

**Afzender**

Expertisecentrum Privacy

5.1.2.e @politie.nl

21 Typ Telefoonnr. afzender

**Ontvanger(s)**

5.1.2.e, Team IV-experts

5.1.2.e, Team onderzoek  
(COM PDC)**Rubricering**

Politie INTERN - Bedrijfsvoering

|                    |                                                                                                                   |                       |                                                    |
|--------------------|-------------------------------------------------------------------------------------------------------------------|-----------------------|----------------------------------------------------|
| <b>Datum</b>       | 3 april 2025                                                                                                      | <b>Behandeld door</b> | 5.1.2.e<br>5.1.2.e, senior privacy<br>adviseur ECP |
| <b>Ons kenmerk</b> | Memo rechtmatige grondslag voor de gegevensverwerkingen met de crisis media monitoring en analyse tool?           | <b>Kopie aan</b>      | n.v.t.                                             |
| <b>Uw kenmerk</b>  | n.v.t.                                                                                                            | <b>Bijlage(n)</b>     | n.v.t.                                             |
| <b>Onderwerp</b>   | Advies over rechtmatige grondslag(en) voor de gegevensverwerkingen met de crisis media monitoring en analyse tool |                       |                                                    |

Beste 5.1.2.e en 5.1.2.e

In januari 2025 hebben jullie contact opgenomen met het ECP in het kader van een door de politie nog te verwerven "media monitoring en analyse tool" (hierna: "tool"). Mijn collega 5.1.2.e heeft jullie toen gewezen op de mogelijkheid van het uitvoeren van het Privacy by design in procurement assessment (PDPA), zodat in het verwervingsproces passende privacy eisen kunnen worden opgenomen en de te verwerven tool privacy compliant in gebruik kan worden genomen door de politie. Vervolgens heb ik een aantal gesprekken gevoerd met 5.1.2.e en heeft een uitgebreide e-mailwisseling plaatsgevonden om het doel en de precieze inzet door de politie van de tool te bespreken en achterhalen. De (voor)vraag die daarbij centraal stond was of de politie juridisch een geldige grondslag heeft om persoons en/of politiegegevens met de tool rechtmatig te verwerken. Immers, als een dergelijke grondslag ontbreekt, dan kan de beoogde tool niet rechtmatig worden verworven en ingezet door de politie.

Kort samengevat is – op basis van alle huidige aangeleverde informatie over de tool – (nog) geen eenduidig antwoord te geven op de vraag of al dan niet sprake is van een geldige verwerkingsgrondslag voor de gegevensverwerkingen met de tool en kunnen hier serieuze kanttekeningen bij worden geplaatst. Zoals telefonisch al kort toegelicht aan 5.1.2.e heb ik een en ander ook besproken met een collega van de Gegevensautoriteit (GA) en is onze (voorlopige) conclusie dat een flink aantal (juridische) knelpunten te benoemen zijn. In onderstaande memo worden deze knelpunten benoemd en summier toegelicht.

Daarbij heb ik ervoor gekozen niet alle knelpunten volledig juridisch uit te werken omdat jullie dat nu niet verder helpt en ook niets afdoet aan het (eind)advies om de Portefeuillehouder Communicatie en/of de Directeur Communicatie contact op te laten nemen met de GA en aan de GA de volgende vragen voor te leggen:

- Welk beleid hanteert de politie met betrekking tot Sociale media monitoring en analyse?

- Kan de GA een (eind)oordeel geven over de vraag of er een grondslag is voor de politie om gegevens rechtmatig te verwerken met de tool?

Mocht er naar aanleiding van deze memo behoefte zijn aan een verdere toelichting, neem dan gerust contact met mij op.

