Risico Analyse 112 App

Kwartier Informatie Beveiliging
10.2.e / 10.2.e / 10 2 e

Concept

Versie 0.2

Versie datum 9 november 2020

Rubricering Politie Intern

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	28-10-2020	Eerste opzet n.a.v. vragen en antwoorden, ntake en workshop	
0.2	09-11-2020		

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1	29-10-2020	10.2.e , 10 2 e	10.2.e en Quality Assurance LMS
0.2	09-11-2020	10.2.e , 10.2.e , 10.2 e , 10 2 e	Adviseurs en 10.2.e Team RMIB, en Integrale Beveiligings Coördinatie MDC

Review commentaar

Versie	Wanneer	Wie	Functie
0.1	05-11-2020	10.2.e	Lead architect 10.2.g

Met opmerkingen [A1]: Functie controleren

Participanten Risicoanalyse

Wie	Functie / Afdeling
10 2 e	Projectleider 112 app
10 2 e	Project 112 app
10 2 e	Project 112 app
10 2 e	Project 112 app
10 2 e	Project 112 app
10 2 e	IB adviseur Kwartier IB
10 2 e	IB adviseur Kwartier IB
10 2 e	IB adviseur Kwartier IB

Rubricering

Toelichting voor gebruik van rubricering
Deze code is verplicht voor ICT documenten

Het actuele document is van 2015 en staat op intranet. Met de zoekfunctie onder 'rubriceringsregeling Politie 2015'.
http://intranet.politie.local/zoeken?query=rubriceringsregeling+2015&sortBy=none
Deze informatie is naar eigen inzicht te verwijderen.

Inhoudsopgave

Samenvatting en advies

Door de politie is een 112 app ontwikkeld. Met behulp van deze 112 app kunnen burgers noodmeldingen plaatsen bij de gemeenschappelijke meldkamers. De 112 app voorziet in eerste instantie over de functionaliteiten: locatiebepaling, chat en het uploaden van foto en video bestanden naar de meldkamer.

Dit advies heeft betrekking op de onderdelen die binnen de scope (zie 1.3. Scope) vallen van dit onderzoek. Tijdens de risico analyse zijn als belangrijkste aandachtpunten benoemd:

- Het gebruik van de nieuwe technieken (app, multimedia, enz.) is mogelijk onvoldoende geborgd in de bestaande wet- en regelgeving rondom de 112 toepassing;
- Contracten met betrokken leveranciers/dienstverleners bieden mogelijk onvoldoende dekking voor de risico's ten aanzien van het gebruik van de nieuwe technieken en functionaliteiten van de 112 app (app, chat, multimedia, enz.);
- Voor bestanden waarop mogelijk een bewaartermijn vanuit specifieke wetgeving van toepassing is, zijn aanvullende handelingen van de centralist noodzakelijk om aan deze bewaartermijn te kunnen voldoen;
- Logging en monitoring is nog niet ingeregeld m.b.t. de 112app. Daardoor wordt niet voldaan aan wettelijke kaders en de eisen die worden gesteld vanuit de BIO;
- Het projectteam neemt aan dat de geldende richtlijnen voor een 112 gesprek (audio), 1-op-1 kunnen worden toegepast op de 112 app chat gesprekken. Door de verschillende vorm (audio of getypte tekst) en de verschillende wijze van opslag (voicelogger of in GMS) worden risico's mogelijk onvoldoende afgedekt

Een volledig overzicht van alle geïnventariseerde risico’s is weergegeven in hoofdstuk 4

Om de belangrijkste risico’s te mitigeren zijn tijdens de risico analyse de volgende maatregelen benoemd:

- Controleer of het gebruik van de 112 app keten in overeenstemming is met wet- en regelgeving en de afspraken in het Landelijk Convenant Gegevensverwerking Meldkamers;
- Controleer of bestaande contracten met de betrokken leveranciers/dienstverleners voldoende dekking bieden voor het gebruik van de 112 app keten en pas deze aan waar dat noodzakelijk is. Sluit met nieuwe partijen contracten en verwerkingsovereenkomsten af;
- Onderzoek of er technische mogelijkheden zijn waardoor de wettelijke bewaartermijn die van toepassing is, automatisch wordt bewaakt;
- Richt de logging en monitoring in conform geldende beleidskaders;
- Onderzoek of de vertrouwelijkheid en integriteit van de chat data en de foto- en videobestanden voldoende gewaarborgd zijn.

