

PELS RIJCKEN

Landsadvocaat

Notitie

voor Ministerie van Justitie & Veiligheid
van **5.1(2)(e)** (kantoor landsadvocaat)
datum 29 maart 2023
inzake Juridische analyse persalarmering **buiten re kwijde**
zaaknr 11016277

1 Inleiding

- 1.1 Op 9 december 2021 heeft de Landsadvocaat het ministerie van Justitie en Veiligheid ('JenV') geadviseerd over de mogelijkheden voor de politie, de brandweer en de ambulancediensten om in het licht van de toepasselijke privacyrechtelijke regelgeving persalarmeringen te doen.¹

Uitkomst van dit advies was – kort gezegd – dat de politie, onder de huidige wet- en regelgeving, enkel een persalarmering mag versturen als deze in het concrete geval geen persoonsgegevens bevat of als de persalarmering noodzakelijk is voor de uitvoering van de politietaak (als bedoeld in artikelen 3 en 4 Politiewet). Gelet op het acute karakter van een 112-melding zal daar (veelal) echter geen tijd voor zijn. Zekerheidshalve moet er dan ook van uit worden gegaan dat een persalarmering door de politie inderdaad persoonsgegevens bevat en niet noodzakelijk is voor de uitvoering van de politietaak. Dat betekent dat het de politie op dit moment niet is toegestaan persalarmeringen te versturen.

Ook vanuit de ambulancedienst zullen op dit moment geen persalarmeringen kunnen worden verstuurd. Verzending van persalarmeringen stuit naar ons oordeel af op het medisch beroepsgeheim van de centralist-verpleegkundige. Dat geldt óók als een persalarmering in een concreet geval geen persoonsgegevens zou bevatten: het beroepsgeheim strekt zich uit tot alle gegevens die bij de intake worden verkregen en niet alleen tot persoonsgegevens.

Het voorgaande ligt anders voor de brandweer. Wij achten goed verdedigbaar dat het de brandweer wel is toegestaan persalarmeringen te versturen; de Algemene Verordening Gegevensbescherming ('AVG') staat daar naar ons oordeel niet aan in de weg. Het Landelijk convenant gegevensuitwisseling meldkamers lijkt daar evenmin aan in de weg te staan.

¹ Zie het advies van de Landsadvocaat van 9 december 2021 inzake de toelaatbaarheid van persalarmeringen onder toepasselijke privacyregelgeving (hierna aangeduid als: 'ons eerdere advies').

- 1.2 Het advies van de Landsadvocaat en de uitkomst van de verkenning voor een wettelijke grondslag heeft de minister van JenV doen besluiten om de huidige vorm van persalarmeringen per 1 april 2023 stop te zetten. De minister heeft samen met de leden van het Bestuurlijk Meldkamer Beraad, de hulpdiensten en de Nederlandse Vereniging van Journalisten ('NVJ') een zgn. 'hackathon' georganiseerd om alternatieve modellen van de persalarmeringen te verkennen.
- 1.3 U heeft ons gevraagd om een 'hoog-over' analyse te verrichten van de houdbaarheid van de voorstellen, in het bijzonder of de voorstellen in lijn zijn met het in ons eerdere advies geschetste privacyrechtelijke kader. Ook zullen wij per alternatief model inventariseren of en zo ja, welke (nadere) maatregelen getroffen moeten worden om het alternatieve model mogelijk te maken. Aan de hand van onze analyse, kan de minister vervolgens een nadere keuze maken voor, dan wel een nadere verkenning te verrichten naar, één of meerdere van de kansrijke voorstellen.

2 Beschrijving van de voorstellen

- 2.1 De hackathon heeft geresulteerd in diverse voorstellen voor een alternatief persalarmeringssysteem. De voorstellen zien op persalarmeringen door de brandweer, de politie en de Veiligheidsregio en hebben uitdrukkelijk geen betrekking op het versturen van persalarmering door ambulancediensten. Het medisch beroepsgeheim, noch de huidige wettelijke uitzonderingen op het medisch beroepsgeheim, staan een dergelijke persalarmering momenteel toe.² In het vervolg van dit advies zullen wij dus slechts toetsen in hoeverre de voorgestelde alternatieve persalarmeringen kansrijk kunnen worden geacht in het licht van de relevante privacyrechtelijke wet- en regelgeving. Hoewel dit niet expliciet volgt uit de beschrijving van de voorstellen, gaan wij er bovendien vanuit dat de persalarmering, evenals onder het huidige systeem, wordt verzonden onder de verantwoordelijkheid van de hulpdienst die de intake doet.³
- 2.2 Drie van de voorstellen, te weten 'OESTER', 'ZOKHO' en '112 PAS', zijn door de aanwezigen van de hackathon het meest kansrijk geacht (zie hoofdstuk 3 voor een nadere analyse van deze voorstellen).

Open of gesloten systeem

- 2.3 Verreweg de meeste voorstellen, waaronder de bovengenoemde drie voorstellen, zien op een gesloten (persalarmering)systeem. Daarmee wordt bedoeld dat middels technische autorisaties of andersoortige maatregelen op voorhand de kring van ontvangers van persalarmeringen wordt vastgesteld. Door middel van een dergelijk gesloten systeem kan controleerbaar worden gemaakt wie de persmeldingen ontvangt.

² Zie nr. 3.16 van het eerdere advies van 9 december 2021.

³ En dus niet reeds bij reeds het aannemen van de melding door de politie.

Tijdens de hackathon zijn de volgende 'gesloten' systemen, althans elementen daarvan, aan bod gekomen:

- (a) een gesloten systeem waarbij geaccrediteerde journalisten (met een politieperskaart), eventueel in combinatie met een Verklaring omtrent Gedrag ('VOG'), na autorisatie door de hulpdienst of veiligheidsregio toegang verkrijgt tot de beveiligde omgeving;
- (b) een beveiligde omgeving waarbij je moet inloggen om toegang te verkrijgen tot de persalarmeringen;
- (c) een overeenkomst (met voorwaarden) voor het gebruik van het systeem, inclusief een gedragscode voor alle gebruikers van het systeem. Een onderdeel van de gedragscode is dat de toegang wordt geweigerd zodra de gebruiker meerdere keren (bijv. 3x) in strijd met de gebruiksvoorwaarden handelt;
- (d) afspraken over de privacyrechtelijke aspecten van de verslaglegging van de persalarmeringen, zoals bijvoorbeeld het blurren van kentekens en het niet noemen van namen.

