Handreiking

Signalerend openbronnenonderzoek in de gemeentelijke openbare ordepraktijk

18-2-2026

THORBECKE ACADEMIE
NHL STENDEN

HOOGHIEMSTRA & PARTNERS
strategisch en juridisch advies

pro facto

Handreiking
Signalerend openbronnenonderzoek in de gemeentelijke openbare ordepraktijk

Lectoraat Bestuur en Veiligheid in een Digitaliserende Samenleving,
NHL Stenden Hogeschool

THORBECKE ACADEMIE
NHL STENDEN

Hooghiemstra & Partners

HOOGHIEMSTRA & PARTNERS
strategisch en juridisch advies

Pro Facto

pro facto

18 februari 2026 – versie 1.1

Colofon

NHL Stenden Hogeschool
Rengerslaan 8-10
8917 DD Leeuwarden

https://www.nhlstenden.com/onderzoek/lectoraten/cybersafety

Deze handreiking is gebaseerd op de bevindingen en aanbevelingen uit het onderzoeksrapport *"Signalerend openbronnenonderzoek in de gemeentelijke openbare ordepraktijk: Kennis, vaardigheden en juridisch-ethische randvoorwaarden voor verantwoorde toepassing door gemeenten"* (Sajoe et al., 2026). De handreiking is ontwikkeld in opdracht van het Regionaal Bestuurlijk Politie Overleg (RBPO) en biedt een praktische vertaling van de onderzoeksresultaten naar toepasbare werkwijzen voor gemeenten.

Auteurs:	Dustin Sajoe, Willem Bantema (NHL Stenden Hogeschool), Christian Boxum (Pro Facto) en Thijs Drouen (Hooghiemstra & Partners)
Opdrachtgever:	Regionaal Bestuurlijk Politie Overleg (RBPO)
Datum:	18 februari 2026
Versie:	1.1 (definitief)

Deze handreiking is bedoeld als een praktisch hulpmiddel voor gemeenten om signalerend openbronnenonderzoek verantwoord en proportioneel uit te voeren. De inhoud is gebaseerd op het onderzoeksrapport, maar is specifiek toegespitst op de uitvoeringspraktijk.

Inhoud

1 Doel, scope en uitgangspunten

1.1 Aanleiding en context

Gemeenten krijgen steeds vaker te maken met incidenten en maatschappelijke spanningen die online beginnen en vervolgens doorwerken in de fysieke leefomgeving. Digitale platformen spelen hierbij een belangrijke rol: deze verspreiden informatie, mobiliseren mensen, beïnvloeden de perceptie en kunnen escalatie versnellen. Hierdoor zijn signalen die relevant zijn voor de openbare orde vaak vroegtijdig online zichtbaar, terwijl de impact zich lokaal manifesteert.

Dit vraagt om tijdig en proportioneel inzicht voor bestuurders: Wat speelt er precies, hoe serieus is het, en wat betekent dit voor de voorbereiding en besluitvorming? Het is daarbij van belang om in aanmerking te nemen dat gemeenten een **bestuurlijke rol** hebben en dus geen opsporingsmandaat.[1] Dat betekent dat online informatieverzameling en -duiding niet kan plaatsvinden zoals bij politie of inlichtingendiensten.

Deze handreiking richt zich op **signalerend openbronnenonderzoek**, een **versimpelde vorm van OSINT** specifiek gericht op de gemeentepraktijk binnen het domein openbare orde en veiligheid (OOV/AOV). Het gaat om doelgericht en tijdelijk werken met publiek toegankelijke online informatie, om bestuurlijke duiding en voorbereiding te ondersteunen.

In de praktijk zien we verschillen tussen gemeenten in begripsgebruik (wat is "OSINT"?), werkwijzen, rolopvattingen en borging. Dit leidt tot handelingsverlegenheid ("Mogen we dit wel?") of risico's op ongeoorloofde privacyschendingen van burgers doordat de grenzen niet duidelijk zijn. Deze handreiking biedt daarom een **eenduidig en toetsbaar kader** voor signalerend openbronnenonderzoek in de gemeentelijke praktijk.

1.2 Doel en gebruik van deze handreiking

1.2.1 Doel

Deze handreiking helpt gemeenten om verantwoord en doelgericht online signalen te verzamelen en te duiden. Het gaat om publiek toegankelijke informatie, die tijdelijk en proportioneel wordt gebruikt voor bestuurlijke voorbereiding en besluitvorming in het domein openbare orde en veiligheid.

Tijdelijk betekent dat het onderzoek plaatsvindt binnen een begrensd tijdvenster, bijvoorbeeld rond een specifiek evenement of incident, en stopt zodra de bestuurlijke informatiebehoefte is beantwoord. Proportioneel betekent dat er alleen informatie

[1] Gemeenten hebben een bestuurlijke taak (Gemeentewet, art. 172 lid 1) en geen strafrechtelijk opsporingsmandaat. Zie ook: Hooghiemstra & Partners & Pro Facto. (2023a). *Handreiking voor gemeenten voor online onderzoek bij het handhaven van de openbare orde.*

wordt verzameld die noodzakelijk is voor het doel, zonder onnodige inbreuk op privacy of opschaling naar zwaardere onderzoeksmethoden.

Voorbeeld: Een gemeente merkt op sociale media een oproep voor een demonstratie bij het gemeentehuis. Het onderzoek richt zich dan alleen op het verzamelen van publiek toegankelijke informatie over deze specifieke oproep binnen een afgebakend tijdvenster, zoals 48 uur voor het evenement. Zodra de informatiebehoefte is beantwoord, stopt het onderzoek.

De handreiking ondersteunt bij het vertalen van een bestuurlijke informatiebehoefte naar een concrete werkwijze:

- Wat moeten we weten?
- Waarom is dit nodig?
- Binnen welke grenzen werken we?

Daarmee versterkt de handreiking de samenwerking tussen opdrachtgevers en uitvoerders (bijv. OOV/AOV, communicatie, informatie/veiligheid), inclusief toetsing en verantwoording.

1.2.2 Voor wie

Deze handreiking is bedoeld voor verschillende rollen binnen de gemeente en ketenpartners:

- **Bestuurders en opdrachtgevers** (burgemeester, OOV/AOV-leiding): zij bepalen de informatiebehoefte, het doel, en de grenzen van het onderzoek.
- **Uitvoerders/analisten** (OOV/AOV, communicatie, informatie/veiligheid): zij voeren het onderzoek uit, binnen de afgesproken publiek toegankelijke bronnen en randvoorwaarden.
- **Toetsers en ondersteuners** (privacy officer/FG, juridisch adviseur, informatiebeheer): zij controleren of het onderzoek voldoet aan de juridische en ethische kaders, en borgen de verantwoording, dossiervorming en bewaartermijnen.
- **Ketenpartners** (politie, veiligheidsregio, OM): voor afstemming over de informatiepositie en escalatie wanneer dat nodig is.

Onderstaande RASCI-tabel geeft een overzicht van de verantwoordelijkheden per taak:

Tabel 1. RASCI-tabel: Rolverdeling en verantwoordelijkheden bij signalerend openbronnenonderzoek

Taken/ Verantwoordelijk-heden	Bestuurders/ Opdrachtgevers	Leidinggevenden (OOV/AOV-leiding)	Uitvoerders/ Analisten	Toetsers/Privacy Officer	Juridisch Adviseur	Informatiebeheer	Ketenpartners
Bepalen informatiebehoefte	A	R	I	C	C	I	I
Uitvoeren onderzoek	A	C	R	C	C	S	
Toetsen juridische/ethische kaders	A	C	I	A	R	S	
Dossiervorming en bewaartermijnen	A	C	R	C	C	R	
Escalatie en afstemming	A	R	C	I	I	I	I

Toelichting op de RASCI-tabel:

- **Accountable** (A): De persoon of rol die eindverantwoordelijk is voor de taak.
- **Responsible** (R): De persoon of rol die uitvoerend verantwoordelijk is voor de taak.
- **Consulted** (C): De persoon of rol die raadgevend is en betrokken wordt bij de taak.
- **Supportive** (S): De persoon of rol die ondersteunend is bij de uitvoering van de taak.
- **Informed** (I): De persoon of rol die geïnformeerd moet worden over de uitvoering of resultaten van de taak.

1.2.3 Wat deze handreiking wel en niet doet

Deze handreiking:

- **Biedt een duidelijk kader:** afbakening, begripsuitleg, stappenplannen, checklists, rolverdeling, logging, en kwaliteitsroutines. Ook bevat het escalatiepunten als er grenzen in zicht komen.
- **Biedt geen training:** het leert medewerkers niet hoe ze specifieke zoektechnieken of verificatietools moeten gebruiken. Wel benoemt het welke vaardigheden nodig zijn, zodat gemeenten gericht kunnen trainen en ontwikkelen.