Een volledig overzicht van alle geadviseerde maatregelen is weergegeven in hoofdstuk 4.

1. Inleiding

1.1. Doelstellingen

Het doel van de uitgevoerde risicoanalyse (RA) is het inzichtelijk maken van mogelijke risico's. Een risico is een gebeurtenis die op kan treden en die een bedreiging vormt voor het behalen van een doelstelling. Op strategisch niveau zijn de volgende doelstellingen geformuleerd:

1. *Wij realiseren continuïteit van ICT dienstverlening;*
2. *Wij maken het mogelijk dat ICT voorzieningen toekomstbestendig, snel en wendbaar worden ingezet;*
3. *Wij zorgen voor betaalbare en betrouwbare ICT voorzieningen;*
4. *Wij handelen met het perspectief van de eindgebruiker voor ogen;*
5. *Wij zorgen voor professionele en trotse medewerkers.*

Naast het voldoen aan deze strategische doelstellingen moet ook worden voldaan aan de wettelijke kaders en interne beleidsrichtlijnen. De risico's die in deze RA worden beschreven zijn dus gebeurtenissen die het behalen van deze doelstellingen, of daaraan afgeleide doelstellingen, bedreigen.

1.2. Onderzoeksvraag

Het project 112 Appketen heeft het Team Risicomanagement van het Kwartier Informatiebeveiliging verzocht om een risicoanalyse uit te voeren op de door het project op te leveren voorzieningen.
Concreet houdt dit in:

- Keten brede toetsing van de beveiligingsmaatregelen die van toepassing zijn op de applicatie 1-1-2 app
- Toetsing naleving AVG in zake applicatie 1-1-2 app

1.3. Scope

De 112 app voor de smartphone is een uitbreiding op de bestaande diensten voor 112 telefoongesprekken (spraak) en de Advanced Mobile Location (AML) voor de Gemeenschappelijke Meldkamers.

De volgende onderdelen vallen volledig binnen de scope van deze risico analyse:

- Informatie beveiligingsmaatregelen ter bescherming van de (persoons)gegevens t.a.v. het gebruik van de 112app;
- De informatie beveiligingsaspecten met betrekking tot de ontwikkeling van de 112 app;
- De 112 App front-end bij 10.2.g ;
- De 112 app backend op de LMS infrastructuur;
- De chat functionaliteit in de 112 app;
- De upload functionaliteit in de 112 app (foto en video).

Van de volgende onderdelen vallen de koppelvlakken met de 112 app backend binnen de scope van dit onderzoek (donkergroen in figuur 1):

- De koppeling met de GMS Web services;
- De koppeling met GMS.

De volgende onderdelen vallen **buiten** de scope van dit onderzoek:

- Inhoudelijke privacy aspecten;
- De 112 spraak infrastructuur van KPN;
- De AML infrastructuur bij 10.2.g ;
- De interne infrastructuur bij politie en LMS achter de 112 App Backend voor de verwerking van de data van de 112 app in het Geïntegreerd Meldkamer Systeem (GMS). Met uitzondering van genoemde koppelingen.
- Toekomstige ontwikkelingen in de 112 app.

Van deze bestaande onderdelen is geen onderzoek gedaan of aan de geldende richtlijnen wordt voldaan. Voor toekomstige ontwikkelingen van de 112 app kan een aanvullende risico analyse noodzakelijk zijn.

1.4. Verantwoordelijkheden

De functionarissen verantwoordelijk voor de informatieverwerking binnen de 112 app zijn dienstenmanager Rob Dignum en directeur Jan van Loosbroek.

1.5. Leeswijzer

In hoofdstuk 2 wordt met een situatiebeschrijving de werking van de app toegelicht, compleet met gegevens, techniek, logging en beheer.
In hoofdstuk 3 behandelt de IB uitgangspunten wat betreft wet en regelgeving, BIV normering en rubricering
Hoofdstuk 4 bevat de geconstateerde risico's en de voorgestelde maatregelen om de risico's te mitigeren.