- 2.4 Twee groepen hebben tijdens de hackathon een voorstel gedaan voor een (gedeeltelijk) open systeem. Binnen het voorgestelde open systeem heeft een ieder toegang tot de persalarmeringen, maar wordt (slechts) gemeld op het niveau van de viercijferige postcode. De journalist (maar ook ieder ander) kan zelf alvast naar de wijk/het gebied gaan. Ter plaatse kan een uitgebreidere persalarmering worden afgewacht. Verdiepende informatie wordt vervolgens ontsloten door middel van een gesloten systeem.

Belangenafweging

- 2.5 Tijdens de hackathon is duidelijk geworden dat het automatisch (zonder voorafgaande belangenafweging) doorsturen van persmeldingen niet wenselijk is. De hulpdiensten hebben de dringende wens uitgesproken dat er enige tijd (een aantal minuten) tussen de alarmering van de hulpdiensten en de persalarmering zit. Dit om de veiligheid en de goede hulpverlening ter plaatse van het incident te kunnen borgen. De wijze waarop de belangenafweging plaatsvindt, verschilt per oplossing. De groepen hebben de volgende voorstellen gedaan:

- (a) het handmatig afwegen van iedere melding door een centralist, de meldkamer of een woordvoerder;
- (b) de inzet van een algoritme/script dat geautomatiseerd een afweging maakt of een melding wordt doorgezet naar de pers, waarbij een deel van de meldingen handmatig wordt beoordeeld indien de uitkomst van het geautomatiseerde script daartoe aanleiding geeft. Een dergelijke oplossing is mede gebaseerd op het zogenoemde 'Rotterdamse model', waarbij alle

meldingen automatisch worden doorgezet en vervolgens handmatig aanpassingen in meldingen worden doorgevoerd of meldingen, bijvoorbeeld gezien de privacyrechtelijke consequenties, worden ingetrokken.⁴

Governance

2.6 Een aantal van de groepen heeft ook nagedacht over de governance van het systeem. Samengevat zijn de volgende voorstellen gedaan:

- de verantwoordelijkheid bij het systeem zou volgens de groepen belegd moeten worden bij de meldkamer, de veiligheidsregio of de NVJ;
- deze partijen dienen gezamenlijk afspraken te maken over wat en niet gedeeld mag worden;
- de onderlinge verantwoordelijkheden en afspraken moeten goed worden vastgelegd tussen partijen.

Gebruiksvriendelijkheid

2.7 Tot slot hebben de groepen ook nagedacht over de gebruiksvriendelijkheid van de voorgestelde oplossingen. Een aantal teams wil het voorgestelde systeem koppelen aan bestaande systemen. Genoemd zijn:

- het hergebruik van bestaande componenten en systemen;
- verfijning van het huidige systeem;
- geen nieuwe app maken met alle tijd, kosten, risico's en kinderziektes die erbij horen.

2.8 Tijdens de hackathon zijn ook aanvullende functionaliteiten besproken, zoals het gebruik van filters die bepalen wat voor meldingen je wel/niet wilt krijgt en uit welke regio. Een app zonder notificaties (zoals een SMS) wordt door de groepen niet voldoende geacht.

3 Algemene privacyrechtelijke analyse

3.1 Alvorens wij toekomen aan een analyse van de afzonderlijke voorstellen, staan wij stil bij enkele algemene vragen die zijn gerezen ten aanzien van de hiervoor beschreven oplossingen bij het ministerie. U heeft ons de volgende algemene vragen gesteld:

1. Welke van de in randnrs. 2.3 en 2.4 beschreven elementen van het open/gesloten systeem zijn privacyrechtelijk gezien kansrijk of nuttig? Welke

⁴ Naar wij begrijpen, hebben deelnemers van de politie aangegeven dat zij hun twijfels hebben bij het Rotterdamse model, waarbij alles altijd eerst automatisch wordt doorgezet en dan aanpassingen worden doorgevoerd of berichten worden ingetrokken. In het verleden zijn er een aantal incidenten automatisch doorgezet die eigenlijk niet automatisch doorgezet hadden mogen worden.

- maatregelen dienen (aanvullend) getroffen te worden om het gesloten of open systeem te verwezenlijken?
2. Waaraan moet de (handmatig of geautomatiseerde) belangenafweging ten aanzien van het ontsluiten van de meldingen privacyrechtelijk voldoen, met name wanneer gebruikt wordt gemaakt van algoritmes c.q. Artificial Intelligence ('AI')?
 3. In hoeverre achten wij het privacyrechtelijk mogelijk en verstandig dat de verantwoordelijkheid voor de governance en beheer van het nieuwe systeem wordt belegd bij de NVJ?

Hieronder treft u onze antwoorden op bovengenoemde vragen aan.

Open of gesloten systeem

- 3.2 De eerste vraag van het ministerie heeft betrekking op het 'open' of 'gesloten' karakter van het systeem. Wij stellen voorop dat een gesloten systeem vanuit privacyrechtelijk oogpunt de voorkeur geniet boven een open systeem. Dit volgt uit de reikwijdte en kwaliteitseisen die op grond van de Wpg resp. de AVG aan de wettelijke grondslagen van de politie resp. de brandweer worden gesteld, maar ook uit het beginsel van dataminimalisatie⁵ en het vereiste van privacy by design & default. Zowel oplossingen (a) en (b) achten wij op het eerste oogpunt privacyrechtelijk haalbaar. Het gaat in dat verband om:
- (a) een gesloten systeem waarbij geaccrediteerde journalisten (met een politieperskaart), eventueel in combinatie met een Verklaring omtrent Gedrag ('VOG'), na autorisatie door de hulpdienst of veiligheidsregio toegang verkrijgt tot de beveiligde omgeving;
 - (b) een beveiligde omgeving waarbij je moet inloggen om toegang te verkrijgen tot de persalarmeringen;

Wij lichten dit toe.

- 3.3 Voor de politie geldt dat voor het nieuwe systeem eerst een basis gecreëerd moet worden in de Wet politiegegevens ('Wpg'). De Wpg kent een gesloten verstrekkingssysteem.⁶ Dat betekent dat de persalarmering alleen kan worden gedaan als de Wpg daarvoor een basis biedt (art. 3 Wpg). Dat is het geval als, voor zover van belang, i) de persalarmering noodzakelijk is met het oog op de uitvoering van de politietaken (zie par. 2 van de Wpg) of ii) met de persalarmering sprake is van een verstrekking aan bij of krachtens de Wpg genoemde derden en daarin genoemde doelen (zie par. 3 van de Wpg jo. het Besluit politiegegevens ('Bpg')).

