan gemeenten.		X	X	X				X	X	X	
art. 2.1.3. lid 4 Wmo 2015			X	X			X		X	X	
art. 2.9 sub d Jeugdwet				X			X		X	X	
Art 7.4.0 van de Jeugdwet				X			X		X	X	

In het overzicht is een duidelijke samenhang te zien met de Burgemeesters-bevoegheden, die toezien op het beschermen van het collectief en het voorkomen van misstanden:

- Algemene bevoegdheid tot handhaving openbare orde (Gw, Artikel 172)

- Noodbevel (Gw, Artikel 175)
- Noodverordening (Gw, Artikel 176)
- Preventief fouilleren (Gw, Artikel 151b en 174b)
- Cameratoezicht (Gw, Artikel 151c)
- Bestuurlijke ophouding (Gw, Artikel 154a en 176a)
- Bestrijding voetbalvandalisme en ernstige overlast (artikel 172a)
- Bevel aan ouders/verzorgers van 12-minners (Gw, Artikel 172b)
- Toezicht op openbare vermakelijkheden en inrichtingen (Gw, Artikel 174)
- Sluiten woning, Wet Victoria (Gw, Artikel 174a)
- Drank- en horecawet (artikel 20 en 44a)
- Wet herziening kinderbeschermingsmaatregelen en jeugdwet
- Opiumwet – wet Damocles (Artikel 13b)
- Stelsel bewaken en beveiligen
- Wet tijdelijk huisverbod
- Wet openbare manifestaties
- Wet Publieke gezondheid
- Wet bijzondere opnemingen in psychiatrische ziekenhuizen (Wet BOPZ)
- Wet Bibob, nader uitgewerkt in toepassingsgebied in het gemeentelijk Bibobbeleid
- Wet aanpak woonoverlast
- Politiewet 2012, met name artikel 11: Het gezag over de politie in de handhaving van de openbare orde omvat twee elementen:
  1. de daadwerkelijke voorkoming en beëindiging van zich concreet voordoende of dreigende verstoringen van de openbare orde en
  2. de algemene bestuurlijke voorkoming van strafbare feiten, die vorm krijgt in de participatie van de politie in het preventieve veiligheidsbeleid.
- Wet veiligheidsregio's (…. waardoor een ernstige verstoring van de fysieke veiligheid is of dreigt te ontstaan en waarbij een gecoördineerde inzet van diensten en organisaties van verschillende disciplines is vereist om de dreiging weg te nemen of de schadelijke gevolgen te beperken …)
- Algemene plaatselijke verordening

14.1 Thema's Integraal Veiligheidsplan 2017 – 2020 gemeente Rheden

In het Integraal Veiligheidsplan (IVP) zijn de lokale prioriteiten vastgelegd die de basis vormen voor de in de Politiewet artikel 13 vastgelegde bevoegdheden van de burgemeester. Om die bevoegdheden uit te kunnen oefenen dient hij zich door zijn gemeenteambtenaren te laten informeren over eventuele signalen die uit het eigen apparaat naar voren komen.

Algemene doelstelling
Verbetering van leefbaarheid en vermindering van (georganiseerde) criminaliteit waardoor inwoners zich veilig voelen binnen de gemeente Rheden; Er vindt gerichte communicatie plaats naar de inwoners over de problematiek en aanpak op het gebied van veiligheid.

- **Sociale kwaliteit:** Door het activeren van inwoners op (veiligheids-)zaken is in 2020 de participatiegraad verbeterd naar 25%. Hierdoor gaat de sociale kwaliteit (kwaliteit van de sociale netwerken, de betrokkenheid van bewoners, de informele sociale controle) en de veiligheid in de woon- en leefomgeving tot 2020 naar een rapportcijfer van minimaal 7.5.
- **Verminderen jeugdoverlast:** Door de uitvoering van de aanpak problematische jeugdgroepen en de samenwerking met de ketenpartners komt het aantal meldingen jeugdoverlast niet boven de 150 meldingen. De onveiligheidsgevoelens van inwoners over groepen jeugd daalt naar 30%. We investeren in de individuele aanpak door onze zorgpartners te betrekken.
- **Klimaatverandering:** in 2017 is er zicht op het effect van klimaatverandering op het risico van (natuur)rampen en ontwikkelen hiervoor plannen en protocollen.
- **Rampen en Crisis:** in 2017 is de organisatie voorbereid op een ramp. In 2018 is dit 'going concern'.
- **Aanpak georganiseerde criminaliteit:** We blijven zicht houden op de ondermijning in onze gemeente en bestrijden deze door een integrale aanpak, het vergroten van bewustwording en normbesef. Hierdoor herstelt het vertrouwen in de overheid.
- **Polarisatie en Radicalisering:** Polarisatie en radicalisering binnen onze gemeente zo veel mogelijk terugdringen door te investeren in integratie en onze samenwerkingspartners toe te rusten op vroeg-signalering en handelingsplan.