2. Situatiebeschrijving

De politie heeft een 112 app ontwikkeld welke gratis beschikbaar wordt gesteld aan alle burgers via de gebruikelijke openbare kanalen(Google Playstore en Apple App store).

De 112 app is bedoeld als ondersteuning aan het 112 telefoongesprek. Via de app kan de burger in contact komen met een centralist van de gemeenschappelijke meldkamer om een noodmelding te plaatsen. Met de app kan onder meer via chat (“Real Time Tekst”) met de meldkamer worden gecommuniceerd en foto en video materiaal worden geüpload. Door een vertaalfunctie is de app ook geschikt voor mensen die de Nederlandse taal niet machtig zijn.
Door deze extra functionaliteiten kan de centralist ervoor kiezen om een 112 gesprek bij aanvang(in verband met functiebeperking van de melder) of op een later moment via chat te voeren.

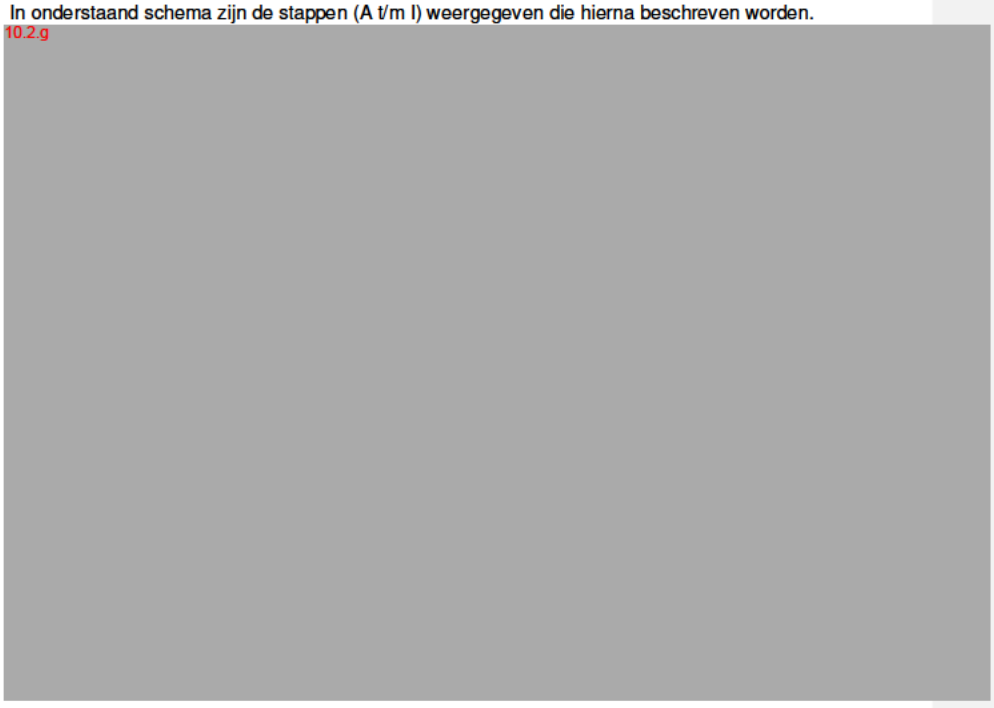
Op dit moment vindt de doorverwijzing vanuit de 112 app naar de betreffende meldkamer en discipline handmatig plaats door de afdeling DL112 van de Landelijke Eenheid (LE). In de toekomst zal het doorverwijzen automatisch plaatsvinden op basis van een algoritme.

2.1. Processen

Tijdens de installatie van de 112 app software op de telefoon van de burger wordt gevraagd om het opgegeven telefoonnummer te bevestigen via SMS authenticatie. Ook wordt gevraagd om akkoord te gaan met de toestemmingen die noodzakelijk zijn voor de werking van de app. Na installatie en akkoord verklaring met de voorwaarden kan met behulp van de app een noodmelding worden geplaatst.

In onderstaand schema zijn de stappen (A t/m I) weergegeven die hierna beschreven worden.

10.2.g



A) **112 Bellen**: Een burger zet met behulp van zijn smartphone een telefoongesprek op via de bestaande spraakinfrastructuur van het 112 noodnummer. Dit gesprek kan zowel vanuit de normale belfunctie van de mobiele telefoon als vanuit de 112 app worden gevoerd.

