SAMENVATTING

Deze analyse is gemaakt om duidelijkheid te krijgen over de juridische aspecten van verwerking van gegevens (met name persoonsgegevens) in het kader van het gebruik van een 112App, die burgers tijdens een noodoproep kan laten chatten en bestanden kan laten uploaden.

Conclusie: De LMS behandelt chat logs uit de 112App en bestanden die een melder uploadt als persoonsgegevens. Als dat de ambulancediscipline betreft behandelen we het als bijzondere persoonsgegevens van medische aard, en stellen we de centralist in staat om het medisch beroepsgeheim te waarborgen. De LMS verwerkt deze gegevens voor geen ander doel dan het verlenen van noodhulp, behoudens uitzonderingen die verankerd zijn in de wet.

Status: er kunnen fouten staan in dit document omdat het nog niet door een jurist is gecorrigeerd.

1 WETTELIJKE KADERS

De 112App maakt deel uit van de 112-keten en omvat de processtappen “aanname” en “intake”[1]. In de processtap “uitzetten” wordt de 112App niet gebruikt. Voor aanname geldt de AVG, omdat daar nog geen discipline bij betrokken is. Daarom is in deze fase de Politie verwerkingsverantwoordelijk (Convenant Artikel 6, lid 1). De discipline die de intake doet (Ambulance, Politie, Brandweer, KMar) is verantwoordelijk voor de melding, waarbij de LMS faciliteert. In een convenant[2] over de gegevensverwerking hebben partijen invulling gegeven aan deze gezamenlijke verantwoordelijkheid. De 112-meldingen en de overige meldingen die door een convenantpartner worden aangenomen en verwerkt tot uitgifte van in te zetten eenheden, vallen onder de privacyregels van de convenantpartner (Convenant Artikel 6, lid 3). Bij intake voor de brandweer geldt de AVG. Bij intake door een RAV geldt de AVG, waarbij de 112App-keten ook bijzondere persoonsgegevens verwerkt. Daarnaast zijn voor de ambulance-meldingen specifieke wetten over het beschermen van medische gegevens van toepassing, met name de Wet op de geneeskundige behandelingsovereenkomst (Wgbo) en de Wet op de beroepen in de individuele gezondheidszorg. Voor gegevens van de Politie en KMar gaan we uit van de WpG, aangevuld met het Addendum BIO, wat een Politie-specifieke aanvulling is op het overheidsbreed geldende BIO. Voor de onderliggende technologie zijn verder nog relevant de Telecommmunicatiewet en het Besluit 1-1-2 alarmcentrales.

2 THEMA’S

2.1 Verwerkingsverantwoordelijke

Wie is verwerkingsverantwoordelijke voor gegevens die gerelateerd zijn aan de 112App? De AVG verstaat onder verwerkingsverantwoordelijke een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In dit geval worden doel en middelen vastgesteld door het SMB,

[1] In de processtap “uitgifte” maakt een centralist weliswaar geen gebruik van de 112App-keten, maar verwerkt wel informatie die via dit kanaal is verkregen.

[2] Landelijk convenant gegevensverwerking meldkamers, vs. 2.1, uitg: Instituut Fysieke Veiligheid, 1 okt 2018.

waarin het LMS samen met de disciplines verwerkingsverantwoordelijk is. Er is dus sprake van gezamenlijke verantwoordelijkheid ex. Artikel 26 AVG. Deze gezamenlijke verwerkingsverantwoordelijkheid is verankerd in Artikel 3 sub n van het Convenant.

Als het gaat om een melding, dan stellen we vast dat de melding altijd is verwerkt door één van de disciplines. Alleen de verwerkende discipline is samen met de LMS aansprakelijk voor eventuele schade die iemand lijdt ten gevolge van een inbreuk op de privacy. Aansprakelijkheid voor een niet-verwerkende discipline is uitgesloten in Art. 82 AVG als deze bewijst dat hij op geen enkele manier verantwoordelijk is voor het schadeveroorzakende feit. Om die reden beschouwen we de LMS samen met de discipline die een melding heeft verwerkt als gezamenlijk verwerkingsverantwoordelijk.