1.3 Begrippen en definities

In dit domein worden termen zoals OSINT, online onderzoek, online monitoring, digitale signalering en openbronnenonderzoek niet altijd eenduidig gebruikt. Deze handreiking geeft **duidelijke definities** om een gedeeld begrippenkader te creëren tussen bestuurders, uitvoerders en toetsers. Zo voorkom je verschillende verwachtingen over doel, reikwijdte en bevoegdheden, en wordt duidelijk welke werkwijzen wel en niet passen binnen **signalerend openbronnenonderzoek** in het OOV/AOV-domein.

1.3.1 Open-source intelligence

OSINT is het doelgericht verzamelen en analyseren van publiek beschikbare informatie om een specifieke informatiebehoefte te beantwoorden. Voor gemeenten betekent dit:

- Het start bij een **concrete aanleiding** (bijv. een incident, een oproep op sociale media, of een signaal uit de samenleving), die leidt tot een **expliciete bestuurlijke vraag** (bijv. van de burgemeester of AOV-opdrachtgever).
- Het wordt proportioneel vertaald naar wat binnen publiek toegankelijke bronnen rechtmatig en zorgvuldig kan worden gedaan.

1.3.2 Signalerend openbronnenonderzoek

Signalerend openbronnenonderzoek is het doelgericht en tijdelijk verzamelen, analyseren en duiden van publiek toegankelijke online informatie door gemeenten. Het **ondersteunt bestuurlijke duiding** en voorbereiding binnen het domein openbare orde en veiligheid, binnen strikte juridische en ethische grenzen en passend bij het niet-opsporende mandaat van gemeenten.

Deze werkwijze is niet-intrusief en omvat geen:

- Gebruik van valse accounts of social engineering.
- Toegang vragen tot besloten groepen of kanalen.
- Bijzondere opsporingsbevoegdheden (zoals onderschepping of stelselmatige observatie).
- Grootschalige geautomatiseerde verzameling (scraping), profiling of persoonsgericht volgen.
- Doelbewust zoeken in omgevingen met een redelijke privacyverwachting.

Kortom: het gaat om openbare signalen herkennen en wegen, met dataminimalisatie, proportionaliteit en verantwoording als leidende principes (om bestuurlijke duiding en voorbereiding te ondersteunen).

1.3.3 Publiek toegankelijke bronnen

Publiek toegankelijke bronnen zijn online informatiebronnen die voor iedereen vrij raadpleegbaar zijn, zonder toestemming, lidmaatschap, betaalmuur of andere toegangsdrempels. Het gaat om informatie die een gemiddelde internetgebruiker via normale functionaliteiten kan zien en gebruiken.

1.4 Afbakening en uitgangspunten

Deze handreiking richt zich op signalerend openbronnenonderzoek door gemeenten binnen het domein openbare orde en veiligheid (OOV/AOV). Het gaat om doelgericht en tijdelijk werken met publiek toegankelijke online informatie, om bestuurlijke duiding en voorbereiding te ondersteunen.

1.4.1 Afbakening

- **Binnen scope**: het signaleren, verzamelen, ordenen en duiden van **publiek zichtbare** online signalen die relevant kunnen zijn voor openbare orde, veiligheid of bestuurlijke voorbereiding passend binnen de taakuitvoering van de burgemeester op grond van de wet.
- **Buiten scope**: opsporing, inlichtingenwerk, stelselmatige observatie, of handelingen die passen bij strafrechtelijke of bijzondere bevoegdheden.
- **Niet toegestaan**: binnendringen in besloten omgevingen, misleiding (bijv. valse identiteit), grootschalige geautomatiseerde dataverzameling, of profilering/persoonsgericht volgen.

1.4.2 Wanneer toepassen

- **Bij een concrete aanleiding** (bijv. aankondiging van een demonstratie, oplopende maatschappelijke spanningen, online oproepen tot verstoring, dreiging rond een locatie of evenement), passend binnen de taakuitvoering van de burgemeester op grond van artikel 172 van de Gemeentewet en andere relevante wettelijke bevoegdheden (bijv. sluiting van een woning).
- **Vraaggestuurd**: er is een expliciete informatiebehoefte vanuit de bestuurlijke lijn, met een duidelijk doel en een beoogd product (bijv. duidingsnotitie, risico-inschatting).
- **Tijdelijk en gebeurtenisgericht**: start, loopt en stopt op basis van de aanleiding; geen structurele monitoring.

1.4.3 Uitgangspunten voor verantwoord handelen

- **Mandaat en rolzuiverheid**: gemeenten handelen bestuurlijk; niet als opsporingsorganisatie.
- **Proportionaliteit en subsidiariteit**: doe alleen wat nodig is voor het doel; kies de minst ingrijpende werkwijze.
- **Dataminimalisatie en doelbinding**: verzamel en bewaar alleen noodzakelijke (persoons)gegevens; verwerk allen voor het afgesproken doel.
- **Transparantie en verantwoording**: keuzes, bronnen en afwegingen zijn uitlegbaar en controleerbaar (o.a. via logging/verslaglegging en toetsmomenten).
- **Escalatie en overdracht**: als signalen niet passen binnen het gemeentelijke mandaat of wijzen op strafbare feiten, draag dan over aan de juiste ketenpartner.

1.4.4 Ketenpartners

- Gemeenten bouwen hun informatiepositie op publieke bronnen; ketenpartners (politie/veiligheidsregio) kunnen een andere informatiepositie hebben.
- Deze handreiking helpt duidelijk te maken:
  - **Wat de gemeente zelf rechtmatig kan doen**.
  - Welke vragen je kunt neerleggen bij partners.
  - Wanneer overdracht/escalatie aangewezen is.

1.5 Leeswijzer

Deze handreiking is primair bedoeld voor gebruik in de **koude fase**: het opbouwen, inrichten en borgen van signalerend openbronnenonderzoek in de organisatie. In een **acute casus** kan de handreiking vervolgens als **referentiekader** worden gebruikt om snel te werken binnen afgesproken rollen, grenzen en procesnormen.

- **Hoofdstuk 2**: De werkwijze in stappen, gebaseerd op de 'intelligence cycle': van opdracht en afbakening tot verzamelen, verwerken, analyseren, duiden en opleveren.
- **Hoofdstuk 3**: Wanneer stop je, wanneer escaleer je en wanneer draag je over aan ketenpartners? En wat leg je daarbij vast?
- **Hoofdstuk 4**: Hoe richt je het uitvoerbaar en verantwoord in? Met aandacht voor rollen, kwaliteitsroutines, informatiebeheer, veilige uitvoering en competentieontwikkeling.
- **Hoofdstuk 5**: Welke vaardigheden hebben professionals minimaal nodig om het onderzoek zorgvuldig uit te voeren en bestuurlijk bruikbaar te rapporteren?
- **Hoofdstuk 6**: Overzicht van de bijlagen (templates) en hoe je ze beheert, zodat de werkwijze licht, uniform en herleidbaar blijft.

2 Werkwijze: van informatiebehoefte naar bestuurlijke duiding

2.1 De 'intelligence cycle'

De intelligence cycle is een beproefde proceslogica om informatie **vraaggestuurd, proportioneel en controleerbaar** te verzamelen en te duiden. Voor gemeentelijk signalerend openbronnenonderzoek betekent dit: je werkt **tijdelijk en doelgericht**, uitsluitend met **publiek toegankelijke bronnen**, en je borgt dat keuzes **uitlegbaar** zijn (o.a. via afbakening, logging en toetsmomenten).[2] De cyclus bestaat uit vijf stappen:

1. **Opdracht en richting** (*Planning and Direction*)
2. **Verzamelen** (*Collection*)
3. **Verwerken en verrijken** (*Processing and Exploitation*)
4. **Analyse en bestuurlijke duiding** (*Analysis and Production*)
5. **Delen en besluitvorming** (*Dissemination*)

In deze werkwijze functioneren **juridische en ethische randvoorwaarden als procesnormen**. Ze structureren het werk (toetsmomenten, logging, minimaliseren, deelbeslissingen) en maken interne controle en escalatie mogelijk wanneer grenzen in zicht komen

2.2 Stap 1 – Opdracht en richting

Doel: **Een bestuurlijke informatiebehoefte vertalen naar een afgebakende, toetsbare onderzoeksopdracht.**

2.2.1 Wat je vastlegt (minimaal):

- **Aanleiding:** wat is de reden om onderzoek te doen (bijv. aankondiging van een demonstratie, oplopende maatschappelijke spanningen, online oproepen tot verstoring, dreiging rond een locatie of evenement).
- **Vraag opdrachtgever** (bijv. burgemeester/OOV-/AOV-leiding) en **doel** (waarom is dit nodig?)
- **Scope**: tijdvenster, locatie, thema/incident, beoogd product (bijv. duidingsnotitie)
- **Stopcriterium**: wanneer is er "genoeg" informatie?