Met vriendelijke groet,

5.1.2.e

Senior adviseur privacy

## 1. Aanleiding

Binnen de politie is een project gestart om een nieuwe “media monitoring en analyse tool” (hierna: “tool”) aan te schaffen die de huidige tool van leverancier Spottler zal vervangen. De inzet en het doel van deze tool is in de aangeleverde informatie als volgt omschreven: “de tool is gericht op het leveren van een bijdrage aan goede crisiscommunicatie. Crisiscommunicatie is onderdeel van crisismanagement (...) De missie van crisiscommunicatie bij de politie is het verdienen en behouden van publiek vertrouwen in de politie door verbinding te maken tussen de politie en de samenleving.” In dat verband is privacy advies gevraagd aan het ECP. Het ECP stuit daarbij op de onder punt 2 vermelde (voor)vraag.

## 2. (Onderzoeks)vraag

Beschikt de politie over een grondslag voor de rechtmatige verwerking van persoonsgegevens en/of politiegegevens met de te verwerven tool?

## 3. Gesignaleerde (juridische) knelpunten

Vooropgesteld wordt dat de gegevens die met de te verwerven tool zullen worden verwerkt – naam en e-mailadres van media analisten van de politie en namen van (publieke) figuren in de sociale media - kwalificeren als persoonsgegevens in de zin van art. 4 sub 1 Algemene verordening gegevensbescherming (AVG) en/of politiegegevens in de zin van art. 1 sub a van de Wet politiegegevens (Wpg) - behoudens de daarin genoemde uitzonderingen - gelezen in samenhang met art. 3 van de Politiewet (Pw). Ik volsta in dat verband met een verwijzing naar de al per e-mail verstrekte adviezen waarin dit is uitgewerkt.

Als vervolgens wordt gekeken naar een geldige verwerkingsgrondslag en/of een geldig verwerkingsdoeleinde voor de politie om deze persoonsgegevens en/of politiegegevens rechtmatig te mogen verwerken met de te verwerven tool, worden zowel op basis van de Wpg als de AVG de hieronder benoemde knelpunten gesignaleerd.

### Gesignaleerde knelpunten op basis van de Wpg

- ✓ De Wpg kent – anders dan de AVG – geen zelfstandige verwerkingsgrondslagen voor de verwerking van persoonsgegevens, maar vereist wél dat gegevens rechtmatig zijn verkregen (verkrijgingsgrondslagen). In dit geval kan de verkrijging van persoonsgegevens in het kader van de politietaak (“daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven”) alleen gebaseerd zijn op art. 3 Pw. Bij een verkrijgingsgrondslag op basis van art. 3 Pw is het criterium dat alleen een geringe inbreuk mag worden gemaakt op de rechten en vrijheden van betrokkenen. Het is zéér de vraag of de te verwerven tool deze toets zal doorstaan;
- ✓ Over de vraag wanneer en voor welke taken precies de politie zich mag baseren op art. 3 Pw bestaat veel discussie. Binnen de politie loopt al ruim 2 jaar het zogenaamde Andromedaproject dat zich buigt over complexe vraagstukken rondom (nieuwe) taken/bevoegdheden van de politie en de daarmee samenhangende vraag of deze taken/bevoegdheden al dan niet op art. 3 Pw kunnen worden gebaseerd. Denk hierbij bijvoorbeeld aan het verzamelen en analyseren van (persoons)gegevens door de politie die verkregen zijn uit publiek toegankelijke bronnen (OSINT: Open Source Intelligence). Het “zomaar aanschaffen” van de tool – dat wil zeggen zonder vooraf de kritische vraag te stellen of dit überhaupt mag en welke risico’s hieraan verbonden zijn – doorkruist dit Andromeda project. Dat is niet alleen onwenselijk, maar zou ook kunnen leiden tot de hieronder genoemde afbreukrisico’s voor de politie;
- ✓ Bij de in art. 3 Pw verwoorde politietaak “het verlenen van hulp aan hen die deze behoeven” moet het (gelet op de wetsgeschiedenis) gaan om acute hulpverlening. Lang niet alle hulpverleningstaken die de politie in het kader van een concrete crisis uitvoert voldoen hieraan, zodat in voorkomend geval géén sprake is van verwerking van persoonsgegevens in



het kader van een politietaak en de Wpg dus niet van toepassing zal zijn, zodat de vervolgvraag is welk wettelijk regime en welke eventuele verwerkingsgrondslag dan wél van toepassing is. (Zoals hieronder toegelicht kom je – als je vervolgens naar de AVG kijkt - in een soort “loop”/cirkel terecht.)