B) **AML versturen:** Het operating systeem van het toestel start de ingebouwde AML functie voor het versturen van een SMS locatiebericht.

C) **112 app verbinden:** Over de dataverbinding worden de gegevens (telefoonnummer, geo-locatie, roepnaam, wel/geen communicatiebeperking) naar de 112 backend verzonden.

D) **DO112 informeren**: Het 112 telefoongesprek wordt door de Centrale Poort applicatie bij KPN aangeboden aan de Landelijke 112 centrale in Driebergen. De centralist van deze centrale kan zien of de 112 app is gebruikt. Op basis van de meegezonden geo-locatie gegevens bepaalt de Meldkamer Locatie Service naar welke meldkamer het 112 gesprek moet worden doorgeschakeld.

E) **Doorverbinden naar meldkamer:** Na controle van het telefoonnummer (CLI gegevens en de ingevoerde gegevens in de 112 app) wordt het 112 telefoongesprek handmatig doorverbonden aan de aangegeven discipline van de beoogde meldkamer. Opm.: In een volgende release van de 112 app software kan deze doorverbinding automatisch plaatsvinden.

F) **Intake meldkamer**: Na binnenkomst van het 112 gesprek op de beoogde meldkamer wordt in het GMS automatisch een nieuwe melding aangemaakt en wordt de melding door de centralist van de gekozen discipline in behandeling genomen.

G) **Gebruik extra functies:** De centralist kan tijdens het 112 gesprek gebruik maken van extra functies van de 112app.

- De centralist kan via een chat client (Service H) de chat functie (Service I) aanbieden aan de melder. De centralist wordt tijdens de chat sessie ondersteund met behulp van een aantal standaard vragen. Indien de melder een buitenlandse taal spreekt, dan wordt naast de originele getypte tekst ook een vertaling van deze tekst weergegeven in de chat sessie.
- Daarnaast kan de centralist de mogelijkheid voor het uploaden van bestanden (Service G) aanbieden en activeren.

H) **Chat client Service**

I) **Chatfunctie aanbieden aan de melder**

De centralist kan stukken tekst uit de chat in GMS kladblok zetten d.m.v. kopieren & plakken. Ook wordt de integrale chat sessie na afloop van het 112 gesprek in de vorm van een chat log in het GMS kladblok opgeslagen als deel van de melding. Op dit moment gebeurt dit nog in het historisch kladblok maar dit is niet toegestaan omdat dit, vergelijkbaar met de voicelog van een 112 gesprek, niet vrij te benaderen informatie is.

De centralist kan verzoeken om een upload van foto/video. In de eerste release van de 112 app wordt als upload server gebruik gemaakt van dezelfde server als politie.nl maar wel in een aparte container. De link naar het geüploade bestand verschijnt als link in het GMS kladblok, bij aanklikken opent het bestand in een browser. De URL naar de upload is alleen te benaderen binnen de meldkameromgeving. Het bestand wordt 7 dagen bewaard, en daarna verwijderd. De centralist kan het bestand op twee manieren aan de discipline verstrekken: door de link te kopiëren of door het bestand te downloaden op de kantooromgeving. 10.2.g werkt aan een beter beveiligde versie in een volgende release– een afzonderlijke mediaserver voor de LMS.

Voor de vertaling van chat teksten wordt gebruik gemaakt van Google Translate. Op dit moment bestaat hiervoor geen contract. Het uitgangspunt is dat alleen de tekst die vertaald moet worden wordt uitgewisseld. Er vindt geen opslag geen analyse en geen nabewerking plaats door Google. Hiervoor wordt betaald per verzoek, deze betalingen zijn inzichtelijk in een dashboard. De API(Application Programming Interface) key die hiervoor wordt gebruikt is beveiligd, en in beheer bij het Systems Team.

2.2. Gegevens

De gegevens die worden verwerkt bij het gebruik van de 112 app zijn:

- **Bij installatie van de 112 app**:
  - Mobiel telefoonnummer
  - (roep)naam
  - moedertaal
  - wel/niet functiebeperking

  Deze gegevens worden op de smartphone opgeslagen en bij het plaatsen van een noodmelding via de 112 app verzonden naar de 112 app backend.