Het meldkamerdienstencentrum wordt aangemerkt als een verwerker voor de KMar, de RAV en VR (Convenant Artikel 11 lid 3). Als verwerker verzorgt het meldkamerdienstencentrum onder meer de geautomatiseerde landelijke uitwisseling van gegevens over incidenten tussen meldkamers en de gegevensverstrekking aan externe organisaties. De 112App-keten valt dan ook binnen de werking van de verwerkersovereenkomst tussen de convenantpartners en de korpschef.

2.2 Persoonsgegevens

Wat persoonsgegevens zijn staat in Art. 4 AVG lid 1:

> "persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Om te bepalen of iets een persoonsgegeven is, is de hamvraag: zijn de gegevens direct of indirect herleidbaar naar een natuurlijke persoon? De complexiteit ontstaat door het combineren van gegevens. Afzonderlijke brokjes (bijv: “Dorpsstraat”, “Piet”) die niet herleidbaar zijn naar een persoon kunnen in samenhang met andere gegevens wél herleidbaarheid opleveren (bijv. “Piet Kelder, Dorpsstraat 15, Nuenen”). Voor de 112App-keten beschouwen we persoonsgegevens en politiegegevens als synoniem, met als karakteristiek verschil dat zij gedefinieerd zijn in verschillende bronnen (AVG resp. Wpg). De meldkamers verwerken uitsluitend de strikt noodzakelijke persoonsgegevens verwerkt volgens artikel 25 AVG, en dat geldt dus ook voor de 112App-keten.

2.3 Doelbinding

AVG Artikel 5, eerste lid onder b. zegt dat we persoonsgegevens mogen gebruiken voor het beoogde doel:

> Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding”);

Art. 5 AVG verlangt dus een welbepaald en uitdrukkelijk omschreven doel waarvoor de 112App gegevens verzameld. Dit doel is om acute hulp te verlenen in noodsituaties, wat nauwkeuriger omschre-

ven is in artikel 4 van het convenant. De LMS en de discipline verwerken de persoonsgegevens uitsluitend voor dit doel. Toestemming van de melder is alleen nodig als gegevens worden verwerkt voor een ander doel.

Bij een intake door de Politie en Marechaussee is de AVG niet meer van toepassing, maar de Wpg. Ook daar is doelbinding vereist, maar er gelden uitzonderingen. Als er bijvoorbeeld door de chat een misdrijf ter kennis van de politie komt, mag ze die gegevens delen voor opsporingsdoeleinden. Dat is een ander doel, maar wel rechtmatig vanwege de Wpg. Voor Ambulance en Brandweer is de AVG onverkort van toepassing. Met name de Ambulancecentralist mag niet zomaar persoonsgegevens delen met de politie, ook niet voor opsporingsdoeleinden die in de Wpg wel zijn toegestaan. Het convenant stelt dan ook de centralist centraal bij het beslissen of een gegeven gedeeld wordt. Dit principe is in de 112App-keten consequent doorgezet.

2.4 Bewaarbeleid

Het convenant (Artikel 20 lid 1) zegt over het bewaren van gegevens: Op de gegevens die in de gemeenschappelijke systemen of voor gezamenlijke doeleinden door de convenantpartners of hun verwerkers zijn verwerkt, zijn verschillende bewaartermijnen als gevolg van wet- en regelgeving van toepassing. Het gaat onder meer om:
a. De identificeerbare gegevens die volgens artikel 5 AVG beperkt bewaard worden nl. voor zolang dat nodig is voor de doeleinden waarvoor het verzameld is;
b. De gegevens die de politie als beheerder heeft verkregen als gevolg van een 112-melding die maximaal twee maanden bewaard mogen worden of langer zoals bepaald in artikel 11.10, leden 7 en 10 Telecommunicatiewet;
c. De gegevens die voor de MKA minimaal 15 tot 20 jaar bewaard moeten worden.