⁵ Zie artikel 5, eerste lid, aanhef en onder c, AVG en artikel 3, eerste en tweede lid, Wpg.

⁶ Zie *Kamerstukken II* 2005/06, 30 327, nr. 3, p. 9 en 31. Zie ook de uitspraak van de Afdeling van de Raad van State van 4 februari 2015, ECLI:NL:RVS:2015:254.

- 3.4 Zoals blijkt uit ons eerdere advies, vindt de persalarmering slechts in bepaalde gevallen plaats voor de uitvoering van de politietaak. Het voorgaande maakt dat de wetgever, bij of krachtens de wet, een expliciete grondslag dient te creëren voor de verstrekking van de politiegegevens die niet nodig is ter uitvoering van de politietaak (zie par. 3 Wpg). Wij menen in dit verband dat artikel 18 Wpg een toereikende wettelijke grondslag kan vormen voor de beoogde (gesloten) persalarmering van de politie. Een langetermijnoplossing is dat de minister van JenV overeenkomstig artikel 18, eerste lid, Wpg voor de persalarmering een expliciete wettelijke grondslag opneemt in de Bpg. Daarbij zal de minister helder moeten beschrijven aan wie de politiegegevens worden verstrekt en met het oog van welk zwaarwegend algemeen belang. Mede gezien het gesloten stelsel van de Wpg, en gezien het beginsel van dataminimalisatie en privacy by design, ligt het daarbij in de rede dat de groep ontvangers beperkt blijft tot vooraf afgebakende groep personen, in dit geval dus de (geaccrediteerde) pers. Zoals toegelicht in ons eerdere advies,⁷ zou het zwaarwegend algemeen belang kunnen worden gemotiveerd aan de hand van de middels artikel 10 EVRM en artikel 11 Handvest beschermde belangen van de pers om (persalarmerings)informatie te ontvangen.⁸ In deze motivering moet tot uitdrukking worden gebracht dat dit belang voor de samenleving van meer dan gewone betekenis. Het belang dat gediend wordt met de verstrekking van de gegevens wordt afgewogen tegen het belang van de persoonlijke levenssfeer van degene op wie de politiegegevens betrekking hebben.⁹
- 3.5 In aanloop naar een dergelijke expliciete wettelijke grondslag, zou de minister nog in overweging kunnen nemen om via artikel 18, tweede lid, Wpg een tijdelijke grondslag te creëren in afwachting op de definitieve wettelijke grondslag in de Bpg. Op grond daarvan is het mogelijk om in bijzondere gevallen aan een derde gegevens te verstrekken indien dit noodzakelijk is met het oog op een zwaarwegend algemeen belang en indien de minister van J&V hier opdracht voor heeft gegeven door middel van een machtigingsbesluit. Voor een dergelijk machtigingsbesluit gelden dezelfde motiveringsvereisten als bij het hiervoor besproken eerste lid van artikel 18 Wpg. Een aanvullende voorwaarde is evenwel dat van het machtigingsbesluit mededeling wordt gedaan aan de Autoriteit persoonsgegevens ('AP'). Ook in dat licht is het verstandig om de reikwijdte van het machtigingsbesluit te beperken tot de pers. Een 'open systeem' zal naar verwachting minder snel door de AP rechtmatig worden geacht, nu dat op voorhand zich niet verhoudt met het beginsel van dataminimalisatie.

Voor de goede orde: de incidentele verstrekkingmogelijkheid van artikel 19 Wpg, kan niet worden ingeroepen ten behoeve van de persalarmeringen van de politie. Daargelaten dat de persalarmering geen incidenteel karakter draagt, wordt met de persalarmering géén van de in artikel 19 beschreven doeleinden gediend. Artikel 20 Wpg (de structurele verstrekking van politiegegevens aan derden voor samenwerkingsverbanden) vormt evenmin

⁷ Zie nrs. 3.21 t/m 3.22 van ons eerdere advies.

⁸ Zie ook de nadere bespreking van het grondrecht op informatievrijheid in nr. 3.10 van dit advies.

⁹ *Kamerstukken II* 2005/06, 30 327, nr. 3, p. 74.

een toereikende grondslag. De persalarmeringen vinden niet plaats op grond van één van de in artikel 20, eerste lid, Wpg beschreven doeleinden.

- 3.6 Voor de brandweer achten wij verdedigbaar dat het verzenden van de persalarmering gebaseerd wordt op artikel 6, vierde lid, AVG jo. artikel 10 EVRM en artikel 11 van het EU-handvest. Voor zover daarbij *bijzondere* persoonsgegevens worden verwerkt (artikel 9 AVG), menen wij dat artikel 9, tweede lid, aanhef en onder g, AVG jo. artikel 10 EVRM en artikel 11 van het EU-handvest een toereikende grondslag kunnen bieden.¹⁰

U heeft ons nog de vraag voorgelegd op welke wijze dient te worden omgegaan met multidisciplinaire meldingen waarbij (naast de inzet van bijvoorbeeld politie en brandweer) ook inzet van de ambulance plaatsvindt. Naar wij begrijpen, is het niet mogelijk om de inhoud van de persalarmering te splitsen naar hulpdienst. Ook is niet op voorhand te voorspellen onder de verwerkingsverantwoordelijkheid van welke hulpdienst de persmelding valt. Een dergelijke melding kan bij de politie, brandweer of de ambulancedienst binnenkomen, waarna de betreffende dienst (bijv. de politie), de andere diensten (bijv. de ambulance of de brandweer), zo nodig aan de melding toevoegt. Hoewel een antwoord op uw vraag uiteindelijk afhankelijk is van de concrete inhoud van de melding, dient als uitgangspunt te worden genomen dat multidisciplinaire meldingen die zijn binnengekomen bij de ambulancedienst (en waar later de politie en/of de brandweer aan wordt toegevoegd) niet ten behoeve van de persalarmering worden doorgezet. Het medisch beroepsgeheim van de ambulancedienstmedewerkers staat daaraan in de weg. Een multidisciplinaire melding die binnenkomt bij de politie en/of de brandweer (en waar later de ambulancedienst) aan wordt toegevoegd, zouden in beginsel ten behoeve van de persalarmering kunnen worden doorgezet, mits voor de politie en de brandweer een grondslag bestaat (of is gecreëerd) én de multidisciplinaire melding geen bijzondere persoonsgegevens bevat.