2.2.2 Toetsmoment 1: juridisch én ethisch (twee sporen)

1. **Juridische check**:
    - **Rechtmatigheid**: is er een rechtsgrondslag op grond van artikel 6, eerste lid, AVG?

[2] Zie: Hooghiemstra & Partners & Pro Facto. (2023a, 2023b, 2023c).

- Proportionaliteit, subsidiariteit, doelbinding, dataminimalisatie, (persoons)gegevens alleen indien noodzakelijk;
- Bewaartermijnen/archivering volgens afspraken.

2. **Ethische check (eigen gemeentelijke criteria)**: leg als gemeente expliciet vast *waaraan je toetst*, los van het minimum van de wet. Bijvoorbeeld: "wat vinden wij passende terughoudendheid?", "wanneer dragen we een signaal over aan een ketenpartner?", "hoe wegen we impact op burgers?" **Deze criteria komen uit een gemeentelijke visie/uitgangspunten op signalering/onderzoek en worden per casus kort toegepast en genoteerd.**

Output stap 1: een korte opdrachtregel + scope + toetsnotitie (kan ½ A4).

2.3 Stap 2 – Verzamelen

Doel: **Gericht en niet-intrusief verzamelen binnen publiek toegankelijke online bronnen.**

2.3.1 Kernregels:

- Gebruik alleen publiek zichtbare informatie; geen besloten groepen, geen misleiding, geen "toegang vragen", geen grootschalige scraping, niet persoonsgericht volgen.
- Werk **vraaggestuurd**: elke zoekslag moet herleidbaar zijn naar de informatiebehoefte.

2.3.2 Kernactiviteiten:

- Kies passende bronnen bij de vraag (bijv. openbare kanalen, lokale pagina's, nieuws, open data) en leg kort uit waarom deze bronnen relevant zijn.
- Voer zoekslagen uit met zoektermen/filters/tijdvenster; pas aan als de zoekslag te breed of te smal is.
- Selecteer en bundel signalen: onderscheid *ruwe signalen* (observaties) van *duiding* (die komt in stap 4).
- Markeer direct onzekerheden/risico's (bijv. mogelijk oud materiaal, onduidelijke herkomst, mogelijk persoonsgericht).

2.3.3 Wat je vastlegt:

- Opdracht/zoekvraag + datum/tijd van uitvoering en wie de zoekslag uitvoert.
- Platforms/bronnen, zoektermen, filters, tijdvenster (incl. aanpassingen: "zoekslag 1→2").
- Relevante vondsten: bronverwijzing (URL/permalink waar mogelijk), datum van raadplegen, korte omschrijving, en waarom relevant.
- Korte notitie over betrouwbaarheid/zekerheid (bijv. "onverifieerbaar", "herkomst onduidelijk").
- Wat je bewust níet hebt vastgelegd (bijv. persoonsnamen weggelaten omdat dit niet noodzakelijk is voor het doel of in strijd is met privacyregels) indien dat relevant is voor uitlegbaarheid.

Output stap 2: bronnenlijst + eerste set signalen (ruw).

2.4 Stap 3 – Verwerken en verrijken

Doel: **Ordenen, opschonen en zodanig vastleggen dat analyse controleerbaar wordt.**

2.4.1 Kernactiviteiten:

- Verwijder dubbelingen, cluster informatie (bijv. per thema/tijdlijn/locatie).
- **Controleer de juistheid en actualiteit**: noteer bij belangrijke items of je aannames hebt over datum/tijd/context en of er aanwijzingen zijn dat informatie verouderd of onjuist kan zijn. Dit sluit aan bij het AVG-beginsel dat gegevens, voor zover verwerkt, **juist** moeten zijn en waar nodig **actueel** (in de zin van niet misleidend of evident verouderd voor het doel).
- Minimaliseer relevante (persoons)gegevens: bewaar alleen wat strikt noodzakelijk is voor het doel.

Output stap 3: geordende set signalen + korte kwaliteitsnotities (juistheid/actualiteit/onzekerheid).

2.5 Stap 4 – Analyse en bestuurlijke duiding

Doel: **Vertalen van signalen naar bestuurlijke betekenis: wat betekent dit voor voorbereiding, risico-inschatting en handelingsopties?**

2.5.1 Kernactiviteiten:

- Beoordeel de bron en duid de context (wat is de herkomst, welk bereik, welke dynamiek?).
- Voer proportionele verificatie[3] uit (triangulatie, plausibiliteit, datum/tijd check) en maak **onzekerheden expliciet.**
- **Trianguleer[4] expliciet met offline context en keteninformatie** (wijk- en gebiedskennis, eerdere incidenten, vergunning/aanmeldingen, meldingen, partnerbeelden) en benoem wat je wel/niet kunt vaststellen.
- Scheid in je product: **feitelijke observaties** vs. **interpretatie** vs. **implicaties/advies**.

Output stap 4: bestuurlijk bruikbare duiding (bijv. notitie of briefing).

---

[3] **Proportionele verificatie** is het **afstemmen van de verificatiemethode op het risico**. Bij een **laag risico** (bijv. een lokale markt) volstaat een snelle check; bij **hoog risico** (bijv. dreiging) is diepgaandere controle nodig. *Voorbeeld:* Een gerucht over een demonstratie alleen verder onderzoeken als er concrete aanwijzingen zijn voor escalatie.

[4] ***Voorbeeld***: een online oproep ("kom vanavond naar locatie X") lijkt groot door veel shares, maar triangulatie met wijkinformatie en ketenpartners laat zien dat het vooral herplaatsingen door enkele accounts zijn, terwijl er lokaal geen aanloop of mobilisatie zichtbaar is. *Let extra op wanneer:* (a) één bron/één platform het beeld domineert, (b) screenshots of doorplaatsingen circuleren zonder originele bron, (c) (ironische) memes/inside jokes letterlijk worden geïnterpreteerd, (d) oude beelden/oproepen opnieuw opduiken, of (e) een kleine groep zeer actieve accounts het volume "opblaast".

2.6 Stap 5 – Delen en besluitvorming

Doel: **De uitkomst doelgericht delen, met expliciete keuzes over wat wel/niet gedeeld mag worden, en de verantwoording borgen.**

2.6.1 Deelbeslissing: AVG-check vóór verstrekking

Voordat je (persoons)gegevens of herleidbare informatie deelt – intern of met ketenpartners – beoordeel en leg je vast:

- **Mag dit gedeeld worden voor dit doel?** (doelbinding/noodzakelijkheid)
  - Is er een **rechtsgrondslag** voor verstrekking (art. 6, eerste lid, AVG)?
  - Is er sprake van een **verenigbare verwerking** (art. 6, vierde lid, AVG)?
  - Bij persoonsgegevens van strafrechtelijke aard: is er een **aanvullende reden** (art. 32 UAVG)?
- **Welke minimale set aan informatie is voldoende?** (dataminimalisatie)
- **Onder welke voorwaarden**? (beveiligd kanaal, need-to-know, afspraken/grondslag, eventuele anonimisering/pseudonimisering)
- **Wat is vastgelegd?** (wat is gedeeld, met wie, waarom)

Dit zorgt ervoor dat "verantwoord handelen" niet alleen gaat over *wat* je vindt, maar ook over *hoe* je het gebruikt en deelt. In de koude fase kan al met een privacy officer besproken worden wat (U)AVG-technisch mogelijk is wat betreft het verstrekken van persoonsgegevens.

2.6.2 Borging na afloop:

- **Zijn er bewaartermijnen vastgesteld?** Zo niet, stel deze dan alsnog vast volgens gemeentelijke afspraken.
- Archiveer en sla op volgens gemeentelijke afspraken.
- Korte evaluatie: is escalatie/overdracht nodig geweest? Waren grenzen in zicht?

Output stap 5: gedeelde output + deel-/logbeslissing + borgingsstap (archief/evaluatie).

3 Stop-, escalatie- en overdrachtsregels (beslisregels)

Signalerend openbronnenonderzoek is begrensd tot niet-intrusieve raadpleging en duiding van publiek toegankelijke bronnen. Tijdens het werk moet expliciet worden beoordeeld of voortzetting binnen het gemeentelijk mandaat nog passend is.

Dit hoofdstuk beschrijft de minimale beslisregels voor **stoppen, escaleren en overdragen**. Juridische en ethische randvoorwaarden fungeren hierbij als **procesnormen**: ze structureren toetsmomenten, logging en escalatie wanneer grenzen in zicht komen.