Artikel 20 van het convenant heeft nog geen uitwerking gekregen in een retentiebeleid van de LMS. De archiefwet en de AVG leggen echter wel de verplichting op om het bewaren van gegevens in beleid te verankeren. Het maken en invoeren van zulk beleid valt echter buiten bereik van het 112App-project. Als gevolg daarvan sluit de 112-App keten aan bij het retentieregime zoals dat in GMS is gerealiseerd. De 112App Back-end zal dan ook geen gegevens persisteren en de permanente opslag (indien nodig) overlaten aan GMS. Dit betreft de extra meldingsgegevens en de chat log. Voor het opslaan van bestanden (media/foto's/video's) is nog niet duidelijk hoe de 112App-keten daarmee omgaat.

2.5 Inclusiviteit

De 112App is bedoeld voor iedereen, en heeft ten behoeve van spraak en gehoorbeperkten een chatfunctionaliteit. Voor niet-Nederlandssprekenden is er ook een vertaalfaciliteit op de chat, die momenteel 109 verschillende talen aankan. Er is nog geen live-streaming faciliteit die real-time gebarentaal zou kunnen ondersteunen. (Die wens staat wel op de agenda, waarop meerdere toekomstige features van de 112App staan). Ook zijn er nog geen centralisten die Nederlandse gebarentaal machtig zijn, anders dan centralisten die dit door persoonlijke omstandigheden al kunnen.
Voor inclusiviteit moet de 112App voldoen aan de eisen uit hoofdstuk 9 van de Europese standaard EN 301 549. Dit staat gelijk aan WCAG 2.1, niveau A en AA.
Per 23 juni 2021 is een toegankelijkheidsverklaring nodig voor de 112App op basis van het Besluit digitale toegankelijkheid overheid. Deze beschrijft welke maatregelen de LMS neemt om zo snel mogelijk aan de eisen te voldoen en wanneer die maatregelen zullen zijn uitgevoerd.

De consequenties bij niet-naleven zitten voornamelijk in imagoschade. Het toezicht op naleving is belegd in het reguliere toezicht op de meldkamers, onder gezag van het SMB. Het interbestuurlijk toezicht is belegd bij het Ministerie van J&V.

2.6 Vertalen

Bij het vertalen van de chat sturen we woorden, zinsdelen en hele zinnen naar Google translate. Ook dit beschouwen we als persoonsgegevens omdat het mogelijk herleidbaar is tot personen. We bieden deze gegevens aan Google aan met als enige doel “vertalen”.

Dat betekent dat zolang Google onze gegevens alleen vertaalt dan mag het, want er is sprake van doelbinding.

Maar wat doet Google met deze gegevens? Zolang Google Translate deze gegevens alleen vertaalt is er niets aan de hand, dan valt het gewoon onder doelbinding. Wat we nu weten is dat Google claimt dat ze deze gegevens niet opslaat indien wij dit contractueel regelen. Er is geen aanleiding om te veronderstellen dat Google een dergelijke contractafspraak niet zou naleven.

3 INFORMATIEVEILIGHEID

Onderdeel van het beschermen van persoonsgegevens is de veilige verwerking ervan. De LMS hanteert het voorgeschreven tactisch normenkader (TNK) van de Baseline Informatiebeveiliging Rijksdienst (BIR: 2012), om te garanderen dat de informatie veilig wordt behandeld. De BIR:2012 omvat de voorgeschreven normen NEN/ISO 27001 en NEN/ISO 27002, waarvoor de verplichting geldt: comply or explain.

Omdat de gegevens in de chat en de geüploade bestanden persoonsgegevens *kunnen* bevatten, behandelt de LMS ze als departementaal vertrouwelijke (DepV) informatie met vertrouwelijkheidniveau WBP-risicoklasse 2 (WBP2). In veel gevallen zou WBP1 van toepassing kunnen zijn, maar we kunnen niet uitsluiten dat de meldkamer persoonsgegevens verwerkt over godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens. Omdat de gehele verwerking berekend is op deze vertrouwelijkheidniveaus (WBP2 en DepV) hoeft een medewerker zich niet per geval af te vragen of de communicatie voldoende veilig is en of de meldkamer het bericht wel voldoende veilig behandelt (Bron: BIR:2012).

