

## Protocol fenomeen, netwerk- en signaalanalyses inzake de aanpak radicalisering, extremisme en polarisatie

### Samenvatting

Gemeenten zijn verantwoordelijk voor de lokale integrale aanpak van radicalisering, extremisme en polarisatie. De gemeenten Delft, Midden-Delfland, Rijswijk en Westland (district E) kennen hierin een gezamenlijke aanpak, die gecoördineerd wordt door de gemeente Delft. In het kader van deze aanpak voeren de gemeenten fenomeen, netwerk- en signaalanalyses uit middels legale, openbare en publiek toegankelijke bronnen ('Open Source Intelligence', OSINT). De analyses worden uitgevoerd op fenomenen, netwerken en signalen die een risico op radicalisering, extremisme, polarisatie en/of maatschappelijke onrust met zich meebrengen en hierdoor een verstoring van de openbare orde kunnen veroorzaken.<sup>1</sup> Door het uitvoeren van fenomeen, netwerk- en signaalanalyses wordt de gemeentelijke informatiepositie m.b.t. radicalisering, extremisme en polarisatie versterkt, waardoor de openbare orde effectiever kan worden gehandhaafd. Daarnaast kan hierdoor worden bezien met welke kwetsbaarheden, maar ook met welke mate van weerbaarheid de gemeenten rekening moeten houden.

Dit protocol biedt een leidraad en grondslag voor het uitvoeren van fenomeen, netwerk- en signaalanalyses middels OSINT in het kader van de aanpak radicalisering, extremisme en polarisatie. Voor het goed kunnen uitvoeren van dergelijke analyses wordt het werkproces met dit protocol nader toegelicht. Er wordt nadrukkelijk stilgestaan bij het doel en belang van de fenomeen, netwerk- en signaalanalyses, de stappen in het proces, de wettelijke grondslag hiervan en de ingebouwde waarborgen in het proces.

### 1. Inleiding

#### 1.1 Achtergrond

Gemeenten zijn verantwoordelijk voor de veiligheid en het welzijn van hun inwoners. Radicalisering, extremisme en polarisatie<sup>2</sup> kunnen een serieuze bedreiging vormen voor de veiligheid van de inwoners van de gemeente. Zij kunnen bovendien de democratische rechtstaat ernstig ondermijnen. De afgelopen jaren is de maatschappij geconfronteerd met diverse vormen van extremisme. Denk hierbij o.a. aan het gewelddadig jihadisme, rechtsextremisme en het anti-institutioneel extremisme. Daarnaast is er een verscherping van tegenstellingen in de samenleving te zien en lijkt de afstand van diverse groepen tot de overheid groter te worden.<sup>3</sup> Radicalisering, extremisme en polarisatie zijn fenomenen die, gezien het potentiële ingrijpende karakter ervan, vragen om een blijvende inzet. Als regiehouder heeft de gemeente een cruciale rol bij de aanpak van deze problematiek. Het is daarom belangrijk dat gemeenten effectieve processen hebben ingericht die zien op signalering, preventie, repressie en nazorg.

De gemeenten Delft, Midden-Delfland, Rijswijk en Westland (district E) kennen een gezamenlijke aanpak van radicalisering, extremisme en polarisatie. Deze aanpak wordt gecoördineerd door de gemeente Delft en is vastgelegd in het document *Aanpak extremisme, polarisatie en radicalisering*. Het doel van de aanpak voor het district is om de gemeenten 'weerbaar te maken en houden tegen extremisme, polarisatie en radicalisering, om dit actief tegen te gaan en adequaat in te grijpen als maatschappelijke spanningen ontstaan of personen afglijden'.<sup>4</sup> Dit protocol ziet op het uitvoeren van fenomeen, netwerk- en signaalanalyses middels legale, openbare en publiek toegankelijke bronnen (OSINT<sup>5</sup>) in het kader van de aanpak radicalisering, extremisme en polarisatie. De analyses worden uitgevoerd op fenomenen, netwerken en signalen die een risico op radicalisering, extremisme, polarisatie en/of maatschappelijke onrust met zich meebrengen en hierdoor aanleiding kunnen geven tot een verstoring van de openbare orde.

Met het uitvoeren van dergelijke analyses wordt bijgedragen aan het realiseren van het algehele doel van de aanpak voor district E (zoals hierboven geformuleerd). De gemeentelijke informatiepositie inzake de aanpak wordt hiermee namelijk versterkt, waardoor de openbare orde effectiever kan worden gehandhaafd. Er kan bekeken worden in hoeverre er sprake is van maatschappelijke spanningen of ongewenste polarisatie en welk handelingsperspectief effectief zou kunnen zijn om mogelijke ordeverstoringen

1) Het gaat hierbij enkel om fenomenen, netwerken en signalen. Er worden geen analyses uitgevoerd op specifieke individuen.