Bij het plaatsen van een noodmelding worden naast de opgeslagen gegevens de volgende gegevens verzonden:

- **Locatie gegevens**
  De locatiegegevens afkomstig vanuit de 112 app worden via het https protocol verzonden naar de backend van de 112 app.
- **Chat gesprek**
  Dit is getypte tekst. Op grond van de ingestelde moedertaal bij installatie van de 112 app wordt bepaald of vertaling van de ingevoerde tekst via de Google vertaalservice noodzakelijk is.
- **Foto- en video bestand**
  Dit zijn foto en video bestanden eventueel voorzien van meta data. Deze bestanden worden opgeslagen op een (media) server binnen de backend van de 112 app.
- **Metadata van de foto- en video bestanden**
  Metagegevens van de foto- en video bestanden worden, voor zover relevant, in het GMS opgeslagen. De metadata wordt als een onlosmakelijk deel van het bestand bewaard.

Overzicht van de gegevens die gebruikt worden voor de verwerking met behulp van de 112 app.

Type gegeven	I	G	B	Toelichting
Telefoonnummer	X	X		Het telefoonnummer wordt geverifieerd middels SMS
Roepnaam	X	X		Wordt getoond op het moment van gebruik van de app
Moedertaal	X	X		Bepaalt of vertaling van de chat noodzakelijk is
Communicatie beperking	X	X	X	Is te selecteren door het plaatsen van een vinkje in de app.
Locatie		X		Bij gebruik van de app wordt de geo-locatie verzonden
Chat gesprek		X	O	De getypte tekst door burger en centralist
Foto- / videobestanden		X	O	De bestanden die worden geüpload door de burger
Metadata		X		

(I=Installatie G=Gebruik B=Bijzonder persoonsgegeven AVG O=Opmerking)

Met opmerkingen [A2]: Is dit correct? Of is dit achtergrond info?

Door het projectteam van de 112 app wordt aangegeven dat de inhoudelijke gegevens in de 112 front end en in de 112 backend gedurende zeer korte tijd bewaard blijven. De wettelijke bewaartermijn van deze gegevens is gewaarborgd in de bestaande meldkamer systemen waarmee deze gegevens worden gedeeld.

Bewaartermijn

Het project geeft aan dat voor het bewaren van het chat gesprek dezelfde regels worden gehanteerd als de regels die gelden voor de voicelogging van het 112 gesprek. Het chat-verkeer(in- en uitgaande berichten) wordt in de vorm van een integrale chat-sessie opgeslagen in GMS als deel van de melding. De 112App Back-end vernietigt de chat na afloop van de sessie, zodat de chat alleen in GMS is

opgeslagen. De autorisatie wordt op precies dezelfde manier ingericht als meldingen die via een 112 gesprek in GMS zij vastgelegd.

Verder wordt aangegeven dat de veiligheid dat bijvoorbeeld medische data niet met andere disciplines wordt gedeeld is daarmee precies zo groot als die bij andere meldingen.

2.3. Techniek

Voor een overzicht van de 112 keten, de structuur van de back end, van de 112 app en de koppelingen naar de diverse systemen, wordt verwezen naar de grafische weergave in bijlage 1.

Op basis van de verstrekte informatie worden de onderstaande (technische) stappen onderkend, daar waar dat van toepassing is wordt aangegeven of de stap buiten scope valt.