3.1 **Stop:** wanneer het niet meer past binnen signalerend openbronnenonderzoek

Stop (of pauzeer) het onderzoek en leg dit vast zodra één of meer van de volgende situaties ontstaat:

- **Doel is (nog) onvoldoende scherp, noodzakelijk of ontbreekt een concrete aanleiding**: de informatiebehoefte is te breed ("thermometer"), niet herleidbaar naar bestuurlijke noodzaak, of er is geen proportionele koppeling aan besluitvorming/voorbereiding.
- **Toegangsdrempel of beslotenheid**: relevante informatie zit achter een login, in besloten groepen/kanalen of in (semi-)besloten omgevingen waarvoor toelating nodig is.
- **Methodische overschrijding dreigt**: er ontstaat behoefte aan intrusieve handelingen of opsporings-/inlichtingenmethoden (bijv. misleiding, stelselmatig volgen, grootschalige geautomatiseerde verzameling).
- **Persoonsgerichtheid of stelselmatigheid groeit**: het onderzoek verschuift van gebeurtenisgericht signaleren naar het langdurig of herhaald gericht volgen van personen of groepen, of het opbouwen van profielen.
- **Kwaliteit/actualiteit onzeker**: de beschikbare informatie is te fragmentarisch, verouderd of ambigu om verantwoord te duiden; voortzetting vergroot dan het risico op misinterpretatie.

Bij stoppen: documenteer kort **waarom** is gestopt en **welke vervolgroute** nodig is (bijv. herformuleren informatiebehoefte, interne toetsing, of ketenafstemming).

3.2 **Escaleren:** wanneer extra toetsing of autorisatie nodig is

Escaleren betekent: **niet automatisch doorgaan**, maar eerst aanvullende toetsing/autoriseringsstap organiseren. Escaleer intern in de volgende situaties:

- **(Potentiële) verwerking van persoonsgegevens:** als de noodzaak, dataminimalisatie, bewaartermijn of grondslag expliciet moet worden afgewogen.
- **Wijziging in methode of scope:** als tijdens het onderzoek blijkt dat de gekozen werkwijze moet worden aangepast (bijv. door nieuwe inzichten of onvoorziene omstandigheden), en hierdoor de proportionaliteit/subsidiariteit opnieuw moet worden beoordeeld.
- **Delen buiten het eigen team/organisatie**: zodra informatie (mogelijk) aan ketenpartners verstrekt moet worden of in bestuurlijke besluitvorming terechtkomt.

- **Hoge onzekerheid en hoge bestuurlijke druk**: als de organisatie toch "iets" wil, moet expliciet worden gemaakt wat wél en niet kan worden geconcludeerd en wie dat autoriseert.[5]

Escalatie vindt plaats via de vooraf ingerichte rolverdeling (opdrachtgever–uitvoerder–toetser–autoriseerder), zodat keuzes uitlegbaar en controleerbaar blijven.

3.3 **Overdragen**: wanneer het thuis hoort bij ketenpartners

Overdracht betekent: de gemeente **rekt het eigen mandaat niet op**, maar brengt signalen via passende routes bij de bevoegde en toegeruste partij. Overdracht is aan de orde wanneer:

- Er **aanwijzingen zijn voor strafbare feiten** of voorbereiding daarvan, of wanneer opsporingsbevoegdheden nodig zijn om de informatiepositie te verbeteren.
- Er sprake is van **acute dreiging** of veiligheidsrisico's die onmiddellijke operationele opvolging vragen.
- De benodigde vervolgstappen **intrusief** zijn of een **gesloten informatiepositie** vereisen (bijv. besloten kanalen, interceptie, stelselmatige observatie).
- Er structurele signalen ontstaan die **ketenbreed** relevant zijn (bijv. bovenlokaal, georganiseerde beïnvloeding, herhaald patroon), waarbij afstemming noodzakelijk is.

Overdracht is geen "doorsturen van alles", maar een **gerichte en geminimaliseerde** informatieoverdracht: alleen wat noodzakelijk is voor het doel van de ontvanger en passend binnen afspraken.

3.4 Wat je minimaal vastlegt bij stop/escalatie/overdracht

Bij elk beslismoment leg je minimaal hert volgende vast:

- **Aanleiding:** welk signaal of welke vraag leidde tot deze stap, en **wat was het doel?**
- **Reden**: welke grens of onzekerheid speelde een rol bij het stoppen, escaleren of overdragen?
- **Beslisser/autoriseerder**: wie heeft de beslissing genomen of geautoriseerd?
- **Gedeelde informatie:** wat is gedeeld (inhoudelijk niveau, met dataminimalisatie) en met wie (bij overdracht)?
- **Vervolgactie**: wat gebeurt hierna, door wie en binnen welke termijn?

Deze beslisregels zorgen ervoor dat signalerend openbronnenonderzoek bestuurlijk bruikbaar en toetsbaar blijft, zonder te verschuiven naar zwaardere (niet-gemeentelijke) vormen van digitaal onderzoek.

---

[5] ***Voorbeeld:*** Bij een dreigende demonstratie met onduidelijke signalen over geweldsrisico's, kan de burgemeester onder druk staan om snel te handelen. In dat geval moet eerst worden vastgesteld welke conclusies **wel** (bijv. "er is sprake van een verhoogd risico") en **niet** (bijv. "er zullen zeker rellen uitbreken") verantwoord zijn, en wie deze autoriseert.

4 Organisatie en borging: de werkwijze uitvoerbaar maken

Dit hoofdstuk beschrijft de minimale organisatorische inrichting die nodig is om de werkwijze uit hoofdstuk 2 consequent, toetsbaar en proportioneel uit te voeren. Borging is geen "extra", maar een randvoorwaarde: zonder expliciete rollen, toetsmomenten, logging en kwaliteitsroutines worden stappen persoonsafhankelijk en neemt het risico op juridische en ethische overschrijding toe.

4.1 Rollen en opdrachtsturing (wie vraagt–wie doet–wie toetst–wie autoriseert)

Doel: **Zorgen dat signalerend openbronnenonderzoek vraaggestuurd plaatsvindt, met eenduidige verantwoordelijkheid en toetsing.**

4.1.1 Kernregels

- **Opdrachtgestuurd werken**: er is altijd een expliciete bestuurlijke informatiebehoefte (startpunt stap 1), met doel, scope en tijdvenster.[6]
- **Rolverdeling is expliciet**: scheid ten minste vier functies:
    1. **Opdrachtgever** (bijv. burgemeester/OOV-leiding): de burgemeester is verwerkingsverantwoordelijke en stelt doel, proportionaliteit en governance vast.
    2. **Uitvoerder/analist**: voert stap 2–4 uit.
    3. **Toetser** (privacy/juridisch/FG/ethische adviescommissie waar passend): toetst vooraf of bij escalatie;
    4. **Autoriseerder**: accordeert product en eventuele verstrekking.
- **Escalatiepad is vooraf ingericht**: als grenzen worden geraakt (stelselmatigheid, persoonsgerichtheid, besloten omgevingen, strafbare feiten/acute dreiging), wordt opgeschaald volgens hoofdstuk 3 en niet "opgerekt" in de uitvoering.

4.1.2 Wat je vastlegt (minimaal)

- RASCI of rolbeschrijving per fase (opdracht, uitvoering, toetsing, autorisatie).
- Contactpunt(en) voor toetsing en escalatie (naam/rol, bereikbaarheid, doorlooptijd-afspraak).
- Standaard opdrachtformat (1 pagina) met: doel, aanleiding, scope, bronnenklasse (publiek), tijdvenster, gewenste output.

Output: Een vast opdracht- en rolmodel waarmee elke inzet op dezelfde manier start en eindigt.

[6] Zie: Hooghiemstra & Partners & Pro Facto. (2023a, 2023b, 2023c).

4.2 Kwaliteits- en verantwoordingsroutines (controleren, herleiden, leren)

Doel: **Zorgen dat producten reproduceerbaar, uitlegbaar en controleerbaar zijn, en dat onzekerheid expliciet wordt gemaakt.**

4.2.1 Kernregels

- **Light logging is standaard**: elke inzet heeft een korte registratie van zoekslagen, bronnen en afwegingen.[7]
- **Vier vaste controlevragen** (voor elk product):
    1. Is het doel helder en proportioneel?
    2. Zijn bronnen publiek toegankelijk en werkwijzen niet-intrusief?
    3. Wat is geverifieerd en wat is onzeker?
    4. Welke gegevens zijn vastgelegd en waarom (dataminimalisatie/doelbinding)?
- **Twee-paar-ogen bij hogere impact**: bij gevoelige context, hoge publieke impact of mogelijke persoonsgevolgen: collegiale review of toetsmoment vóór verspreiding
- **Onzekerheid expliciteren**: scheid observaties/feiten, interpretatie en implicaties; label betrouwbaarheid/zekerheid (bijv. laag–middel–hoog) en onderbouw dit met de gebruikte verificatiestappen.