- ✓ Verder kunnen bepaalde onderdelen van crisiscommunicatie – zoals het signaleren en wegnemen van desinformatie bij de burger, het meten van het sentiment rondom de (hulpverlening van de) politie en het voorlichten van burgers – in het merendeel van de gevallen niet worden aangemerkt als politietaak, zodat ook hier de beschreven vervolgvraag aan de orde is. Bovendien is de ene crisis de andere niet en verschilt de juridische kwalificatie ervan per crisis. Kortom, nuancering is geboden: daar waar bijvoorbeeld sentimentmeting nooit een politietaak vormt, is niet uitgesloten dat bij sommige (dreigende) calamiteiten het informeren van burgers over desinformatie wél past binnen de politietaak van hulpverlening. Hierbij kan bijvoorbeeld gedacht worden aan een aanslag waarbij de schutters nog vrij rondlopen terwijl op het internet (des)informatie circuleert dat alle schutters al zijn opgepakt. In een dergelijk geval is het de taak van de politie om het publiek voor dit gevaar te behoeden door hierover te informeren;
- ✓ Het zomaar aanschaffen van de tool - zonder de hierboven weergegeven knelpunten op basis van de Wpg verder te onderzoeken en deugdelijk te onderbouwen waarom aanschaf van de tool juridisch is toegestaan - leidt tot een (aanzienlijk) politiek en/of bestuurlijk afbreukrisico voor de politie. De politie ligt al onder een vergrootglas en krijgt vanuit diverse hoeken - waaronder de Autoriteit persoonsgegevens (AP) en diverse belangen-en/of mensenrechtenorganisaties - het verwijt zich bezig te houden met “massa surveillance” van burgers. Als de door de politie te verwerven tool (die de sociale media monitort en analyseert) in de media verkeerd “geframed” wordt, dan zal dit afbreukrisico zich in de vorm van imagoschade verwezenlijken.

Uit het voorgaande blijkt dat een aantal elementen van crisiscommunicatie (als onderdeel van crisisbeheersing) in veel gevallen niet kwalificeren als politietaak, zodat de Wpg hierop niet van toepassing is. De vervolgvraag is dan ook of de gegevensverwerkingen die in het kader van deze onderdelen van crisiscommunicatie plaatsvinden onder het toepassingsbereik van de AVG vallen en er sprake is van een geldige verwerkingsgrondslag op grond van de AVG?

Bovendien rijst de vraag of de te verwerven tool door de politie uitsluitend wordt ingezet voor operationele politietaken of dat de tool ook een beleidsmatige, strategische en/of bestuurlijke component kent (hetgeen voor de hand ligt) die dan eveneens onder het toepassingsbereik van de AVG valt en waarvoor een geldige verwerkingsgrondslag noodzakelijk is. Op basis van de AVG worden de hieronder weergegeven knelpunten gesignaleerd.

### **Gesignaleerde knelpunten op basis van de AVG**

- ✓ Uitgangspunt van de AVG vormt dat persoonsgegevens alleen rechtmatig kunnen worden verwerkt als sprake is van een geldige verwerkingsgrondslag zoals opgenomen in art. 6 AVG. Op basis van alle aangeleverde informatie is de inschatting dat alleen de grondslag genoemd in art. 6 lid 1 sub e AVG (noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag) mogelijk in aanmerking komt als geldige grondslag voor de persoonsgegevensverwerkingen in de tool. De overige grondslagen zijn niet aan de orde (zoals kort toegelicht in de al per e-mail verstrekte adviezen). Als vervolgens wordt onderzocht waarin “de taak van algemeen belang” gelegen zou kunnen zijn, dan leidt dit tot de uitkomst van de in art. 3 Pw en de Wpg (art. 1 sub a) genoemde politietaken. Daarmee kom je in een rare “loop”/cirkel terecht omdat de AVG en de Wpg elkaar wederzijds uitsluiten (zie art. 2 lid 2 sub d AVG), en de AVG en Wpg dus nooit



beide op eenzelfde verwerkingsdoeleinde van toepassing kunnen zijn. Het is dan ook de vraag of art. 6 lid 1 sub e kan worden aangemerkt als geldige verwerkingsgrondslag voor de persoonsgegevensverwerkingen in de tool die onder het toepassingsbereik van de AVG vallen;