1. De 112app kan gebruikt worden op de besturingssystemen Android en IOS.
2. Een melding in het GMS wordt automatisch aangemaakt volgens het bestaande mechanisme voor 112 meldingen. (buiten scope)
3. De locatiegegevens van de melder worden ook met behulp van AML berichten (SMS) via 10.2.[redacted] aangeleverd. Het AML traject via 10.2.g [redacted] valt buiten de scope van deze risico analyse. (buiten scope)
4. Door de 112 app worden ook locatiegegevens van de melder verzonden via het https protocol.
5. De 112 app backend draait op het Web Application Hosting(WAH)-platform op servers van 10.2.g [redacted]. Dit platform is een bestaand platform dat reeds door de politie gebruikt wordt. (buiten scope)
6. De chat-client draait binnen de politie infrastructuur.
7. Het platform waarop de chat client draait zijn de bestaande GMS servers in RC3 van de Politie. Van deze bestaande servers wordt aangenomen dat zij voldoen aan de voorwaarden zoals gesteld in de uitvoeringsregelingen van de Dienst ICT. (buiten scope)
8. Elk 112 app-chat gesprek is een unieke sessie. Voor elke sessie wordt een unieke URL gecreëerd die verwijst naar een “pagina” op de Webbased Chat Client (een van de 112 app Services op het WAH bij 10.2.g [redacted]). Op die “pagina” kan de centralist in de browser van zijn GMS werkstation communiceren met de melder via de 112 app. *Opmerking IB: niet duidelijk hoe de vertaal optie werkt.*
9. De socket time parameters van de chatsessie zijn zo ingesteld dat na het beëindigen van het gesprek de chat conversatie weer kan worden opgepakt
10. De centralist ziet de unieke URL op het moment dat deze via de GMS client aan hem of haar wordt aangeboden via een aanklikbare hyperlink in het kladblok bericht dat de centralist ontvangt. De unieke URL is zodanig samengesteld dat de kans op het raden van de URL is te verwaarlozen.
11. De informatie in de chat wordt d.m.v. data encryptie m.b.v. SSL getransporteerd, waarbij de inhoud alleen voor de deelnemers zichtbaar is.
12. De geüploade bestanden worden beperkte tijd (7 dagen)bewaard en niet gearchiveerd door de infrastructuur waaruit de 112 app-keten is opgebouwd. De opslag is alleen bedoeld voor het technisch bewaren van de upload. Binnen deze beperkte tijd worden de bestanden beschikbaar gesteld aan de centralist om de bestanden te gebruiken voor de verdere verwerking in de primaire informatiesystemen van de eigen discipline.
13. In een later stadium kunnen (nood)voorzieningen van derden aansluiten op de 112 app. (buiten scope)

2.4. Technische protocollen

Het is onbekend van welke protocollen gebruik wordt gemaakt. Het project heeft aangegeven dat in het architectuurdocument van de 112 app een hoofdstuk zal worden opgenomen waarin alle security ontwerpkeuzes worden gedocumenteerd.

2.5. Beheer

Het technisch beheer van de 112 app omgeving is deels belegd bij de Dienst ICT van de politie, deels bij het Meldkamer Diensten Centrum(MDC) en deels bij 10.2.g , die het platform beheert waarop de 112 backend gehost wordt. De levering van de WAH dienst wordt bewaakt door Politiediensten Centrum, Dienst ICT Productiehuis, Servicelijn 10.2.g Digitaal Politie Contact(DPC). De LMS en het MDC nemen de functionele dienst 112APP (app met backend services en connectiviteit) af van de afdeling Servicelijn Connect van het DPC.

Het is de voorlopige aanname dat de ontwikkeling en het applicatiebeheer van de 112 app wordt uitgevoerd door het 10.2.g van het Productiehuis van de politie. Afhankelijk van strategische keuzes van het 10.2.g kan hier in de toekomst verandering in komen. Het beheer is nog niet ingeregeld en dus nog niet definitief belegd.

Op dit moment is een bestand met standaard vragen t.b.v. de chat cliënt de enige component voor functioneel beheer. De verwachting is dat in latere releases van de 112 app door meer functionaliteit ook meer functionele beheertaken bij zullen komen. De functioneel beheerstaken zijn nog niet belegd.

2.6. Technische Logging

De logging van de chat sessies die bij 10.2.g worden gegenereerd worden aangeboden aan de Dienst ICT van de politie.

Van de 112 app wordt van een sessie tussen de burger en de centralist de volgende gegevens vastgelegd:

- De starttijd
- De eindtijd
- sessie-Id

Deze logging wordt gebruikt om te onderzoeken of de werking van de functies in technische zin correct zijn uitgevoerd en of de processen technisch gezien foutloos zijn verlopen.

Voor de technische logging wordt het opstellen van nader beleid overwogen. In ieder geval wordt deze logging mede gebruikt voor actieve monitoring door het Security Operations Centre (SOC), door het Meldkamer Monitoring Centre (MMC) en door andere technische systeembeheer partijen binnen de IV-keten van de politie.