4.2.2 Wat je vastlegt (minimaal)

- **Logtemplate**: zoektermen/filters/tijdvenster, bronverwijzing, selectiecriteria, bevindingen.
- **Reviewchecklist**: wie heeft gereviewd en wanneer? (inclusief drempels voor wanneer review verplicht is).
- **Standaard formats**: bronnenlijst, duidingsnotitie/briefing, onzekerheidslabel.

Output: Een minimale kwaliteitscyclus: loggen → review (waar nodig) → product met onzekerheidsduiding → leerpunten vastleggen.

4.3 Informatiebeheer en gegevensbescherming (bewaren, beveiligen, kunnen verantwoorden)

Doel: Zorgen dat vastlegging, toegang en bewaartermijnen passen bij doelbinding, dataminimalisatie en verantwoordingsplicht. Bewaartermijnen, dossierstructuur en opslaglocaties vallen onder informatiebeheer/informatiemanagement en worden door de gemeente organisatiebreed ingericht. Deze handreiking veronderstelt dat hierover lokale afspraken bestaan (proceseigenaar OOV/AOV; inrichting en uitvoering door informatiebeheer, in afstemming met privacy/juridisch).

[7] Zie: Hooghiemstra & Partners & Pro Facto. (2023b).

4.3.1 Kernregels

- **Rechtmatige en minimale verwerking van persoonsgegevens**: verwerk alleen wat noodzakelijk is voor de bestuurlijke informatiebehoefte, op basis van een geldige rechtsgrondslag (art. 6 AVG), en vermijd onnodige identificatie.
- **Eenduidige dossiervorming**: waar worden logs, screenshots en producten opgeslagen; wie heeft toegang; hoe is terugvindbaarheid geregeld.
- **Vaste bewaartermijnen**: koppel deze aan het doel en producttype; verwijder/anonimiseer wanneer niet langer nodig.[8]
- **Actualiteit en juistheid**: leg vast wanneer informatie is verzameld; voorkom dat verouderde signalen zonder context blijven bestaan.

Wat je vastlegt (minimaal)

- Opslaglocatie(s) en toegangsrollen (incl. logging van toegang waar passend).
- Bewaar- en opschoningsafspraken per producttype (log, bronnenlijst, briefing).
- Richtlijn "wat nemen we over in het dossier en wat niet" (dataminimalisatie).

Output: Een praktisch informatiebeheermethodiek die auditing en verantwoording mogelijk maakt, zonder onnodige dataverzameling.

4.4 Veilige uitvoering en weerbaarheid (digitale veiligheid, exposure, belasting)

Doel: Medewerkers, processen en systemen beschermen tegen digitale risico's en ongewenste exposure, en borgen dat de werkwijze vol te houden is.

4.4.1 Kernregels

- **Veilige werkplek**: gebruik alleen afgesproken accounts/werkstations; voorkom gebruik van privé-accounts of privéapparatuur.
- **Exposure beperken**: maak afspraken over doxing-risico's, contact met platformen/gebruikers en omgang met bedreigende content.
- **Incidentprocedure**: meld (digitale) dreiging, doxing of intimidatie direct via de vaste route.
- **Werkbelasting en nazorg**: bespreek casuïstiek en impact; voorkom dat "incidentgedreven" werk zonder reflectie standaard wordt.

4.4.2 Wat je vastlegt (minimaal)

- Veiligheidsinstructie (basis) + incidentmeldroute.
- Afspraken over accountgebruik, 2FA, wachtwoordbeheer, logging van toegang.
- Afspraak over betrokkenheid van CISO/IB: zowel vooraf in de koude fase (bijv. bij het opstellen van beleid en afspraken) als bij incidenten. wie contact onderhoudt met CISO/IB en HR/veiligheid bij incidenten.

[8] Zie: Hooghiemstra & Partners & Pro Facto. (2023c).

Output: Een veilige werkomgeving en een handelingskader voor digitale incidenten en persoonlijke risico's.

4.5 Competentieontwikkeling en oefening (structureel, niet ad hoc)

Doel: **Zorgen dat vaardigheden (hoofdstuk 6) op niveau komen en blijven, en dat grenzen en procesnormen consistent worden toegepast.**

4.5.1 Kernregels

- **Structureel opleiden en oefenen**: niet alleen "tooltraining", maar ook duiding, biasbewust werken, proportionele verificatie, en procesmatig/juridisch-ethisch handelen.
- **Intervisie en casuïstiek**: bespreek periodiek bespreken om interpretatieverschillen te verkleinen en leerpunten te borgen.
- **Kalibratie op grenzen**: oefen met situaties waarin grenzen in zicht komen (bijv. stelselmatigheid, persoonsgerichtheid, besloten omgevingen) en koppel dit aan hoofdstuk 3.

4.5.2 Wat je vastlegt (minimaal)

- Jaarcyclus (of kwartaalritme) voor training, oefening en casuïstiekoverleg.
- Minimale instapeisen (wie mag uitvoeren) en hercertificering.
- Overzicht van leerpunten en updates van werkinstructies.

Output: Een doorlopende leer- en kwaliteitslijn, zodat uitvoering niet afhankelijk is van individuele ervaring of incidentdruk.

5 Vaardigheden: wat professionals minimaal moeten kunnen

Dit hoofdstuk beschrijft de minimale vaardigheden die nodig zijn om OSINT/signalerend openbronnenonderzoek zorgvuldig en proportioneel uit te voeren binnen het gemeentelijke mandaat. Het gaat om "wat men moet kunnen" (competenties), niet om een trainingsprogramma of toolinstructie.

5.1 Technische vaardigheden

Doel: **Snel en efficiënt relevante, publiek zichtbare signalen vinden, zonder intrusieve werkwijzen.**

5.1.1 Wat je minimaal moet kunnen

- **Vraaggestuurd zoeken**: zoekslagen baseren op de informatiebehoefte (wat zoek je, waarom, in welk tijdvenster?).
- **Zoekstrategie toepassen**: zoekoperators, filters, tijdvensters, trefwoordenvarianten; herkennen waar een platform "publiek" eindigt.
- **Bronkenmerken herkennen**: herkomst/vindplaats, zichtbaarheid (openbaar vs. achter drempel), basis-indicatoren van authenticiteit (bijv. accountkenmerken op hoofdlijnen).
- **Bewijsbaar werken**: relevante vondsten vastleggen met bronverwijzing (link/screenshot) voor herleidbaarheid.

5.1.2 Veelvoorkomende valkuilen

- "Breed verzamelen" zonder scherpe vraag → leidt tot ruis en onnodige gegevensverwerking.
- Vergeten dat "zichtbaar" niet altijd "publiek toegankelijk" is (bijv. content achter login).
- Onbedoeld persoonsgericht volgen door herhaald terugkeren naar dezelfde persoon/bron.

5.2 Analytische vaardigheden (bronbeoordeling, contextduiding, biasbewuste interpretatie)

Doel: **Ruwe online signalen vertalen naar bestuurlijke betekenis: wat is relevant, wat is ruis, en wat betekent dit voor risico-inschatting en voorbereiding.**

5.2.1 Wat je minimaal moet kunnen

- **Bronbeoordeling**[9]: betrouwbaarheid en positie van de bron inschatten (wie, waarom, hoe zichtbaar) en onderscheid maken tussen primaire en secundaire bronnen.
- **Contextduiding**: online dynamiek herkennen (amplificatie, framing, herhaling, coördinatie, ironie/satire) en signalen plaatsen in lokale context.
- **Biasbewust werken**[10]: eigen aannames expliciteren; zoeken naar ontkrachtende informatie en bevestigingsbias vermijden.
- **Bestuurlijke relevantie bepalen**: expliciet maken waarom een signaal bestuurlijk relevant is (en voor wie), los van nieuwsgierigheid.

5.2.2 Veelvoorkomende valkuilen

- **"Luid = belangrijk"**: bereik/impact overschatten door zichtbaarheid of emoties.
- **Context missen**: lokaal, cultureel of tijdsgebonden context negeren, waardoor de duiding te stellig wordt.
- Feit en interpretatie verwisselen in het eindproduct.