Voor gegevens die een Politiecentralist verwerkt geldt de rubricering “Politie intern”[3] tenzij er een reden is om dat anders te doen, om te voorkomen dat de 112App-keten de privacy van personen schendt dan wel dat de uitvoering van de politietaak kan worden aangetast. De grondslag hiervoor is de Uitvoeringsregeling rubricering VG-Land (vs. 1.1b, januari 2010) en het Rubriceringsbeleid vtsPN (vs. 1, oktober 2010).

[3] BIO paragraaf 12.1.4.pi1 zegt: Operationele gegevens met de rubricering Politie Intern mogen niet gebruikt worden voor testdoeleinden. Als gevolg daarvan moet bij het testen ofwel een analyse worden gemaakt en toestemming verkregen, ofwel een artificiele dataset voor testen worden gebruikt.

4 GEGEVENS

4.1 Chat log en bestanden

Als we een chat opslaan, beschouwen we de inhoud ervan (de chat log) als persoonsgegevens omdat we niet kunnen uitsluiten dat deze inhoud persoonsgegevens bevat. Dit is een keuze die zorgt dat we aan de veilige kant uitkomen. Dit past ook goed in Artikel 7 van het convenant. Bestanden die een melder uploadt via de 112App behandelt de 112App-keten hetzelfde. Ook die beschouwen we als persoonsgegevens omdat er een kans is dat er gegevens in zitten die herleidbaar zijn naar personen. Bijzondere persoonsgegevens genieten een extra bescherming. Daarom behandelen we alle chatlogs en bestanden die vanuit de 112App ontstaan zijn en verwerkt door de Ambulancediscipline als bijzondere persoonsgegevens. Daarop zijn de AVG en de UAVG van toepassing, maar daarnaast ook nog bescherming van medische gegevens conform de Wgbo.

Bij de ambulancedienst hanteert de centralist het medisch beroepsgeheim. Het delen van informatie uit de chat, ook richting kladblok, vereist dan ook uitdrukkelijk een handeling van de centralist, conform Artikel 8 van het convenant. De centralist kan zo zelf uitvoering geven aan de bescherming van medische gegevens. Omdat deze situaties vallen binnen de bestaande regels van doelbinding is het niet nodig om toestemming te vragen aan de melder voor verwerking van deze gegevens.

De 112App Back-end houdt gedurende een 112App-sessie een chat log bij in een database. Na afloop van de sessie slaat GMS de volledige chat log op mij de meldingsgegevens. De 112App Back-end vernietigt de chat log na afloop van de sessie, zodat de chat alleen in GMS is opgeslagen. De privacy-issues van GMS zijn in deze analyse niet meegenomen omdat wijzigingen aan GMS tbv privacy buiten scope van het 112App project zijn. Het 112App project wijzigt bij voorkeur niets aan GMS.

Bestanden die de melder uploadt via de 112App worden opgeslagen in een mediaserver bij de Politie. GMS slaat een URL op die verwijst naar dit bestand om het nodeloos kopiëren van grote bestanden te voorkomen. Nog niet duidelijk is hoe de afscherming van bestanden in de mediaserver is geregeld. Om verwerking van onveilige informatie (virussen, malware, e.d.) te voorkomen, scant het SOC alle binnenkomende verkeer, inclusief de geüploade bestanden en chat logs, op ongerechtigheden.

Niet-meldingsrelevante gegevens

Er kunnen situaties ontstaan waarin persoonsgegevens verwerkt worden die niet nodig zijn voor het verlenen van acute hulp in een noodsituatie. Zo kan het gebeuren dat er medische gegevens in de chat worden opgenomen die niet noodzakelijk zijn voor het verlenen van acute hulp in een noodsituatie. Voor zulke gegevens zou de centralist aan de melder moeten vragen of opslag akkoord is. Echter, dat is niet werkbaar, want dan zou de centralist de gegevens moeten beoordelen en selectief moeten opslaan. We behandelen de hele chat log dan ook als persoonsgegevens, inclusief eventuele niet-meldingsrelevante gegevens. Zo kunnen we voorkomen dat elke chatlog “gekuist” moet worden van niet-meldingsrelevante gegevens.