- ✓ De aanschaf van media monitoring en analyse tools staat rijksbreed ter discussie en ligt politiek gevoelig. Nagenoeg elk ministerie is bij deze discussie betrokken, waarbij de vraag centraal staat of er een geldige grondslag bestaat voor de persoonsgegevensverwerkingen met de media monitoring en analyse tools, of deze verwerkingen rechtmatig zijn en/of is voldaan aan alle overige vereisten van de AVG. Daar komt bij dat de AP er “bovenop” zit en de rechtmatigheid van de gegevensverwerkingen met deze tools nauwlettend in de gaten houdt;
- ✓ Relatief recent (2020-2023) speelde bij het ministerie van Defensie de kwestie LIMC. Het Land Information Manoeuvre Centre (LIMC) was een experimentele eenheid die ten tijde van de coronapandemie wekelijks een Open Source Intelligence-rapportage (OSINT) opleverde met behulp van social media monitoring en scraping tools om op die manier het sentiment rondom de coronacrisis in kaart te brengen. Naar aanleiding hiervan is een onderzoek ingesteld naar social media monitoring tools bij het ministerie van defensie dat is aangeboden aan de Tweede Kamer. De conclusies van dit onderzoek zijn (onder meer) dat “de huidige juridische kaders (AVG/Wpg) beperkte mogelijkheden geven voor het gebruik van social media monitoring en scraping tools voor het verwerken van persoonsgegevens van publiek toegankelijke bronnen waaronder social media sites voor de taken van Defensie” en “dat onvoldoende inzichtelijk is geworden dat bij inkoop of ingebruikname van de tools er toereikende aandacht was voor de potentiële inbreuk die een tool zou kunnen hebben op fundamentele rechten (recht op privacy) van de betrokkenen en de afweging en beoordeling van de proportionaliteit en subsidiariteit van het middel.”

De kwestie LIMC onderstreept dus eens te meer het belang om vóór inkoop van de tool zorgvuldig af te wegen wat de potentiële inbreuk op de privacy rechten van betrokkenen is en te beoordelen of het gebruik van de tool juridisch toelaatbaar en verdedigbaar is.

- ✓ Het aanschaffen van de tool - zonder de hierboven weergegeven knelpunten op basis van de AVG verder te onderzoeken en deugdelijk te onderbouwen waarom aanschaf van de tool juridisch is toegestaan - leidt dan ook tot een (aanzienlijk) politiek en/of bestuurlijk afbreukrisico voor de politie.

#### 4. Advies

In dit memo zijn op hoofdlijnen (niet limitatief en niet volledig) enkele juridische knelpunten weergegeven op basis van de Wpg en de AVG met betrekking tot de te verwerven tool. Al deze knelpunten tezamen rechtvaardigen de conclusie dat het antwoord op de vraag of sprake is van een geldige verwerkingsgrondslag voor de voorgenomen gegevensverwerkingen met de tool op dit moment onzeker is. Ons (eind)advies is dan ook om de Portefeuillehouder Communicatie en/of de Directeur Communicatie contact op te laten nemen met de GA en aan de GA de volgende vragen voor te leggen:

- Welk beleid hanteert de politie met betrekking tot Sociale media monitoring en analyse?
- Kan de GA een (eind)oordeel geven over de vraag of er een mogelijke grondslag is voor de politie om gegevens rechtmatig te verwerken met de tool?

Op basis van het antwoord op deze vragen kan dan vervolgens een definitief en afgewogen standpunt worden bepaald met betrekking tot de juridische toelaatbaarheid van (de gegevensverwerkingen met) de tool.



Memo rechtmatige grondslag voor de gegevensverwerkingen met de crisis media monitoring en analyse tool?