2) Voor een uitleg van deze drie begrippen, zie: Bijlage 1: Begrippenlijst.

3) *Aanpak extremisme, polarisatie en radicalisering: Delft, Midden-Delfland, Rijswijk en Westland*, blz. 1.

4) *Aanpak extremisme, polarisatie en radicalisering: Delft, Midden-Delfland, Rijswijk en Westland*, blz. 5.

5) Voor een uitleg van dit begrip, zie: Bijlage 1: Begrippenlijst.

te voorkomen. Daarnaast kan hiermee effectiever worden gezien met welke kwetsbaarheden en mate van weerbaarheid<sup>6</sup> de gemeenten rekening moeten houden.

### 1.2 Doel en reikwijdte protocol

Het doel van dit protocol is om een leidraad en grondslag te bieden voor het uitvoeren van fenomeen, netwerk- en signaalanalyses middels OSINT in het kader van de aanpak radicalisering, extremisme en polarisatie voor district E. Zoals eerder vermeld wordt met dergelijke analyses beoogd om de informatiepositie van de gemeenten m.b.t. het onderwerp te versterken, om zo de openbare orde goed te kunnen handhaven. Er wordt in dit protocol o.a. inzicht gegeven in de definities van fenomenen, netwerken en signalen, het proces van fenomeen, netwerk- en signaalanalyses, de wettelijke kaders waarin geopereerd wordt en de waarborgen ingebouwd in het proces.

Belangrijk om te vermelden is dat de OSINT-analyses ten behoeve van de aanpak radicalisering, extremisme en polarisatie uitsluitend gericht zijn op algemene fenomenen, netwerken en signalen. Er worden in dit kader dus geen zoekopdrachten en analyses uitgevoerd op specifieke individuen. Het uitvoeren van persoonsgerichte analyses valt uitdrukkelijk buiten de reikwijdte van dit protocol. Een belangrijke kanttekening hierbij is echter dat niet volledig uitgesloten kan worden dat er tijdens de fenomeen, netwerk- en signaalanalyses in sommige gevallen toch persoonsgegevens worden verwerkt.<sup>7</sup> De verwerking van deze persoonsgegevens is onderhevig aan de Algemene Verordening gegevensbescherming (AVG), de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) en specifieke privacy wet- en regelgeving. Beginselen als verwerkingsgrondslag, doelbinding, transparantie en noodzakelijkheid van de gegevensverwerking vormen hierbij belangrijke uitgangspunten.

De aanpak extremisme, polarisatie en radicalisering voor district E kent vier actielijnen, inhoudende preventieve en repressieve activiteiten en maatregelen.<sup>8</sup> De fenomeen, netwerk- en signaalanalyses waarop dit protocol ziet zijn preventieve activiteiten die worden ingezet in het kader van het vergroten van de weerbaarheid (actielijn 2).<sup>9</sup> De overige actielijnen vallen niet binnen de reikwijdte van dit protocol. Het delen van gegevens met anderen gemeenten ten behoeve van een integrale aanpak radicalisering, extremisme en polarisatie is tevens geen onderdeel van dit protocol. Dit wordt nader uitgekristalliseerd in het conceptvoorstel voor de 'Wet persoonsgerichte aanpak en meldingen radicalisering en terroristische activiteiten' en de 'Wet gegevensverwerking door samenwerkingsverbanden'.

### 1.3 Aanpassen van protocol

Dit protocol is een levend document. Het protocol wordt jaarlijks geëvalueerd door de gemeente Delft, waarbij wordt gezien of in de praktijk conform het protocol wordt gehandeld. Daarnaast wordt jaarlijks beoordeeld of het protocol en de bijlagen aanpassing behoeven n.a.v. bijvoorbeeld veranderde inzichten rondom de aanpak radicalisering, extremisme en polarisatie en/of na een wijziging in relevante wet- en regelgeving. Er wordt nadrukkelijk gekeken wat de gevolgen van die veranderingen zijn voor de bescherming van persoonsgegevens.

### 1.4 Leeswijzer

In hoofdstuk 2 worden de fenomeen, netwerk- en signaalanalyses middels OSINT nader beschreven. Hier wordt allereerst nadrukkelijk stilgestaan bij de definities van de begrippen. Daarna volgt een methodiekbeschrijving. Vervolgens gaat hoofdstuk 3 in op de wettelijke grondslag voor het uitvoeren van de fenomeen, netwerk- en signaalanalyses. Hierbij wordt tevens stilgestaan bij de bewaartermijnen van gegevens, de genomen beveiligingsmaatregelen, de rechten van betrokkenen en informatievoorziening. Tenslotte is in bijlage 1 een begrippenlijst opgenomen.