- 3.7 Hoewel wij in de huidige wet- en regelgeving dus reeds een toereikende basis zien voor de persalarmeringen van de brandweer, verdient het (ook hier) aanbeveling om voor de lange termijn een expliciete wettelijke grondslag te creëren voor de persalarmering van de brandweer. Door middel van een (toekomstige) expliciete grondslag, kan de voorspelbaarheid en voorzienbaarheid van het wettelijk stelsel worden vergroot. Daarmee verkleint de wetgever daarmee de kans dat de (Europese) rechter de wettelijke basis onvoldoende voorzienbaar acht of ongeldig verklaart wegens een gebrek aan wettelijke waarborgen. Hierdoor wordt bovendien (beter) tegemoetgekomen aan de kwaliteitseisen van de AVG.

Artikel 6, derde lid, AVG bepaalt dat de rechtsgrond voor de in artikel 6, eerste lid, aanhef en onder e, AVG bedoelde verwerking moet worden vastgesteld bij Unierecht of bij lidstatelijk recht dat op de verwerkingsverantwoordelijke (in dit geval de minister) van toepassing is.

¹⁰ Zie voor een uitgebreide motivering nrs. 3.26 e.v. van ons eerdere advies. Zie in dit verband ook Gerechtshof Den Haag 24 december 2019, ECLI:NL:GHDHA:2019:3539, nrs. 4.5 t/m 4.7.

Een dergelijke lidstaatrechtelijke rechtsgrond dient volgens de AVG te voldoen aan diverse kwaliteitseisen.

Artikel 6, derde lid, AVG stelt de volgende kwaliteitseisen aan een lidstatelijke of Unierechtelijke rechtsgrond: (a) Het doel van de verwerking moet zijn vastgesteld in de Unierechtelijke bepaling of is noodzakelijk voor de vervulling van de publiekrechtelijke taak; (b) de rechtsgrond kan specifieke bepalingen bevatten om de regels van de AVG aan te passen en; (c) het lidstatelijk recht of het Unierecht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde doel.

Overweging 42 van de Preambule van de AVG bepaalt voorts dat een rechtsgrond duidelijk en nauwkeurig dient te zijn. De toepassing daarvan moet voorspelbaar zijn voor degene die door deze rechtsgrond wordt geraakt.

Een belangrijke kwaliteitseis is dat de wet voldoende duidelijk is en bovendien voldoende wettelijke waarborgen bevat die misbruik voorkomen. De wetgever dient de wet aldus zo te formuleren dat de inbreuk op de privacy van de betrokkenen in verhouding staat tot het nagestreefde doel (het informeren van de pers). Ook dit kwaliteitsvereiste maakt dat een gesloten systeem meer in de rede ligt dan een open systeem. Door de persalarmering voor een breder publiek bekend te maken dan journalisten, neemt de wetgever het risico dat de wettelijke basis voor de persalarmering in strijd wordt geacht met artikel 8 EVRM (recht op persoonlijke levenssfeer) en artikel 7 en 8 van het Handvest van de grondrechten van de Europese Unie ('Handvest'). Zie ter illustratie de recente uitspraak van het Europees Hof van Justitie ('HvJ') van 22 november 2022 waarin het HvJ oordeelde dat een (voor een ieder) openbaar UBO-register in strijd was met artikel 7 en 8 Handvest, omdat – kort gezegd – de noodzaak en het belang van het brede publiek om informatie over uiteindelijke begunstigden te ontvangen, niet kan worden aangenomen. Dit in tegenstelling tot (onder meer) bevoegde autoriteiten, waaronder bijvoorbeeld journalisten, die wel een aantoonbaar belang zouden kunnen hebben bij die informatie.

3.8 Om het beoogde gesloten systeem te verwezenlijken, zullen aanvullende privacyrechtelijke, technische en organisatorische maatregelen getroffen moeten worden. Daarbij wijzen wij (onder meer) op het volgende:

- De politie resp. de brandweer zullen, na overleg daarover met de NVJ, moeten bepalen welke informatie kan en mag worden opgenomen in de persalarmering. Daarbij moet een balans worden gezocht tussen de privacybelangen van de betrokkenen op wie de persalarmering betrekking heeft en het doel van de persalarmering (het effectief en tijdig informeren van de pers over relevante gebeurtenissen). Steeds zal daarbij tot uitgangspunt moeten worden genomen dat eventuele persoonsgegevens beperkt blijven tot het strikt noodzakelijke. Indien de persoonsgegevens niet

noodzakelijk zijn, dienen de persalarmeringen te worden ontdaan van de persoonsgegevens.¹¹

- Voor zover gewerkt wordt in hetzelfde gesloten systeem, is het mogelijk dat sprake is van een zekere gezamenlijke verwerkingsverantwoordelijkheid van de politie en de brandweer voor het gesloten systeem. In dat geval zullen de onderlinge afspraken in een zogenoemde 'onderlinge regeling' beschreven moeten worden (zie daarover nrs. 3.19 en 3.20 van dit advies).
- Zorg dat het gesloten systeem transparant is ingericht, zodat kan worden verantwoord hoe het systeem is vormgegeven, welke persoonsgegevens worden verwerkt en wie toegang tot het systeem kunnen verkrijgen.
- Verricht voorafgaand aan de toepassing van het gesloten systeem een data protection impact assessment ('DPIA'), zodat op voorhand de eventuele risico's voor de rechten van betrokkenen in kaart kunnen worden gebracht en, waar nodig, mitigerende maatregelen kunnen worden getroffen.¹²
- Stel heldere bewaartermijnen vast voor de persmeldingen die in het gesloten systeem worden verwerkt. (Voor zover technisch haalbaar) stel geautomatiseerde verwijderingsprocessen in waarmee wordt geborgd dat persoonsgegevens na het verstrijken van de bewaartermijnen geautomatiseerd worden verwijderd.
- Stel een beveiligingsplan vast waarin de beveiliging van het gesloten systeem wordt vastgesteld.
- Waarborg door middel van een autorisatiematrix en een controleproces dat degene die toegang verkrijgen tot het gesloten systeem daadwerkelijk daartoe bevoegd zijn. Stel daarbij een werkwijze vast hoe beoordeeld wordt dat een persoon toegang verkrijgt tot het gesloten systeem. Stel vast wie de bevoegdheid heeft om de toegang tot systeem te verwezenlijken. Zorg daarbij voor een werkwijze voor het verlies van technische of fysieke sleutels tot het gesloten systeem.
- Maak (met de gezamenlijke verwerkingsverantwoordelijken binnen het project) heldere afspraken over het verrichten van audits en het geven van uitvoering aan de resultaten van beveiligingsaudits.
- Stel een privacybeleid op waarin specifiek wordt ingegaan op de wijze waarop persoonsgegevens verwerkt. Werk dit privacybeleid uit in concrete privacy protocollen.
- Licht in een privacyverklaring toe op welke wijze persoonsgegevens worden verwerkt.
- Stel vast, of en zo ja op welke wijze invulling kan worden gegeven aan de rechten van de betrokkene, voor zover zich geen wettelijke uitzondering voordoet.