Wet- en regelgeving logging 112 app

Door de wetgeving die van toepassing is op de logging op de 112app worden verschillende bewaartermijnen gesteld. De Telecommunicatiewet stelt ten aanzien van het bewaren van aangewezen gegevens ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven een termijn van 6 of 12 maanden. De WPG stelt een bewaartermijn van 5 jaar en de WGBO stelt een termijn van 15 jaar indien medische gegevens in de logging verwerkt is.

Vanuit een expertgroep binnen het Cyber Security project bij de LMS is een beleidsrichtlijn opgesteld met betrekking tot logging. Deze richtlijn is nog niet door het management van de LMS bekrachtigd. Voor nu worden de afspraken gehanteerd zoals gemaakt in het Landelijk Convenant Gegevensverwerking Meldkamers.

De logging kan op verzoek van het Ministerie van Justitie en Veiligheid of in opdracht van de Veiligheidsregio worden opgevraagd, gelijk aan de voice logging van 112 gesprekken en andere bronnen. Bijvoorbeeld in het geval van een onderzoek naar het verloop van een ernstig incident waarbij het proces van hulpverlening moet worden geëvalueerd.

2.7. Contracten

De dienstverlening ten behoeve van de 112app wordt gebaseerd op bestaande contracten met de betrokken leveranciers van het 112 platform. Deze contracten zijn in het verleden afgesloten voor de bestaande 112 functionaliteiten voor het transporteren van spraak, Calling Line Identifier (CLI) gegevens en locatie gegevens (AML). LMS contracteert alleen zelf wat niet door de PDC/DICT gecontracteerd wordt, o.a. KPN voor 112-telefonie en de Centrale Poort toepassing. LMS contracteert intern op basis van OLA's met bijvoorbeeld Servicelijn Connect met DICT. In het kader van de in beheer name moeten SLA's, (DNO's) nog worden afgerond.

De politie heeft geen contract afgesloten met Google voor het gebruik van de diensten van Google Translate. Op dit moment wordt dit verder onderzocht. Medische gegegevens worden ook door Google vertaald. Het is niet bekend of er een extra waarborg is voor de beveiliging van deze gegevens.

Op dit moment loopt een DPIA vanuit het ministerie van Justitie en Veiligheid op Google diensten om de privacy risico's van gegevensverwerkingen in kaart te brengen. De uitkomsten hiervan worden dit najaar verwacht.

3. Uitgangspunten IB

3.1. Wet en Regelgeving

Op de 112 omgeving is de Wet Beveiliging Netwerk- en Informatiesystemen (WBNI / EU NIB richtlijn) van toepassing.

Het 112 telefoongesprek is in eerste instantie een aannamegesprek waarin wordt bepaald of het gesprek moet worden doorverbonden naar de politie, de Koninklijke Marechaussee (KMar), de brandweer of naar de ambulancediensten. Persoonsgegevens die tijdens dit 112 triage gesprek worden uitgewisseld vallen onder de Algemene Verordening Gegevensbescherming (AVG). Na het doorverbinden van het telefoongesprek naar één van de disciplines in de gemeenschappelijke meldkamer is op de informatie die daarna wordt uitgewisseld de wetgeving van toepassing waaraan de afhandelende discipline moet voldoen(NEN7510).Het doorschakelen van een 112 gesprek, ondersteund door het gebruik van de 112app, vindt op dezelfde wijze plaats.

Op het moment dat het selecteren en doorverbinden naar een discipline automatisch plaatsvindt, kan een aanvullend risico analyse noodzakelijk zijn.

Bij gebruik van de 112 app kan naast een algemene 112 optie, de keuze worden gemaakt bij welke discipline de burger zijn noodmelding wil plaatsen. Vanaf de start van het contact met de centralist is de wetgeving van toepassing waaraan die discipline in de gemeenschappelijke meldkamer moet voldoen.