## 2. Fenomeen, netwerk- en signaalanalyses

### 2.1 Definities

In het kader van de aanpak radicalisering, extremisme en polarisatie worden er via legale, openbare en publiek toegankelijke bronnen analyses uitgevoerd op fenomenen, netwerken en signalen in de gemeenten die, door een risico op radicalisering, extremisme, polarisatie en/of maatschappelijke onrust, aanleiding kunnen geven tot een verstoring van de openbare orde. Ter illustratie volgen hieronder de

6) Voor een uitleg van dit begrip in het kader van dit protocol, zie: Bijlage 1: Begrippenlijst.

7) Ter illustratie: het kan bijvoorbeeld zo zijn dat tijdens een OSINT-analyse o.a. een naam, woonplaats of leeftijd van een individu wordt gezien.

8) De vier actielijnen conform de *Aanpak extremisme, polarisatie en radicalisering: Delft, Midden-Delfland, Rijswijk en Westland* betreffen: 1) Verminderen maatschappelijke onrust en ongewenste polarisatie, 2) Vergroten weerbaarheid; 3) Bevorderen deskundigheid, 4) Persoonsgerichte aanpak.

9) Voor een uitleg van dit begrip in het kader van dit protocol, zie: Bijlage 1: Begrippenlijst.

definities van de begrippen inclusief concrete voorbeelden van situaties waarop een fenomeen-, netwerk- of signaalanalyse kan worden uitgevoerd.

**Fenomenen**

Fenomenen richten zich op sociale bewegingen en ontwikkelingen die aanleiding kunnen geven tot een verstoring van de openbare orde door het risico op radicalisering, extremisme, polarisatie en/of maatschappelijke onrust.

**Voorbeeld:** ontwikkelingen rondom (inter)nationale verkiezingen kunnen aanleiding zijn voor maatschappelijke onrust en/of verstoringen van de openbare orde.

**Netwerken**

Netwerken omvatten specifieke groepen die aanleiding kunnen geven tot een verstoring van de openbare orde door het risico op radicalisering, extremisme, polarisatie en/of maatschappelijke onrust.

**Voorbeeld:** links- of rechtsextremistische groepen.

**Signalen**

Specifieke signalen die aanleiding kunnen geven tot een verstoring van de openbare orde door het risico op radicalisering, extremisme, polarisatie en/of maatschappelijke onrust.

**Voorbeeld:** het Project X feest in 2012 in Haren. Lokaal voorbeeld: avondklokrellen tijdens COVID-19.

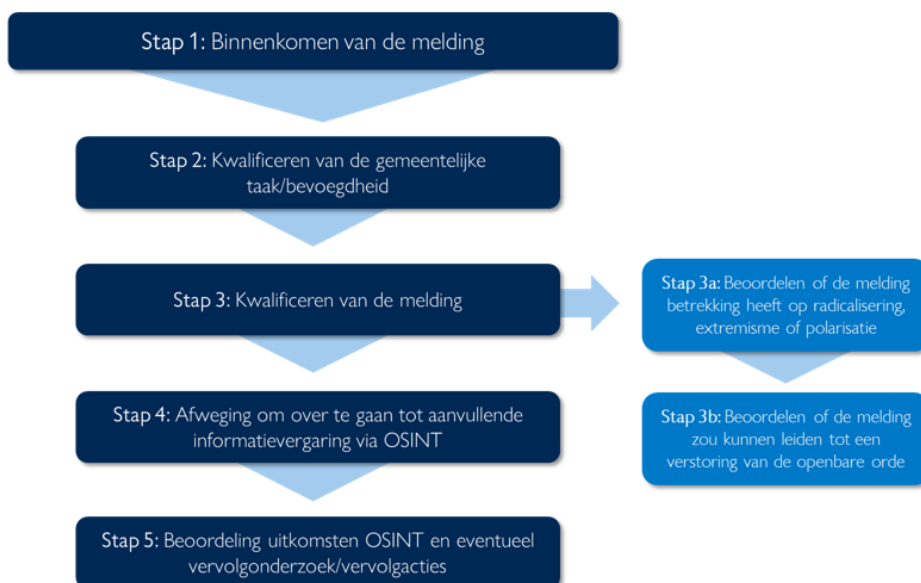
**2.2 Het proces van fenomeen-, netwerk- en signaalanalyses**