3.9 De overige in nr. 2.3 beschreven elementen van de oplossingen: ad (c) een overeenkomst (met voorwaarden) voor het gebruik van het systeem, inclusief een

¹¹ Zie artikel 5, eerste lid, aanhef en onder c, AVG en artikel 3, eerste en tweede lid, Wpg.

¹² Zie artikel 35 AVG en artikel 4c Wpg.

gedragscode voor alle gebruikers van het systeem en; ad (d) afspraken over de privacyrechtelijke aspecten van de verslaglegging van de persalarmeringen, zoals bijvoorbeeld het blurren van kentekens en het niet noemen van namen) vormen geen op zichzelf staande oplossingen, maar betreffen wel aanvullende maatregelen die de privacybescherming van de achter (a) en (b) beschreven gesloten systeem ten goede komen. Het verdient aanbevelingen om deze voorwaarden nader uit te werken en te koppelen aan de toegang tot het gesloten systeem. Beide maatregelen komen het beginsel van dataminimalisatie en privacy by design ten goede. Het verdient aldus aanbeveling om dergelijke waarborgen verder uit te werken. Bij de voorgestelde elementen bestaan overigens wel enkele aandachtspunten.

Aandachtspunt 1: de toegangsvoorwaarden en de gedragscode mogen geen ongerechtvaardigde inbreuk maken op het grondrecht op informatievrijheid (art. 10 EVRM, art. 7 Grondwet en art. 11 Handvest)

Wij wijzen allereerst op de wettelijke grenzen en beperkingen die de informatievrijheid stelt aan de vorm en inhoud van het beoogde gesloten systeem. Zoals uiteengezet in ons eerdere advies van 9 december 2021, stellen wij voorop dat er in onze visie geen verplichting bestaat om een systeem voor persalarmering in het leven te roepen (zie bijv. par. 3.30 van het eerdere advies). Een dergelijke positieve verplichting volgt niet uit het grondrecht op informatievrijheid zoals neergelegd in onder andere artikel 10 EVRM, artikel 7 Grondwet of 11 Handvest. Een dergelijke (concrete) verplichting volgt evenmin uit het door ICT-Recht aangehaalde artikel 85 AVG. Dat betekent dat een eventueel besluit een dergelijk persalarmeringssysteem (in enige vorm) te introduceren of voort te zetten – in het licht van artikel 10 EVRM, 7 Grondwet of artikel 11 Handvest gezien – een niet afdwingbare tegemoetkoming aan de behoeften van de NVJ betreft.

Tegelijkertijd geldt echter dat, als eenmaal wordt besloten een persalarmeringssysteem te introduceren of (in aangepaste vorm) te continueren, er uit diezelfde informatievrijheid wél beperkingen volgen met betrekking tot de vorm waarin het alarmeringssysteem concreet wordt ingericht of gehandhaafd. Voorwaarden die bepaalde groepen journalisten of publicisten zonder legitieme reden uitsluiten of slechts door de NVJ erkende journalisten toegang bieden, zullen vanuit het oogpunt van artikel 10 EVRM juridisch kwetsbaar zijn. Dat betekent dat er grenzen zijn aan hoe ‘gesloten’ een systeem in de praktijk daadwerkelijk kan worden vormgegeven. Voorwaarden die (te veel, of zonder legitieme reden) raken aan de wijze en inhoud van de door de journalisten te publiceren artikelen of de wijze waarop zij hun verslaggeving inrichten (zoals een algemeen verbod op het publiceren van foto’s van betrokkenen, een verplichting ‘voldoende afstand te houden’) kunnen daarnaast schuren met (bijvoorbeeld) het in artikel 7 Grondwet neergelegde censuurverbod. Dat creëert het risico dat dergelijke voorwaarden (of daarop gebaseerde handhavingsmaatregelen) in rechte ter discussie worden gesteld of (achteraf) niet afdwingbaar blijken.

Om de juridische haalbaarheid van een alarmeringssysteem ook vanuit dit oogpunt nader in kaart te brengen, raden wij daarom aan (met de NVJ) in

gesprek te treden over de vraag welke ideeën er over en weer leven met betrekking (i) de precieze afbakening van het beoogde systeem (welke journalisten of publicisten zouden er in het beoogde systeem precies wel of geen toegang moeten krijgen?), (ii) de inhoudelijke regels die het beoogde systeem de deelnemende journalisten/publicisten dienen op te leggen, en (iii) wat de consequentie dienen te zijn als personen die toegang hebben tot het systeem zich niet aan die regels houden. Vervolgens is het mogelijk om nader in te schatten of de daaruit voortvloeiende (beoogde) accreditatieregels vanuit het oogpunt van de informatievrijheid verdedigbaar zijn, en of de optelsom van die beoogde accreditatieregels (daadwerkelijk) een resultaat oplevert dat kan voldoen aan de kaders van het privacyrecht.

Aandachtspunt 2: het verplichtstellen van een VOG

Ook hebben wij onze twijfels bij de haalbaarheid van het voorstel om de toegang tot het gesloten systeem te beperken tot personen die beschikken over een verklaring omtrent het gedrag ('VOG'). Een VOG is een verklaring van de minister van JenV dat uit een onderzoek met betrekking tot het gedrag van de betrokken natuurlijke persoon of rechtspersoon ingesteld, gelet op het risico voor de samenleving in verband met het doel waarvoor de afgifte is gevraagd en na afweging van het belang van betrokkene, niet is gebleken van bezwaren tegen die natuurlijke persoon of rechtspersoon. In de Beleidsregel VOG-NP-RP 2022¹³ is in artikel 2.1 nader uitgewerkt wanneer een onderzoek naar het gedrag van de aanvrager in ieder geval noodzakelijk is. Het artikel lijkt geen ruimte te bieden voor het aanvragen van een VOG ten behoeve van de beoogde toegang tot het persalarmeringssysteem. Het bepaalt dat het aanvragen van een VOG wettelijke moet zijn voorgeschreven,¹⁴ dan wel zien op het bestendigen, dan wel aangaan van een werkrelatie of het aangaan van een zakelijke overeenkomst tussen een eenmanszaak of een rechtspersoon. Daarvan is in het geval van de toegang tot het persalarmeringssysteem, onder de huidige wet- en regelgeving, geen sprake. Voor zover de wetgever deze eis wil stellen, zal een VOG dus wettelijk (bij of krachtens de wet) moeten worden voorgeschreven.