5.3 Verificatievaardigheden (proportioneel toetsen en onzekerheid expliciteren)

Doel: **Betrouwbaarheid op hoofdlijnen toetsen binnen gemeentelijke grenzen, zodat duiding uitlegbaar is en onzekerheid zichtbaar blijft.**

5.3.1 Wat je minimaal moet kunnen

- **Trianguleren**[11] **met open bronnen**: vergelijken met meerdere publiek toegankelijke bronnen (andere platforms, nieuws, open data) en interne/offline context waar toegestaan.
- **Plausibiliteitschecks**: controleer datum/tijd, locatie-indicaties, herkomst en consistentie van claims.

---

[9] **Bronbeoordeling** is het inschatten van de **betrouwbaarheid en intentie** van een bron. Vraag jezelf: *Wie plaatst deze informatie en waarom? Is de bron primair (direct) of secundair (via anderen)? Zijn er belangen of vooroordelen zichtbaar?*

[10] **Biasbewust werken** betekent **actief letten op eigen vooroordelen** die de interpretatie van signalen kunnen vervormen. Stel jezelf vragen als: *"Zoek ik alleen bevestiging van mijn aannames?"* en *"Negeer ik informatie die niet in mijn beeld past?"*.

[11] **Trianguleren** is het **vergelijken van informatie uit meerdere onafhankelijke bronnen** (bijv. sociale media, nieuws, open data) om de betrouwbaarheid van een signaal te toetsen. Doel: **onzekerheid verminderen** en een **gebalanceerde duiding** geven. *Voorbeeld:* Een melding op Twitter checken met lokale nieuwsberichten en openbare gemeentedata.

- **Onzekerheid labelen**: geef aan wat je wel en niet kunt vaststellen en waarom; vermijd schijnzekerheid.
- **Verificatiestappen documenteren**: beschrijf kort welke checks zijn gedaan en met welk resultaat.

5.3.2 Veelvoorkomende valkuilen

- Te snel concluderen ("waar/niet waar") zonder zichtbaar te maken waarop dat berust.
- Alleen online bevestiging zoeken en lokale context/feiten negeren.
- Verificatie "uitbesteden" aan tools zonder inhoudelijke controle.

5.4 Procesmatige, juridische en ethische vaardigheden (afbakening, procesnormen, verantwoording)

Doel: **Binnen mandaat en grenzen werken én het proces zo inrichten dat het toetsbaar, proportioneel en verantwoord is.**

5.4.1 Wat je minimaal moet kunnen

- **Kennis van openbare orde-taken en bevoegdheden**: begrijp de taken en bevoegdheden van de burgemeester (bijv. op grond van art. 172 Gemeentewet) en weet hoe deze zich verhouden tot signalerend openbronnenonderzoek.
- **Kennis van gegevensbeschermingsrecht**: Begrijp wat de **AVG en UAVG** inhouden en pas deze wetgeving toe in de praktijk.
- **Afbakenen**: doel, scope, tijdvenster en bronnenklasse bepalen; herkennen wanneer een vraag **niet past** binnen signalerend openbronnenonderzoek.
- **Dataminimalisatie en doelbinding toepassen**: verwerk alleen noodzakelijke (persoons)gegevens en bewaar ze niet langer dan nodig.
- **Grensherkenning**: signaleer escalatie bij stelselmatigheid, persoonsgerichtheid, besloten omgevingen of behoefte aan bevoegdheden die gemeenten niet hebben; stop of schaal op volgens hoofdstuk 3.
- **Procesnormen uitvoeren**: logging, toetsmomenten, scheiding tussen feiten en interpretatie, onderbouwing van keuzes.
- **Verstrekking beoordelen**: begrijp dat delen/verstrekken (intern/extern) een zelfstandige stap is met AVG-toets.

5.4.2 Veelvoorkomende valkuilen

- **"Doelverschuiving"** tijdens uitvoering (scope creep[12]).
- **Te veel vastleggen "voor de zekerheid"** (in strijd met dataminimalisatie).
- **Escalatiesignalen negeren** omdat er bestuurlijke druk is.

[12] **Scope creep** is het **onzichtbaar uitdijen van een onderzoek** doordat het doel, de vraagstelling of de werkwijze tijdens de uitvoering verschuiven. Bijvoorbeeld: een onderzoek dat begint als een tijdelijke signalering, maar uitgroeit tot langdurige monitoring of het verzamelen van onnodige gegevens. Dit kan leiden tot onnodige werkdruk, juridische risico's of ethische overschrijdingen.

5.5 Schrijfvaardigheid voor bestuurlijke besluitvorming (producten die werken)

Doel: **Duiding opleveren die bestuurlijk bruikbaar is: kort, onderbouwd, met expliciete onzekerheden en handelingsopties.**

5.5.1 Wat je minimaal moet kunnen

- **Helder structureren**: kernboodschap, onderbouwing, onzekerheden, implicaties/opties.
- **Uitlegbaar formuleren**: vermijd suggestieve taal; maak expliciet wat interpretatie is.
- **Bronnen transparant opnemen**: herleidbare verwijzing naar bronnen en uitgevoerde checks.
- **Doelgroepgericht schrijven**: burgemeester/OOV-leiding heeft andere behoefte dan uitvoerende ketenpartners.

5.5.2 Veelvoorkomende valkuilen

- Overladen met details (geen besluitinformatie).
- Te stellige conclusies zonder zichtbare onderbouwing.
- Geen handelingsperspectief of escalatieadvies.

5.6 Noot over training en oefening

De handreiking schrijft geen trainingstraject voor, maar de praktijk laat zien dat deze vaardigheden alleen duurzaam beschikbaar blijven met structurele oefening, casuïstiekbespreking en periodieke kalibratie op grenzen. De organisatorische randvoorwaarden hiervoor staan beschreven in hoofdstuk 4.

6 Werkproducten en minimale vastlegging

6.1 Waarom minimale vastlegging noodzakelijk is

OSINT/Signalerend openbronnenonderzoek is bestuurlijk handelen in een digitale omgeving. Dat betekent dat niet alleen de inhoud ("wat is het signaal?") telt, maar ook de wijze waarop het tot stand is gekomen ("hoe is gezocht, begrensd, gewogen en vastgelegd?"). Juridische en ethische randvoorwaarden begrenzen daarmee niet alleen wat mag, maar functioneren ook als **procesnormen**: zij structureren het werk (toetsmomenten, logging, minimaliseren, deelbeslissingen) en maken interne controle en escalatie mogelijk wanneer grenzen in zicht komen.

Het uitgangspunt in deze handreiking is **zo licht als mogelijk, zo stevig als nodig**: minimale vastlegging die herleidbaarheid, proportionaliteit en verantwoordingsvermogen ondersteunt, zonder onnodige administratieve lasten.

6.2 Overzicht van templates en wanneer je ze inzet

Onderstaande werkproducten (templates) ondersteunen de werkwijze uit hoofdstuk 2 en de beslisregels uit hoofdstuk 3. Ze zijn opgenomen als bijlagen.

Template 1 – Opdracht en afbakening (zoekopdracht/zoekplan) *(Bijlage: 1)*

- Doel: vastleggen van klant/opdrachtgever, informatiebehoefte, doel, scope en grenzen.
- Wanneer: **altijd** bij casusgericht signalerend openbronnenonderzoek (minimaal).

Template 2 – Zoeklog (logging) *(Bijlage: 2)*

- Doel: herleidbaar vastleggen van zoekslagen (waar, wanneer, hoe) en waarom bevindingen relevant zijn.
- Wanneer: **altijd** (minimaal).

Template 3 – Duidingsnotitie/bestuurlijke briefing *(Bijlage: 3)*

- Doel: gestructureerde duiding voor besluitvorming (observaties vs. interpretatie vs. implicaties), inclusief onzekerheid.
- Wanneer: wanneer het onderzoek leidt tot een **product voor besluitvorming** of bestuurlijke voorbereiding.

Template 4 – Verificatie- en triangulatiecheck *(Bijlage: 4)*

- Doel: expliciteren welke verificatiestappen zijn gezet en wat onzeker blijft.
- Wanneer: bij **middel- tot hoog-impact** casussen, bij signalen met mogelijk grote consequenties, of bij twijfel over betrouwbaarheid.

Template 5 – Stop-/escalatie-/overdrachtsregistratie *(Bijlage: 5)*

- Doel: vastleggen dat werk is gestopt of overgedragen, met reden, moment en vervolgactie.
- Wanneer: zodra een stop-, escalatie- of overdrachtsregel wordt geraakt (hoofdstuk 3).

6.3 Waar de bijlagen voor dienen en hoe je ze beheert

De bijlagen zijn bedoeld als **startset** om de werkwijze praktisch toepasbaar en ondersteunen uniforme uitvoering. Gemeenten kunnen templates aanpassen aan eigen huisstijl of interne terminologie, zolang de kernvelden behouden blijven: opdracht/afbakening, herleidbaarheid, onzekerheid, deelbeslissingen, bewaartermijnen.