Hieronder wordt het proces van fenomeen-, netwerk- en signaalanalyses in het kader van de aanpak radicalisering, extremisme en polarisatie stapsgewijs nader uitgewerkt. Dit proces bestaat uit vijf stappen. Deze stapsgewijze aanpak kent verschillende proces- en rechtmatigheidswaarborgen. Deze waarborgen zijn ingebouwd om te garanderen dat gehandeld wordt op een wijze die in lijn is met de AVG, de UAVG en met de sectorale wetgeving. Daarnaast wordt met deze waarborgen voorkomen dat gegevens worden verwerkt die niet noodzakelijk zijn. De vijf stappen in het proces van fenomeen-, netwerk- en signaalanalyses zijn:

1. Binnenkomen van de melding;
2. Kwalificeren van de gemeentelijke taak/bevoegdheid;
3. Kwalificeren van de melding;
  - a. Beoordelen of de melding betrekking heeft op radicalisering, extremisme of polarisatie
  - b. Beoordelen of de melding zou kunnen leiden tot een verstoring van de openbare orde
4. Afweging om over te gaan tot aanvullende informatievergaring via OSINT;
5. Beoordeling uitkomsten OSINT en eventueel vervolgonderzoek/vervolgacties.

Bovenstaande stappen zijn visueel weergegeven in de onderstaande figuur.

Stappenplan fenomeen-, netwerk- en signaalanalyses



*Figuur 1: Weergave stappen tijdens de fenomeen-, netwerk- en signaalanalyses.*

### Stap 1: Binnenkomen van de melding

Het proces start naar aanleiding van een melding omtrent een fenomeen, netwerk of signaal dat mogelijk ziet op radicalisering, extremisme of polarisatie en mogelijk aanleiding kan geven tot een verstoring van de openbare orde. Deze melding kan bijvoorbeeld worden gedaan door een collega, burger of aandachtsfunctionaris.<sup>10</sup> Er kunnen daarnaast ook meldingen binnenkomen via andere routes, zoals door de politie of een samenwerkingsverband. Het proces kan tevens starten n.a.v. bijvoorbeeld een incident bij een andere gemeente of een nieuwsbericht (in het kader van dit protocol kwalificeren voornoemde gevallen tevens als 'melding'). Zoals eerder vermeld is dit protocol beperkt tot meldingen omtrent fenomenen, netwerken en signalen en ziet niet op meldingen over individuen.

Meldingen worden meestal telefonisch, mondeling of per e-mail gedaan bij de experts van de afdeling Veiligheid Advies<sup>11</sup> van de gemeente Delft. De meldingen worden genoteerd in het gehanteerde meldformulier en opgeslagen in een vertrouwelijke map op de beveiligde server van de gemeente Delft. Enkel de medewerkers die zich bezighouden met radicalisering, extremisme en polarisatie hebben toegang tot deze map. Er wordt na ontvangst van de melding een korte terugkoppeling gegeven aan de melder, dat de melding ontvangen is en dat ernaar gekeken wordt. Bij meldingen rondom zwaarwegende mogelijke maatschappelijke onrust wordt, indien van toepassing, vermeld dat de melding wordt doorgegeven aan de politie. In het meldformulier waarin de melding wordt opgeslagen, worden geen persoonsgegevens van de melder of andere personen vermeld. Indien de melding schriftelijk (bijvoorbeeld per e-mail of telefoon) is gedaan, wordt deze binnen twee weken verwijderd. Het meldformulier wordt tevens binnen twee weken verwijderd.

### Stap 2: Kwalificeren van de gemeentelijke taak/bevoegdheid

De melding wordt na ontvangst en vastlegging in het meldformulier beoordeeld door de experts van de afdeling Veiligheid Advies. Allereerst wordt door de experts van de afdeling Veiligheid Advies bekeken of de binnengekomen melding betrekking heeft op een taak of bevoegdheid van de gemeente, of op een taak of bevoegdheid van een andere instantie (bijvoorbeeld van de politie). Een dergelijke gemeentelijke taak is bijvoorbeeld een van de openbare orde-bevoegdheden van de burgemeester. Het is hierbij dus van belang na te gaan of de melding in beginsel tot gemeentelijk optreden zou moeten leiden. Wanneer de melding geen aanleiding kan vormen voor de inzet van een gemeentelijke taak of bevoegdheid, wordt de melding niet in behandeling genomen door de gemeente en wordt de melder, indien nodig, doorverwezen naar de bevoegde instantie. Wanneer de melding wél aanleiding kan vormen voor inzet van een gemeentelijke taak of bevoegdheid, wordt overgegaan naar stap 3.