- 3.10 Tot slot staan wij nog stil bij het voorgestelde 'open' systeem als beschreven in nrs. 2.4 e.v. van dit advies. Bij dit open systeem wordt de huidige opzet van de persalarmering voor de politie en de brandweer voortgezet¹⁵ maar wordt de inhoud van de persalarmering beperkt tot het (geaggregeerde) niveau van vier cijfers van de postcode. Ten aanzien van dit systeem lijkt te worden aangenomen de Wpg niet van toepassing is, omdat in het systeem niet langer *persoonsgegevens* worden verwerkt. Deze aanname lijkt te zijn gebaseerd op het uitgangspunt van het Centraal Bureau voor de Statistiek ('CBS') in zijn beleid dat een gegeven op het niveau van een viercijferige code (oftewel op buurtniveau) in het geval van het CBS niet tot personen herleidbaar is en dus ook niet kwalificeert als een persoonsgegeven.

¹³ Zie Beleidsregels 2022 voor het beoordelen van aanvragen ter verkrijging van een Verklaring Omtrent het Gedrag van natuurlijke personen en rechtspersonen (Strict. 2022, 17343).

¹⁴ Zie artikel 2.1, aanhef en onder b, onder 1, Beleidsregel VOG-NP-RP-2022.

¹⁵ Persalarmeringen van de ambulancediensten zullen niet langer worden doorgezet.

- 3.11 Vanuit privacyrechtelijk oogpunt achten wij deze aanname niet goed verdedigbaar. In geval van het CBS kan inderdaad worden aangenomen dat de informatie op het niveau van een viercijferige code niet leidt tot de verwerking van persoonsgegevens, met name omdat de overige statistische resultaten in beginsel geen (indirecte) herleidbaarheid kunnen opleveren naar een persoon. Bij het beoogde open persalarmeringssysteem ligt dat wezenlijk anders. Een persalarmering op het niveau van een viercijferige postcode, bevat op zichzelf wellicht geen direct identificerende kenmerken over een persoon, maar is naar zijn aard gericht op het informeren van de pers, zodat zij (ter plaatse) daarover kunnen rapporteren. De persalarmering zal, zo verwachten, al snel herleiden zijn tot een individueel persoon, zeker als de inhoud van de persalarmering gecombineerd wordt met nadere informatie dat over het incident naar buiten komt (bijv. via het internet of uit eigen waarnemingen van journalisten ter plaatse). Gezien het gemak en de snelheid waarmee (achteraf) herleidbaarheid kan ontstaan, menen wij dat (ook) in geval van de beoogde persalarmering op het niveau van de viercijferige postcode, niet kan worden uitgesloten dat persoonsgegevens worden verwerkt. De AVG (brandweer) en de Wpg (politie) zijn dus onverkort van toepassing.

Voor de goede orde: wij verwachten dat de AP zal oordelen dat bij de persalarmering op het niveau vier cijfers van de postcode leidt tot de verwerking van persoonsgegevens. Daarbij betrekken wij dat de AP bij haar eerdere beoordeling van andere (technische) toepassingen, waarbij (in vergelijking tot de beoogde persalarmering) verdergaande maatregelen zijn genomen om herleidbaarheid uit te sluiten, standaard lijkt te oordelen dat wél persoonsgegevens worden verwerkt. Zie ter illustratie het advies van de AP van 6 augustus 2020 waarin de AP (zelfs) ten aanzien van de Coronamelder niet aanneemt dat herleidbaarheid is uitgesloten.

- 3.12 Nu bij het beoogde open systeem alsnog persoonsgegevens worden verwerkt, is de minister in dit geval genoodzaakt een wettelijke basis te creëren overeenkomstig artikel 18 Wpg. Dat kan bijvoorbeeld door een machtigingsbesluit uit te vaardigen in de zin van artikel 18, tweede lid, Wpg. Of en zo ja, de AP een dergelijk machtigingsbesluit rechtmatig acht, hangt af van de motivering van het besluit. Daarbij geven wij mee dat wij twijfelen aan de effectiviteit, en daarmee aan de proportionaliteit, van het open systeem. Zonder enige aanduiding van de locatie in aanvulling op de viercijfers van de postcode heeft het voor de pers minder zin een persalarmering te ontvangen. Ook is geen beperking opgenomen in de kring van ontvangers. Wij sluiten dus niet uit dat de AP, ook ten aanzien van het open systeem beperkt tot de viercijferige postcode, in haar advies aan de minister tot een negatief oordeel zal komen. Daar staat echter tegenover dat op korte termijn geen snelle, haalbare juridische oplossing bestaat voor het voortzetten van het huidige systeem, zonder dat de politie daarbij het risico loopt om onrechtmatig politiegegevens te verwerken. In een separaat uit te brengen advies zullen wij bezien hoeverre het vanuit strategisch (juridisch) oogpunt wenselijk is voor de minister om, mede in het licht van het door NVJ aangekondigd kort geding, een machtigingsbesluit uit te vaardigen voor

het open systeem beperkt tot de viercijferige postcode. Deze strategie zullen wij mede afwegen tegen het uitvaardigen van een machtigingsbesluit voor een gesloten systeem met uitgebreidere informatie in de persalarmering.