Hier onder een opsomming per veiligheidsveld van de huidige aanpak.
1. Veilige woon- en leefomgeving:
   - Ik buurt mee!
   - Meldpunt Openbare Ruimte (MOR) voor diverse vormen van overlast
   - Ondersteuning Buurtpreventieteams/ Whatsapp groepen
   - Inzet Burgernet
   - Inzet buurtbemiddeling
   - Integrale Aanpak structurele overlastsituaties (6-stappen aanpak) (participatie veiligheid)
   - Inzet van krachtcoaches
   - Aanpak Huiselijk Geweld en kindermishandeling
   - Veiligheidshuis
   - Gebiedsteams Leefomgeving:
   - Sociale Gebiedsteams
   - Aanpak jaarwisseling
   - Onderhoud openbaar gebied

2. Bedrijvigheid en Veiligheid
   - Aanpak woninginbraken en voertuigcriminaliteit
   - Toezicht en Handhaving 2.0
   - Inzet straatcoaches
   - Stop heling/ Digitaal opkopingsregister (DOR)/ woninginbraken

- Huisverbod
- Keurmerk Veilig Ondernemen (KVO)
- Jaarlijkse bijeenkomst 'laat je niet overvallen'
- Evenementenbeleid

3. Jeugd en Veiligheid
- Aanpak Jongerenoverlast gemeente Rheden
- Subsidiëring van Halt
- Project perspectief 16+
- Drank en Horecawet 2013
- Week van Respect
- Meldpunt discriminatie en pesten

4. Fysieke Veiligheid
- Gemeentelijke verkeersveiligheidsplannen
- Volgen van Duurzaam veilig
- ROV Oost Nederland/ CROW
- Project TOOM
- Voorlichting na brand
- Regionale projecten op de kwetsbare groepen (ouderen) en brandveiligheid
- Notitie externe veiligheid
- Provinciale Risicokaart (risicokaart.nl)
- Landelijke visie natuurbrandbeheersing
- Regionaal Beleidsplan rampenbestrijding en crisisbeheersing 2016-2019
- Regionaal Crisisplan Gelderland-Midden deel 1&2

Integriteit en Veiligheid
- Repressieve aanpak radicalisering
- Meldpunt discriminatie en pesten
- Week van Respect
- Samenwerking met RIEC (Regionaal Informatie- en Expertisecentrum) en landelijk Bureau BIBOB
- Ondermijningsanalyse
- Hennepconvenant Regio Oost-Nederland
- Beleidsregels artikel 13b Opiumwet
- Aanpak mensenhandel/ arbeidsuitbuiting (RIEC/ Veiligheidshuis)
- Melden Agressie-incidenten (GIR)
- Agressie Interventie Team (AIT);
- Beleidsnotitie Agressie en geweld
- Uitvoering beleidsnotitie agressie en geweld
- Melden Datalekken
- Bewustwording informatiebeveiliging
- Informatiebeveiligingsplan 2012
- Gedragscode personeel gemeente Rheden

14.2 RIEC thema's

In het Regionaal Informatie en Expertise Centrum werken verschillende partners, waaronder de gemeente Rheden, samen op specifiek benoemde thema's. Voor Oost Nederland zijn dit:

- Georganiseerde hennepteelt
- Mensenhandel en –smokkel
- Fraude & misbruik in de vastgoedsector
- Witwassen
- Milieucriminaliteit

Door de Regionale Stuurgroep RIEC benoemde handhavingsknelpunten, als bedoeld in artikel 1.7 en artikel 2.3 van het RIEC-convenant:

- Outlaw Motorclubs
- Project Ongebruikelijk Bezit (POB)
- Misstanden in de prostitutie
- Vrijplaatsen
- Zorgfraude
- Shisha lounges

RIEC overlegmodel