### Stap 3: Kwalificeren van de melding

Bij deze stap wordt beoordeeld of de melding te maken heeft met het onderwerp radicalisering, extremisme of polarisatie én of de melding mogelijk zou kunnen leiden tot een verstoring van de openbare orde of voor maatschappelijke onrust kan zorgen. Deze stap in het proces bestaat daarom uit twee onderdelen. Deze worden hieronder nader gespecificeerd.

#### Stap 3a: Beoordelen of de melding betrekking heeft op radicalisering, extremisme of polarisatie

Er wordt naar de aard en inhoud van de melding gekeken en of de melding betrekking heeft op het onderwerp radicalisering, extremisme of polarisatie. Hierbij worden o.a. gelet op de volgende vragen:

- Is de melding voldoende concreet?
- Worden er in de melding persoonsgegevens vermeld?
- Heeft de melding te maken met radicalisering, extremisme of polarisatie?

Indien de melding onvoldoende concreet is, kan aan de melder worden gevraagd om een nadere toelichting op de melding te geven. Indien beoordeeld wordt dat de melding betrekking heeft op een persoon of geen betrekking heeft op het onderwerp radicalisering, extremisme of polarisatie, wordt niet overgegaan naar de volgende stappen in het proces. Indien dit noodzakelijk wordt geacht, wordt wel aan de melder teruggekoppeld wat de daarvoor bestemde instantie of processen/afdeling binnen de gemeente zijn waar de desbetreffende melding gedaan kan worden. Indien de melding wél betrekking heeft op het onderwerp radicalisering, extremisme of polarisatie én gericht is op een fenomeen, netwerk of signaal, wordt overgegaan naar stap 3b.

#### Stap 3b: Beoordelen of de melding zou kunnen leiden tot een verstoring van de openbare orde

10) De gemeente Delft heeft, samen met de districtsgemeenten Midden-Delfland, Rijswijk en Westland, ongeveer 150 personen op sleutelposities opgeleid tot aandachtsfunctionaris. Deze personen zijn getraind in het herkennen van signalen die duiden op radicalisering, extremisme of polarisatie.

11) Met experts van de afdeling Veiligheid Advies wordt in het kader van dit protocol bedoeld de procesregisseur of netwerkregisseur werkzaam in dit vakgebied.

Bij deze stap wordt beoordeeld of de melding zou kunnen zorgen voor een verstoring van de openbare orde of tot maatschappelijke onrust kan leiden. Bij het beoordelen hiervan wordt o.a. gelet op de volgende vragen:

- Zou de melding maatschappelijke onrust kunnen opleveren en in welke mate?
- Zou de rechtsorde in het geding kunnen komen door de mogelijke gevolgen van deze melding?
- Zijn er kwetsbare groepen of personen die in negatieve mate beïnvloed kunnen worden?

Indien wordt beoordeeld dat de melding niet kan leiden tot een verstoring van de openbare orde of niet kan zorgen voor maatschappelijke onrust, wordt de melding afgesloten. Indien nodig wordt de melding wel doorgezet naar de daarvoor bestemde processen/afdeling binnen de gemeente of naar de in dat geval relevante instantie. Indien er wél een risico op verstoring van de openbare orde of op maatschappelijke onrust is, wordt overgegaan naar stap 4.

#### **Stap 4: Afweging om over te gaan tot aanvullende informatievergaring via OSINT**

In deze stap wordt de zwaarte van de melding door de experts van de afdeling Veiligheid Advies afgewogen. Naar aanleiding hiervan wordt beoordeeld of er nadere informatie over de melding opgehaald dient te worden via legale, openbare en publiek toegankelijke bronnen (OSINT). Er wordt allereerst beoordeeld of de zwaarte van de melding het overgaan tot OSINT rechtvaardigt. Er moet tevens een onderbouwd vermoeden zijn dat er op openbare bronnen nadere informatie over de melding te vinden is waarmee de melding beter geduid kan worden. Ook wordt afgewogen of het uitvoeren van nader onderzoek op openbare bronnen bij kan dragen aan het identificeren van de kwetsbaarheden en het vergroten van de weerbaarheid m.b.t. radicalisering, extremisme en polarisatie in de gemeente.