Belangenafweging

- 3.13 Het ministerie vraagt zich af aan welke voorwaarden de (handmatige of geautomatiseerde) belangenafweging ten aanzien van het ontsluiten van de meldingen moet voldoen, met name wanneer gebruikt wordt gemaakt van algoritmes c.q. Artificial Intelligence ('AI').
- 3.14 Voor zowel de handmatige als de geautomatiseerde belangenafweging geldt dat een balans moet worden gezocht tussen de privacybelangen van de betrokkenen op wie de persalarmering betrekking heeft en het doel van de persalarmering (het effectief en tijdig informeren van de pers over relevante gebeurtenissen). Steeds zal daarbij tot uitgangspunt moeten worden genomen dat de verwerking van eventuele persoonsgegevens beperkt blijft tot het strikt noodzakelijke. Incidenten zonder slachtoffers kunnen in beginsel worden doorgezet. Mocht de persmelding (indirect) te herleiden zijn tot een persoon, dan dient de aard en de gevolgen van de meldingen te worden afgewogen. Indien de persoonsgegevens niet noodzakelijk zijn, dienen de persalarmeringen te worden ontdaan van de persoonsgegevens. Gevoelige persalarmeringen die bijzondere risico's met zich meebrengen voor het slachtoffer, bijvoorbeeld omdat de gegevens naar hun aard zeer privacygevoelig zijn (persalarmeringen met bijvoorbeeld medische gegevens), zouden niet moeten worden doorgezet, althans niet zonder dat daarbij enige vorm van pseudonimisering wordt toegepast.
- 3.15 Om te voorkomen dat de politie resp. brandweer worden belemmerd in hun werkzaamheden, verdient het aanbeveling om een vertraging van enkele minuten in te bouwen voordat de gebruikers van het gesloten systeem worden geïnformeerd. Met partijen zal tot een goede en werkbare vertragingstermijn moeten worden gekomen.
- 3.16 Voor zover binnen het gesloten systeem gebruik wordt gemaakt van een script of algoritme, vergelijkbaar met het Rotterdamse model, of mogelijk zelfs complexere vormen van AI, gelden er enkele aanvullende privacyrechtelijke randvoorwaarden. Het komt ons voor dat de inzet van een dergelijk algoritme naar verwachting niet zal resulteren in geautomatiseerde besluitvorming of profilering, als bedoeld in de AVG of de Wpg,¹⁶ waarbij wij wel aantekenen dat de rechtspraak hierover nog in ontwikkeling

¹⁶ De AVG definieert profilering als elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling om zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen. Zie artikel 4, aanhef en onder 4, AVG. De Wpg hanteert een vergelijkbare definitie.

is.¹⁷ Vooralsnog menen wij niettemin dat het in artikel 22 AVG resp. artikel 7a Wpg beschreven verbod op geautomatiseerde besluitvorming of profilering niet zonder meer geldt. Dit omdat er in het te realiseren systeem van persalarmeringen sprake is van betekenisvolle menselijke tussenkomst, en waar dat niet het geval is, de beslissing om een persalarmering door te zetten voor individuele betrokkenen geen rechtsgevolgen of anderszins aanmerkelijke gevolgen heeft, een en ander ervan uitgaand dat er afdoende maatregelen zijn getroffen ter bescherming van betrokkenen (zie nrs. 3.8 en 3.18 van dit advies).

- 3.17 Voor de brandweer en de politie is deze vaststelling van belang, omdat dit tot gevolg heeft dat het verbod op gebruik van bijzondere gegevens bij geautomatiseerde besluitvorming (art. 22, vierde lid, Avg) dan niet geldt. Ook is dit van belang omdat de brandweer en de politie dan geen aanvullende informatie behoeven te verstrekken over de onderliggende logica, het belang en de verwachte gevolgen van de geautomatiseerde besluitvorming (art. 13, tweede lid, onderdeel f resp. art. 14, tweede lid onderdeel f, Avg). Overigens kan het, om andere redenen zoals in het kader van verantwoordingsplichten, wel dienstig zijn om toch inzicht te geven in de werking van het algoritme.
- 3.18 Daarbij zal de politie resp. de brandweer – in aanvulling op de reeds in nr. 3.7, 3.8 en 3.9 beschreven waarborgen en aandachtspunten – in elk geval de volgende maatregelen moeten treffen om het gebruik van het algoritme in het licht van de AVG (brandweer) en de Wpg (politie) privacyrechtelijk te kunnen verantwoorden:
- Stel criteria aan de hand waarvan kan worden bepaal welke persalarmeringen mogen worden doorgezet, en welke persalarmeringen in beginsel een nadere controle vereisen. Gezien de onomkeerbare gevolgen van het plaatsen van de melding, lijkt het aanbeveling te verdienen om bij twijfelgevallen altijd eerst een menselijke controle in te bouwen. Zeker in de beginfase, waarbij de werking van het algoritme nog niet vaststaat, is het raadzaam om altijd een menselijke beoordeling in te bouwen.
 - Zorg dat de beslisboom van het algoritme transparant is ingericht, zodat de politie en de brandweer op de hoogte zijn hoe het algoritme beslist of een bericht al dan wordt doorgezet.
 - Stel een periodiek controleproces vast dat borgt dat fouten in de selectie worden opgemerkt. Stel daarbij concreet vast welke persoon of welke partij dit controleproces uitvoert.
 - Voer steekproefsgewijs een controle uit om te beoordelen of het algoritme voldoende nauwkeurig is.

¹⁷ Zie de Conclusie van AG Pikamäe van 16 maart jl. in zaak C-634/21 (Land Hessen vs. Schufa), [ECLI:EU:C:2023:220](#), waarin een creditscore op zichzelf, dus onafhankelijk van een mede daarop gebaseerde kredietbeslissing, wordt opgevat als geautomatiseerd besluit waarop art. 22, eerste lid, Avg van toepassing is. Van belang zal ook kunnen zijn de uitspraak van het gerechtshof Amsterdam op het hoger beroep tegen de uitspraak van de rechtbank Amsterdam in de Uber-zaak, zijnde [rechtbank Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1020](#)

Governance

- 3.19 Het ministerie vraagt zich tot slot af in hoeverre wij het privacyrechtelijk mogelijk en verstandig achten dat de verantwoordelijkheid voor de governance en beheer van het nieuwe systeem wordt belegd bij de NVJ. Wij zien geen, althans zeer beperkte ruimte, om de governance van het systeem te beleggen bij de NVJ.
- 3.20 Het staat vast dat de Korpschef verwerkingsverantwoordelijk is voor het (verder) verwerken van de politiegegevens ten behoeve van het doorzetten van de persalarmeringen.¹⁸ Voor de brandweer geldt dat het bestuur van de veiligheidsregio de verwerkingsverantwoordelijke is voor de verdere verwerking van de persoonsgegevens ten behoeve van het doorzetten van de persalarmeringen.¹⁹ Voor zover het gesloten systeem het karakter krijgt van een gezamenlijk systeem zullen de Korpschef en het bestuur van de Veiligheidsregio onderlinge afspraken moeten maken over het gesloten systeem. De Korpschef en het bestuur van de veiligheidsregio zijn als verwerkingsverantwoordelijken verantwoordelijk voor de governance en het beheer van het beoogde gesloten systeem. Daarmee verhoudt zich niet dat de verantwoordelijkheid voor de governance en het beheer van nieuwe systeem wordt belegd bij de NVJ. Uiteraard lijkt het daarentegen wel verstandig om in nauw overleg met de NVJ vast te stellen op welke wijze de persmeldingen worden ontsloten en welke toegangsvereisten en gebruiksvoorwaarden daarbij moeten gelden. Ook zouden de Korpschef en het bestuur van de veiligheidsregio de NVJ enige rol kunnen geven bij het screenen of autoriseren van leden van de pers die toegang willen verkrijgen tot het gesloten systeem. Van belang is evenwel dat de Korpschef en het bestuur van de Veiligheidsregio de zeggenschap behouden ten opzichte van het doel en de middelen van de verwerking van de gegevens in het gesloten systeem.