Beheer en actualisatie moeten expliciet belegd zijn (zie hoofdstuk 4):

- **Proceseigenaar:** OOV/AOV (inhoud & toepassing).
- **Toets en advies:** FG/privacy officer en juridisch adviseur (randvoorwaarden, delen en bewaren).
- **Informatiebeheer:** dossiervorming en bewaartermijnen.
- **Onderhoudsritme:** periodieke evaluatie (bijv. jaarlijks) én na incidenten of relevante jurisprudentie/handreikingen.

Literatuurlijst

Canadian Security Intelligence Service. (2019). *The intelligence cycle*. Geraadpleegd op 1 februari 2026, van https://www.canada.ca/en/security-intelligence-service/corporate/publications/2019-public-report/the-intelligence-cycle.html

Central Intelligence Agency. (z.d.). *Briefing: The intelligence cycle*. Geraadpleegd op 1 februari 2026, van https://www.cia.gov/spy-kids/static/59d238b4b5f69e0497325e49f0769acf/Briefing-intelligence-cycle.pdf

Hooghiemstra & Partners & Pro Facto. (2023a). *Handreiking voor gemeenten voor online onderzoek bij het handhaven van de openbare orde* (Versie 1.0, oktober 2023). Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Geraadpleegd van https://open.overheid.nl/documenten/799e3fc2-a01c-4cd8-955f-96408dba56ff/file

Hooghiemstra & Partners & Pro Facto. (2023b). *Juridisch kader online onderzoek in publiek toegankelijke bronnen door gemeenten in het kader van de openbare orde* (Versie 1.0, oktober 2023). Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Geraadpleegd van https://open.overheid.nl/documenten/585ffdce-f8d1-47a3-8952-dc175480b460/file

Hooghiemstra & Partners & Pro Facto. (2023c). *Veelgestelde vragen over online onderzoek door gemeenten in het kader van de handhaving van de openbare orde* (Versie 1.0, oktober 2023). Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Geraadpleegd van https://open.overheid.nl/documenten/43dcd16b-646d-4110-b21e-638c9f0dac83/file

NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid). (2021). *Richtlijn online monitoring overheid*. Ministerie van Justitie en Veiligheid. Geraadpleegd op 29 oktober 2025, van https://www.nctv.nl

NIPV (Nederlands Instituut Publieke Veiligheid). (2020). *Handreiking social media monitoring in de crisisbeheersing*. NIPV. Geraadpleegd op 25 oktober 2025, van https://www.nipv.nl

Office of the United Nations High Commissioner for Human Rights. (2022). *Berkeley Protocol on Digital Open Source Investigations: A practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law*. United Nations. Geraadpleegd op 24 oktober 2025, van https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

U.S. Office of the Director of National Intelligence. (2024). *How the IC works: The six steps in the intelligence cycle*. Geraadpleegd op 1 februari 2026, van https://www.intelligence.gov/how-the-ic-works

VNG (Vereniging van Nederlandse Gemeenten). (2022). *Digitale openbare ruimte: Handreiking voor gemeentelijke signalering*. VNG. Geraadpleegd op 27 oktober 2025, van https://www.vng.nl

VRNL (Veiligheidsregio's Nederland). (2019). *Richtlijn crisiscommunicatie in de digitale omgeving*. Veiligheidsregio's Nederland. Geraadpleegd op 28 oktober 2025, van https://www.veiligheidsregios.nl

Bijlage 1 – Opdracht en afbakening (zoekopdracht/zoekplan)

T1. Opdracht en afbakening – kerngegevens

Veld	In te vullen	Toelichting (kort)
Casusnaam/onderwerp		*Korte herkenbare titel*
Casus-ID/referentie		*Zaaknummer of intern kenmerk*
Datum & tijd start		
Aanvrager/opdrachtgever ("klant")		*Bestuurlijke of ambtelijke opdrachtgever*
Uitvoerder(s)		*Naam/rol (niet per se persoonsgegevens; kan functie)*
Toetser(s)		*FG/PO, juridisch, informatiebeheer (wie wanneer)*
Beoogd werkproduct		*Bijv. korte duidingsnotitie/briefing/ omgevingsbeeld*
Beoogde opleverdatum/tijd		

T1. Informatiebehoefte en doelbinding

Veld	In te vullen	Toelichting (kort)
Aanleiding/context		*Wat is er aan de hand/waarom nu?*
Centrale informatievraag		*1 zin: wat moet bestuurlijk bekend worden?*
Deelvragen (max. 3)		*Concretiseer wat je precies wilt weten*
Doel (doelbinding)		*Bestuurlijke duiding/voorbereiding waarvoor?*
Beoogde beslissing/handeling		*Welke bestuurlijke afweging ondersteunt dit?*
Relevantie openbare orde/veiligheid		*Koppeling aan OOV/AOV-opgave*

T1. Scope en tijdvenster

Veld	In te vullen	Toelichting (kort)
Tijdvenster onderzoek		*Vanaf–tot (bijv. laatste 72 uur/komende 48 uur)*
Geografische scope		*Gemeente/wijk/locatie/regio*
Thematische scope		*Demonstratie, evenement, spanningen, etc.*
Object van onderzoek		*Gebeurtenis/locatie/thema (bij voorkeur niet-persoonsgericht)*
Verwachte looptijd		*Eenmalig/kortdurend/herhaald (met reden)*

T1. Bronnen en zoekstrategie (hoog-over)

Veld	In te vullen	Toelichting (kort)
Publiek toegankelijke bronnen (beoogd)		*Platformen/sites/open data; geen besloten omgevingen*
Zoekaanpak (globaal)		*Kernzoektermen/hashtags/locaties; geen detail (dat komt in zoeklog)*
Inzet tooling (indien van toepassing)		*Alleen toegestane tooling; noteer welke en waarom nodig*

T1. Impact-inschatting en toetsregime

Veld	In te vullen	Toelichting (kort)
Impact-inschatting	☐ Laag ☐ Midden ☐ Hoog	*Impact op openbare orde/bestuurlijke besluitvorming*
Waarom deze impact?		*1–3 bullets (bijv. dreiging, doelgroep, schaal, media)*
Benodigde toetsing vooraf		*Bijv. FG/PO bij persoonsgegevens, juridisch bij grensvragen*
Tweede paar ogen/ collegiale review	☐ Nee ☐ Ja	*Aan te vinken bij midden/hoog of bij twijfel*
Verificatie-intensiteit	☐ Basis ☐ Verhoogd	*Basis = plausibiliteit/triangulatie; verhoogd bij hoge impact*

T1. Escalatiecriteria (wanneer stop/escaleren/overdragen)

Trigger/signaal	Actie	Wie betrekken
Twijfel of bron (semi-)besloten is/ privacyverwachting	*Escaleren*	*FG/PO + juridisch*
Dreiging/aanwijzing strafbaar feit of acute veiligheid	*Overdragen*	*Ketenpartner conform afspraken*
Neiging naar persoonsgericht/stelselmatig volgen	*Stop of escaleren*	*OOV-leiding + FG/PO*
Verzoek om gegevensdeling intern/extern	*Escaleren*	*FG/PO + juridisch*
Onvoldoende doelbinding/"nice to know"	*Stop*	*Opdrachtgever*

T1. Vastlegging en informatiebeheer

Veld	In te vullen	Toelichting (kort)
Waar wordt het dossier bewaard?		*DMS/Zaaksysteem/afgesproken locatie*
Welke logs/templates worden gebruikt?		*Minimaal: zoeklog + duidingsnotitie (indien product)*
Bewaartermijn (conform beleid)		*Verwijs naar intern beleid; noteer toepasbare termijn*
Verwijdermoment/ evaluatiemoment		*Datum of voorwaarde (bijv. na besluit/na incident)*

Bijlage 2 – Zoeklog

Doel: herleidbaar vastleggen **wat** is gedaan, **waarom**, **waar**, **wanneer** en **wat het opleverde**, zonder onnodige persoonsgegevens of detailregistratie.

Gebruik: bij ieder casusgericht signalerend openbronnenonderzoek (minimaal).