Als op basis van de bovenstaande weging beslist wordt dat een analyse middels OSINT benodigd is en aanvullende, gewichtige informatie kan opleveren, wordt de melding bekeken via legale, openbare en publiek toegankelijke bronnen. Hierbij kan gedacht worden aan bijvoorbeeld Google of YouTube. Er wordt, indien van toepassing, via een algemeen account onder naam van de gemeente Delft (dus niet via een schuilnaam) gebruikgemaakt van publiek toegankelijke sociale media platforms zoals Facebook, Instagram en Twitter.<sup>12</sup>

Zoals eerder vermeld richt deze analyse zich enkel op fenomenen, netwerken of signalen die kunnen leiden tot een verstoring van de openbare orde. Deze analyse richt zich nooit op individuen. Indien er analyses worden uitgevoerd via sociale media, wordt er enkel naar openbare groepen gekeken. Er wordt dus niet op individuele profielen geklikt, er vindt geen interactie met andere gebruikers plaats en er is geen sprake van lidmaatschap van groepen en/of pagina's. Er wordt ook niet in kaart gebracht welke personen lid van bepaalde netwerken/groepen zijn. Belangrijk om te vermelden is daarnaast dat er slechts voor een beperkte periode, uiterlijk een aantal weken, naar het signaal gekeken wordt. Er wordt enkel gekeken naar actuele informatie, en niet naar historische informatie.

Indien er relevante informatie via openbare bronnen te vinden is, kan ervoor gekozen worden om een rapport met de bevindingen van de OSINT-analyse op te stellen. Dit hoeft echter niet altijd het geval te zijn. In het eventueel opgestelde rapport staan geen persoonsgegevens opgeslagen. De opgeslagen informatie is daarom niet herleidbaar naar een persoon. Het rapport wordt opgeslagen in een vertrouwelijke map op de beveiligde server van de gemeente Delft. Enkel de medewerkers die zich bezighouden met radicalisering, extremisme en polarisatie hebben toegang tot deze map en kunnen dit rapport inzien.

Indien er geen relevante aanvullende informatie omtrent de melding voorkomt in legale, openbare en publiek toegankelijke bronnen, wordt de melding in het kader van dit protocol niet verder in behandeling genomen. Als de inhoud en zwaarte van de melding dit rechtvaardigen worden er mogelijk wel vervolgstappen gezet, dit valt echter buiten de reikwijdte van dit protocol. Indien er geen vervolgstappen nodig zijn, wordt de melding afgesloten.<sup>13</sup> Indien omtrent een melding wél relevante informatie in legale, openbare en publiek toegankelijke bronnen voorkomt, wordt overgegaan naar stap 5.

#### **Stap 5: Beoordeling uitkomsten OSINT en eventueel vervolgonderzoek/vervolgacties**

In deze stap beoordelen de experts van de afdeling Veiligheid Advies de uitkomsten van de OSINT-analyse van de melding. Zij beoordelen of de bevindingen middels OSINT de melding in voldoende mate bevestigen én of de aard en zwaarte van de melding het continueren van het onderzoek en/of de eventuele inzet van vervolgacties rechtvaardigen. Hulpmiddelen bij het beoordelen hiervan zijn o.a. de volgende documenten: *Aanpak extremisme, polarisatie en radicalisering: Delft, Midden-Delfland, Rijswijk en Westland* en landelijke kaders zoals de Nationale Contraterrorisme Strategie (2022-2026) en het

<sup>12</sup>FG Rapport november 2021.pdf, blz.17.

<sup>13</sup>Voor de gehanteerde bewaartermijnen van de meldingen, zie pg. 12.



meest recente Dreigingsbeeld, de laatste allebei afkomstig van de NCTV. De beoordeling onder stap vijf van het proces kan de volgende uitkomsten hebben:

- De melding behoeft geen vervolgonderzoek of vervolgacties en wordt hierdoor niet verder in behandeling genomen;
- De melding behoeft wel vervolgonderzoek en/of vervolgacties en wordt naar een gemeentelijk onderdeel gestuurd dat de regie vervolgens voert;<sup>14</sup>
- De melding behoeft wel vervolgonderzoek en/of vervolgacties en wordt naar de politie gestuurd die de regie vervolgens voert.<sup>15</sup>

### 3. Wettelijke basis en waarborgen

#### 3.1 Wettelijke basis fenomeen-, netwerk- en signaalanalyses

De wettelijke basis voor het gebruik van OSINT in het kader van de handhaving van de openbare orde is artikel 172 lid 1 van de Gemeentewet. Zoals eerder vermeld zijn de analyses die uitgevoerd worden niet gericht op individuen, maar op fenomenen, netwerken en signalen. Alhoewel bij deze analyses persoonsgegevens verwerkt kunnen worden, wordt er niet ingezoomd op specifieke personen. Er wordt dan ook niet geprobeerd om aliassen te achterhalen of om bepaalde individuen aan elkaar te koppelen. Er wordt ook niet in kaart gebracht welke personen lid van bepaalde netwerken/groepen zijn. Ook is er geen sprake van het stelselmatig volgen van personen. Zo zal er bij het uitvoeren van een netwerkanalyse nooit ingezoomd worden op de deelnemers van het netwerk, maar wel op de eigenschappen van het netwerk zelf. Doordat de analyses niet ingaan op personen en als doel hebben om mogelijke verstoring van de openbare orde preventief te signaleren en te voorkomen, zijn de analyses in het kader van dit protocol in lijn met artikel 172 van de Gemeentewet.<sup>16</sup> De wettelijke grondslag voor het verwerken van persoonsgegevens is artikel 6 lid 1 sub e van de AVG.<sup>17</sup> Hierbij wordt opgemerkt dat het aanpakken van radicalisering, extremisme en polarisatie wordt beschouwd als een zwaarwegende taak met potentieel ontwrichtende gevolgen voor de samenleving.