4 Nadere analyse van de voorstellen

- 4.1 Naar wij begrijpen hebben de aanwezigen van de hackathon hun voorkeur uitgesproken voor drie concrete voorstellen, te weten 'OESTER', 'ZOKHO' en '112 PAS'. Wij hebben de volgende omschrijvingen van u ontvangen:

1. Werknaam: OESTER

Gesloten platform voor geaccrediteerde journalisten die meldingen krijgen die centraal gecheckt zijn. (beveiligd, inloggen, politieperskaart + VOG, overeenkomst en voorwaarden voor gebruik)

Inzet van artificiële intelligentie (vgl. met Rotterdams systeem) -> bv. geen slachtoffers dan melding doorzetten, puur medische meldingen worden

¹⁸ Zie artikel 1 aanhef en onder f, onder 1, Wpg.

¹⁹ Zie artikel 10 aanhef en onder g en artikel 35 lid 1 Wv. Zie ook artikel 2 lid 1 aanhef en onder c Landelijk convenant. Vgl. *Kamerstukken II* 2018-2019, 35 065, nr. 3, p. 8.

helemaal niet doorgezet en categorie meldingen die altijd gecheckt moet worden. Eerst handmatige check, daarna stap voor stap introductie AI.

Incident/ongeval -> melding bij de meldkamer -> landelijk geregelde/onafhankelijke/handmatige/AI check of melding kan worden uitgestuurd -> zo ja, komt melding op besloten omgeving waar journalisten kunnen inloggen en hun werk kunnen doen

2. Werknaam: ZOKHO (zo kan het ook)

Gesloten platform vanuit politie en veiligheidsregio.

Reguliere bedrijfsvoering start in GMS, diensten worden eerst ingezet op incident/ongeval via reguliere systemen (P2000, portofoon, mobilfoon). Mediaservermonitor (naar model Rotterdam Rijnmond) waarbij aan de voorkant vastgelegd voor welke criteria de alarmeringen moeten plaatsvinden, weging per melding, aanvullingen kunnen worden gedaan in kladblok door centralist. Alarmering vindt op verrijkte wijze plaats. Duiding omvang en eventuele bijzonderheden zodat journalist kan afwegen of hij ter plaatse wil gaan. Er zit paar minuten tijd tussen melding/inzet hulpdiensten en het plaatsen van de melding in de mediaservermonitor.

Accreditatie journalisten nodig (bv. politieperskaart), periodiek gezamenlijk aan tafel om te evalueren.

Let op! weging aan de voorkant, weging per melding, bouw, onderhoud, euro's en tijd nodig.

3. Werknaam: 112 PAS (persaccreditatiesysteem)

Bijna gelijk aan ZOKHO. Verantwoordelijkheid neerleggen bij de NVJ. Vergelijkbaar met Rotterdamse model. Zorgen voor een sms/whatsapp bericht faciliteit. In uitwerking nagedacht over fasering en opbouw dergelijk systeem.

- 4.2 Afgaande op deze hoog-over beschrijvingen van de voorstellen, lijken met name 'OESTER' en 'ZOKHO' op het eerste gezicht privacyrechtelijk haalbaar. Beide oplossingen betreffen gesloten systemen. Een dergelijk gesloten systeem heeft, in het licht van de (nog te creëren)²⁰ wettelijke basis en het beginsel van dataminimalisatie de voorkeur. Daarbij zal dan wel nader rekening gehouden moeten worden met de algemene, privacyrechtelijke aandachtspunten als beschreven in nrs. 3.8 en 3.9 van dit advies. Wij sluiten de toepassing van de voorgestelde algoritmes niet uit. Wel geven wij mee dat steeds per persalarmering de bijzondere omstandigheden van het concrete geval moeten worden meegewogen. Wij kunnen niet goed overzien of en zo ja, in hoeverre een algoritme daadwerkelijk in voldoende mate getraind kan worden om een dergelijke beoordeling te maken. Vooralsnog komt het ons het verstandig voor om altijd voorafgaande menselijke tussenkomst in te bouwen voordat een

²⁰ Voor zover het de politie betreft, zie nrs. 3.4 e.v.

persalarmering wordt doorgezet. Om het gebruik van een algoritme in geval van 'OESTER' of 'ZOKHO' te verantwoorden, zouden de teams aansluiting kunnen zoeken bij de aanbevelingen die wij in 3.16 van dit advies hebben opgenomen.

- 4.3 Vanuit een privacyrechtelijk perspectief lijkt de oplossing '112 PAS' minder goed haalbaar te zijn. Dit is met name gelegen in de beoogde rol en verantwoordelijkheid van de NVJ voor het persaccreditatiesysteem. De autorisatie tot en het toegangsbeleid van het gesloten systeem vallen onder de verwerkingsverantwoordelijkheid van de Korpschef (waar het betreft persalarmeringen van de politie) resp. het bestuur van de veiligheidsregio (waar het de persalarmeringen van de brandweer betreft). Met de oplossing '112 PAS' lijkt de NVJ deze rol, en daarmee een deel van de verwerkingsverantwoordelijkheden van de korpschef resp. het bestuur van de veiligheidsregio over te nemen. Wij raden een dergelijke opzet af. Zoals uiteengezet in nr. 3.20 van dit advies, lijkt het daarentegen wel verstandig om in nauw overleg met de NVJ vast te stellen op welke wijze de persmeldingen worden ontsloten en welke toegangsvereisten en gebruiksvoorwaarden daarbij moeten gelden. Ook zouden de Korpschef en het bestuur van de veiligheidsregio de NVJ enige rol kunnen geven bij het screenen of autoriseren van leden van de pers die toegang willen verkrijgen tot het gesloten systeem. Wij merken volledigheidshalve ten opzichte van 112 PAS op dat de sms-functionaliteit een gebruiksvriendelijke functionaliteit betreft.

5 Afsluiting

- 5.1 Tot zover onze hoog-over analyse van de voorstellen die aan bod zijn gekomen tijdens de hackathon. Tot een nadere toelichting zijn wij graag bereid.