Tabel B2.1 Zoeklog

Lognr.	Datum/tijd (start–eind)	Doel van deze zoekslag (1 zin)	Bron/platform (publiek)	Zoekmethode (term/operator/filter)	Tijdvenster content	Selectiecriterium (waarom relevant)	Bevinding (korte observatie)	Betrouwbaarheid (laag/middel/hoog) + korte reden	Vastlegging (link/screenshot-ID)	Actie/volgende stap (incl. escalatie ja/nee)

6.3.1 Minimale invulregels (kort)

- **Doel zoekslag:** altijd herleidbaar naar de opdracht/informatiebehoefte (Template 1).
- **Geen onnodige persoonsgegevens:** noteer geen namen/handles tenzij strikt noodzakelijk voor duiding; zo nodig: minimaliseer (bijv. "account X", "pagina Y").
- **Vastlegging:** gebruik een **screenshot-ID** of bestandsnaam + opslaglocatie; zet alleen een URL als die publiek blijft.
- **Betrouwbaarheid:** altijd één inschatting + 1 reden (bijv. "meerdere onafhankelijke bronnen", "onduidelijke herkomst").
- **Escalatie:** markeer "ja" zodra twijfel ontstaat over grens, stelselmatigheid, persoonsgerichtheid, of overdracht (zie H3).

6.3.2 Optioneel (alleen indien nodig)

- **Gevoeligheidslabel:** openbaar/intern/vertrouwelijk (organisatie-eigen).
- **Opmerking dataminimalisatie:** wat is bewust níét vastgelegd en waarom.

Bijlage 3 – Duidingsnotitie/bestuurlijke briefing

Doel: bestuurlijk bruikbare duiding opleveren die **feitelijke observaties** scheidt van **interpretatie**, en **onzekerheid** expliciet maakt.

Gebruik: wanneer het signalerend openbronnenonderzoek leidt tot een product voor besluitvorming of bestuurlijke voorbereiding.

Tabel B3.1 Basisgegevens

Onderdeel	**Inhoud**
Titel/onderwerp	
Datum/tijd opstellen	
Opdrachtgever/ "klant" (rol, niet naam)	
Opsteller(s) (rol)	
Casus/kenmerk (intern)	
Tijdvenster onderzoek	
Gebruikte bronnen (verwijzing naar Zoeklog)	Zoeklog nr(s).:
Verspreiding/vertrouwelijkheid (organisatie-eigen)	

Tabel B3.2 Samenvatting voor besluitvorming

Onderdeel	**Inhoud (max. 5–8 bullets)**
Kernsignalen (wat is relevant)	
Duiding (wat betekent dit bestuurlijk)	
Onzekerheden/aannames (wat weten we niet)	
Handelingsopties/aandachtspunten	
Advies over vervolg (stop/door/opschalen/overdragen)	

Tabel B3.3 Feitelijke observaties (wat is gezien)

Nr.	Observatie (feitelijk, neutraal)	Bronverwijzing (Zoeklog nr. + screenshot-ID/link)	Datum/tijd van content	Betrouwbaarheid (laag/middel/hoog) + reden
1				
2				

Tabel B3.4 Interpretatie en context (hoe duiden we dit)

Onderdeel	Inhoud
Context (offline/gebiedsinfo/keteninput)	
Online dynamiek (bereik, herhaling, amplificatie, framing)	
Hypothese(s)/verklaringen (expliciet)	
Alternatieve verklaringen	
Wat kan dit betekenen voor openbare orde/veiligheid?	

Tabel B3.5 Onzekerheid, beperkingen en risico's

Onderdeel	Inhoud
Wat is onzeker/niet verifieerbaar	
Wat is mogelijk misleidend/ruis	
Beperkingen door mandaat/bron-toegang	
Risico op overschatting/onderschatting	

Tabel B3.6 Juridisch-ethische procesnormen (kort toetsmoment)

Onderdeel	Inhoud (1–2 zinnen per rij)
Doelbinding & noodzakelijkheid	
Dataminimalisatie (wat is bewust niet vastgelegd)	
Proportionaliteit/subsidiariteit (waarom deze aanpak)	
Grenzen bewaakt (geen besloten bronnen/misleiding/etc.)	
Escalatie/overdracht nodig? (ja/nee + reden)	

Bijlage 4 – Verificatie- en triangulatiecheck

Doel: Expliciteren welke verificatiestappen zijn gezet, wat onzeker blijft, en hoe de betrouwbaarheid is ingeschat.

Gebruik: Bij **middel- tot hoog-impact casussen**, signalen met grote consequenties, of twijfel over betrouwbaarheid.

Tabel B4.1 Verificatie-overzicht

Onderdeel	Inhoud	Toelichting (kort)
Signaal/observatie	*Korte omschrijving van het signaal*	*Bijv. "Oproep tot demonstratie op [datum] bij [locatie]"*
Bron	*Platform/URL + screenshot-ID*	*Bijv. "Twitter, screenshot-ID: 2026-02-04_01"*
Datum/tijd signaal	*Wanneer is het signaal geplaatst?*	*Bijv. "03-02-2026, 14:30"*
Herkomst	*Wie plaatste het signaal?*	*Bijv. "Anoniem account, aangemaakt in 2025"*
Bereik/amplificatie	*Aantal shares/likes/retweets*	*Bijv. "12 shares, 47 likes"*

Tabel B4.2 Triangulatie en verificatiestappen

Stap	Actie	Resultaat	Betrouw-baarheid (laag/ middel/ hoog)	Opmerkingen
1. Bron-beoordeling	*Wie is de bron? Wat is de intentie?*	*Bijv. "Account met 500 volgers, geen eerdere betrouwbare posts"*	Laag	*Geen verificatie van identiteit*
2. Cross-check met andere bronnen	*Welke andere bronnen bevestigen/ontkrachten?*	*Bijv. "Geen vermelding in lokale media of gemeentelijke kanalen"*	Laag	*Geen onafhankelijke bevestiging*
3. Plausibiliteits check	*Klopt datum/tijd/locatie?*	*Bijv. "Datum en locatie zijn plausibel"*	Middel	*Geen directe tegenspraak*

4. Context-check	*Past het signaal in lokale dynamiek?*	*Bijv. "Geen eerdere incidenten op deze locatie"*	Middel	*Geen directe aanleiding*
5. Offline/ keten informatie	*Wat zeggen partners/wijkteams?*	*Bijv. "Geen meldingen bij politie of wijkagent"*	Hoog	*Bevestigd door ketenpartner*

Tabel B4.3 Onzekerheden en conclusie

Onderdeel	**Inhoud**
Wat is bevestigd?	*Bijv. "De oproep bestaat, maar bereik is beperkt"*
Wat blijft onzeker?	*Bijv. "Of de oproep serieus is en of er daadwerkelijk actie volgt"*
Risico op misinterpretatie	*Bijv. "Ironie/satire kan niet worden uitgesloten"*
Aanbeveling	*Bijv. "Monitoren, maar geen verdere actie nodig"*

Bijlage 5 – Stop-/escalatie-/overdrachtsregistratie

Doel: Vastleggen dat werk is gestopt, geëscaleerd of overgedragen, met reden, moment en vervolgactie.

Gebruik: Zodra een stop-, escalatie- of overdrachtsregel (hoofdstuk 3) wordt geraakt.

Tabel B5.1 Beslismoment

Veld	In te vullen	Toelichting (kort)
Casus/referentie	*Bijv. "Demonstratie 04-02-2026"*	*Koppeling aan opdracht*
Datum/tijd beslissing	*Bijv. "04-02-2026, 10:00"*	*Wanneer is besloten?*
Beslisser/autoriseerder	*Naam/rol*	*Bijv. "Burgemeester/Teamleider OOV"*
Type beslissing	☐ *Stop* ☐ *Escalatie* ☐ *Overdracht*	*Wat is besloten?*

Tabel B5.2 Reden en context

Veld	In te vullen	Toelichting (kort)
Aanleiding	*Welk signaal/vraag leidde hiertoe?*	*Bijv. "Oproep tot strafbaar feit"*
Grenzen/onzekerheden	*Welke grens werd overschreden?*	*Bijv. "Behoefte aan opsporingsbevoegdheden"*
Betrokken partijen	*Wie is geïnformeerd/geconsulteerd?*	*Bijv. "FG, juridisch adviseur, politie"*

Tabel B5.3 Gedeelde informatie en vervolg

Veld	In te vullen	Toelichting (kort)
Wat is gedeeld?	*Korte omschrijving*	*Bijv. "Duidingsnotitie + zoeklog"*
Met wie?	*Naam/rol ontvanger*	*Bijv. "Politie, team X"*
Vervolgactie	*Wat gebeurt hierna?*	*Bijv. "Politie neemt over, gemeente monitort"*
Termijn	*Wanneer is actie afgerond?*	*Bijv. "Uiterlijk 05-02-2026"*

Tabel B5.4 Borging

Veld	In te vullen	Toelichting (kort)
Archivering	*Waar wordt dit vastgelegd?*	*Bijv. "DMS, zaaknummer 2026-001"*
Evaluatiemoment	*Wanneer wordt geëvalueerd?*	*Bijv. "Na afloop incident"*