Naast bovengenoemd wettelijk kader wordt het onderzoek naar fenomenen, netwerken en signalen tevens gezien als onderdeel van de nationale aanpak van terrorisme en extremisme. De wettelijke basis voor het gebruik van OSINT kan in de toekomst worden uitgebreid met de inwerkingtreding van de Wet Gegevensdeling door Samenwerkingsverbanden. Dit wetsvoorstel biedt een juridische basis voor het verwerken van persoonsgegevens door samenwerkingsverbanden. Onder 'samenwerkingsverbanden' verstaat men bestuursorganen en private partijen die gezamenlijk gegevens verwerken voor zwaarwegende algemene belangen. Het wetsvoorstel is aangenomen door de Tweede Kamer en wacht nu op goedkeuring door de Eerste Kamer.

#### 3.2 Doeleinde verwerking persoonsgegevens

Het doeleinde van de verwerking van persoonsgegevens is het analyseren van fenomenen, netwerken en signalen die inzicht kunnen geven in radicaliserende, extremistische en polariserende trends in de gemeente. Hiermee wil de gemeente de risico's voor de maatschappij die uitgaan van radicalisering, extremisme en polarisatie reduceren, met als doel het in stand houden van de leefbaarheid in de gemeente en de handhaving van de openbare orde. Dit doeleinde is afgewogen tegen de privacybelangen van de burger. In deze afweging is de voornaamste overweging dat de zwaarte van de inbreuk op de privacy- en gegevensbeschermingsrechten van de betrokkenen beperkt blijft, omdat er, ondanks dat er persoonsgegevens verwerkt kunnen worden, nooit wordt ingezoomd op specifieke personen. De verwerking beperkt zich tot een generieke uitwerking van signalen, fenomenen of netwerken. Mochten er in de OSINT-analyse persoonsgegevens verwerkt worden, dan zullen deze niet worden opgeslagen. De persoonsgegevens die eventueel in een melding voorkomen, kunnen enkel verder worden verwerkt (bijv. doorgezet worden) indien dit verenigbaar is met het doeleinde waarvoor de gegevens aanvankelijk zijn verzameld.

#### 3.3 Waarborgen in de verschillende fasen van het proces

##### 3.2.1 Bewaartermijnen

De oorspronkelijk binnengekomen melding, inhoudende eventuele persoonsgegevens van de melder van het signaal, wordt uiterlijk binnen twee weken verwijderd. In het meldformulier, waarin de melding

<sup>14</sup> Hierbij geldt dat enkel de melding wordt doorgezet, niet het eventueel opgestelde rapport met de bevindingen uit de OSINT-analyse.

<sup>15</sup> Ook hierbij geldt dat enkel de melding wordt doorgezet, niet het eventueel opgestelde rapport met de bevindingen uit de OSINT-analyse.

<sup>16</sup> FG Rapport november 2021.pdf, blz.18.

<sup>17</sup> Artikel 6 lid 1 sub E AVG luidt: "De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen".

wordt geregistreerd, worden geen persoonsgegevens van de melder of andere personen opgeslagen. Het meldformulier wordt tevens uiterlijk binnen twee weken verwijderd. Zoals eerder vermeld kan het zijn dat tijdens de fenomeen, netwerk- en signaalanalyses middels OSINT persoonsgegevens worden verwerkt (in de zin dat er bijvoorbeeld persoonsgegevens gezien worden). Deze persoonsgegevens worden echter nooit opgeslagen en dus niet bewaard.

### 3.2.2 Beveiligingsmaatregelen meldingen

De binnengekomen melding wordt opgeslagen middels een meldformulier. Er worden geen persoonsgegevens opgeslagen tijdens het onderzoeken van het signaal. De eventueel op te stellen rapporten n.a.v. de OSINT-analyses zijn dus volledig anoniem. Ter beveiliging van de gegevens van de melding en het rapport tegen onrechtmatige verkrijging en onjuist gebruik, worden de volgende beveiligingsmaatregelen genomen:

- De meldingen en de eventuele daaruit voortvloeiende rapporten n.a.v. de OSINT-analyses worden opgeslagen in een vertrouwelijke map op de beveiligde server van de gemeente Delft. De opgeslagen informatie wordt beveiligd conform de beveiligingsnormen van de gemeente Delft<sup>18</sup>;
- Toegang tot de opgeslagen informatie wordt beperkt tot een gelimiteerd aantal personen, enkel de medewerkers die zich bezighouden met radicalisering, extremisme en polarisatie hebben hiertoe toegang.

### 3.2.3 Rechten van betrokkenen

Betrokkenen hebben het recht te verzoeken om inzage in de persoonsgegevens die ten aanzien van hen worden verwerkt (artikel 15 van de AVG). Desgewenst kunnen zij verzoeken om rectificatie, het wissen of beperken van die verwerking (artikel 16, 17 en 18 van de AVG). De uitzonderingen van artikel 23 van de AVG en artikel 41 van de UAVG kunnen aan toewijzing van de verzoeken in de weg staan. Belangrijk om hierbij te vermelden is dat er in de meldformulieren en tijdens de OSINT-analyses geen persoonsgegevens worden opgeslagen.

Indien een betrokkene gebruik wil maken van zijn recht op inzage, rectificatie, het wissen of beperken, wordt er verwezen naar de hiervoor ingerichte **procedure** van de gemeente Delft.

### 3.2.4 Informatievoorziening aan de burger

Zoals eerder vermeld zijn de analyses die uitgevoerd worden niet gericht op personen, maar op fenomenen, netwerken en signalen. Indien er persoonsgegevens worden verzameld, moeten betrokkenen hierover worden geïnformeerd (artikel 13 en 14 van de AVG). Dit gebeurt via de online privacyverklaring. Hierin moet in ieder geval de volgende informatie staan:

- Welke gegevens worden verwerkt;
- Waarom de gegevens worden verwerkt (met welk doel);
- Of de gegevens worden gedeeld met andere organisaties en zo ja, welke;
- Hoe lang de gegevens worden bewaard.

Hierbij wordt zo veel mogelijk aansluiting gezocht bij meer generieke uitlatingen over het verwerken van persoonsgegevens door de gemeente Delft, als omschreven in het Gegevensbeschermingsbeleid.

<sup>18</sup>)De beveiligingsnormen van de gemeente Delft zijn te vinden op: <https://www.delft.nl/over-onze-website/verklaring-gegevensbescherming>

## Bijlage 1: Begrippenlijst<sup>19</sup>

**Open Source Intelligence (OSINT):** betreft het verzamelen en analyseren van gegevens die zijn verkregen uit openbare bronnen.

**Radicalisering:** een proces waarbij een persoon of groep in toenemende mate opvattingen ontwikkelt die op gespannen voet staan met, of zelfs haaks staan op, de democratische rechtsorde. Er is een groeiende bereidheid om diepingrijpende veranderingen in de samenleving na te streven of deze te ondersteunen.

**Extremisme:** het actief nastreven en/of ondersteunen van diepingrijpende veranderingen in de samenleving die een gevaar kunnen opleveren voor (het voortbestaan van) de democratische rechtsorde. Hierbij worden eventueel ondemocratische methodes gehanteerd die afbreuk kunnen doen aan het functioneren van de democratische rechtsorde.

**Polarisatie:** de verscherping van tegenstellingen tussen groepen in de samenleving die kan resulteren in spanningen tussen deze groepen en toename van segregatie.

**Weerbaarheid:** het kunnen bieden van tegengewicht en veerkracht tegen ongewenste invloeden en voedingsbodems voor radicalisering.

**Fenomeenanalyse:** analyse die zicht richt op sociale bewegingen en ontwikkelingen die aanleiding kunnen geven tot verstoring van de openbare orde.

**Netwerkanalyse:** analyse die zich richt op bepaalde groeperingen die aanleiding kunnen geven tot verstoring van de openbare orde.

**Signaalanalyse:** analyse die zich richt op signalen die aanleiding kunnen geven tot verstoring van de openbare orde.

**Persoonsgegevens:** alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

**Verwerken van persoonsgegevens:** alles wat een organisatie met persoonsgegevens kan doen, o.a. inzien, verzamelen en vernietigen.

**Doelbinding:** het vereiste dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verwerkt.

---

<sup>19</sup> De definities die worden gehanteerd zijn o.a. afkomstig van de AIVD, de NCTV en Verdonck, Klooster & Associates en naar eigen inzicht (gedeeltelijk) aangepast.