Voor de disciplines is de volgende wetgeving van toepassing:

Politie	Wet Politie Gegevens (WPG)
KMar	Wet Politie Gegevens (WPG)
Brandweer	Algemene Verordening Gegevensbescherming (AVG)
Ambulancedienst	Algemene Verordening Gegevensbescherming (AVG)
	Wet Geneeskundige Behandel Overeenkomst (WGBO/BIG)

Wetgeving op het gebied van informatiebeveiliging van toepassing is WGBO en NEN 7510, 7713 vergelijkbaar met ISO. WBNI van toepassing op 10.2.g (hoge beschikbaarheid) en niet op het netwerk. Indien in de toekomst het meldkamer domein als vitale sector wordt aangewezen dan valt het gehele 112 domein hieronder, inclusief de generieke infrastructuur van de meldkamers.

3.2. Jurisprudentie

Uit een uitspraak van de Hoge Raad van 7 maart 2017 (ECLI:NL:PHR:2017:564)[1] blijkt dat alle informatie (gesproken woord, getypte tekst, foto- en video bestanden) die door een 112 melder met een centralist van de ambulancedienst wordt gedeeld, onderdeel is van het medisch dossier en valt onder het medisch beroepsgeheim.

3.3. Landelijk convenant

Binnen de multidisciplinaire meldkameromgeving wordt informatie tussen de verschillende partijen met elkaar gedeeld. In het “Landelijk convenant gegevensverwerking meldkamers” zijn afspraken vastgelegd met betrekking tot de gezamenlijke verantwoordelijkheden die de convenantpartners hebben ten aanzien van de gegevensverwerking op de meldkamer. In hoofdstuk vijf van dit convenant zijn artikelen opgenomen met betrekking tot Informatiebeveiliging.

[1] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:PHR:2017:564

3.4. BIO en addendum politie

Tot nu toe heeft het project nog geen strijdigheden met de BIO en het politie addendum waargenomen. Er moet nog worden geverifieerd bij de teams hoeverre de 112 applicatie bij het beleidsstuk aansluit.

3.5. BIV normering 112 app

Het project 112 app is uitgegaan van de volgende BIV normering:

- Beschikbaarheid: de 1-1-2 telefonie is maximaal beschikbaar en de 112App draait alleen op een onderliggend 1-1-2 telefonie gesprek. Als de 112App-keten (of een deel ervan) uitvalt, gaat 1-1-2 telefonie gewoon door, dus in die zin heeft de 112App een BIV-categorie van B=2.
- Integriteit: geen specifieke of bijzondere eisen. Dus: integriteit net als elke andere app. BIV-categorie I=1
- Veiligheid: de eisen van Dep-V. BIV-categorie V=1

De besluitvorming over de BIV normering moet nog plaatsvinden door de stuurgroep van het project 112 app.

3.6. Rubricering gegevens

Voor de 112 app worden de maatregelen gehanteerd die passen bij klasse Groen, politie intern.

Indien de politie als gekozen discipline de gemelde gegevens van de burger verder zelf verwerkt, dan classificeert de politie deze gegevens als klasse Rood(politie geheim) of hoger, en is het aan de politie (i.c. de operationele eenheden/DROC's) om dit goed te regelen. Binnen het meldkamer domein worden de noodhulpgegevens dan wel "afgeschermd" voor andere disciplines (onderdeel van GMS functionaliteit)

Deze rubriceringsniveaus zijn niet vastgesteld. De stuurgroep van het project 112 app. besluitvorming moet hierover nog een besluit nemen.

3.7. Privacy

Een GEB is momenteel nog in ontwikkeling, onder regie van de Integrale Beveiliging Functionaris van het MDC, 10.2.e . De bestaande GEB voor 112 wordt aangepast door de 112App hieraan toe te voegen.

Het is niet duidelijk hoe het proces is in geval van een beveiligingsincident/datalek.

3.8. Pentest

Het uitvoeren van een penetratie test (pentest) gestart. Rapportage zullen in december 2020 beschikbaar komen.

4. Risico’s

Tijdens deze risicoanalyse is gekeken naar risico’s ten aanzien van de informatiebeveiligingsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).
Dit betekent nadrukkelijk niet dat deze analyse een volledig beeld geeft van bijvoorbeeld alle mogelijke project en organisatie risico’s.

In de bijgeleverde tabel “overzicht risicoacceptatie 112 app” staan de geïdentificeerde risico’s in combinatie met geadviseerde mitigerende maatregelen.

In bijlage 2 is een toelichting van de BIV aspecten opgenomen samen met een tabel over de kwalificatie van de risico’s voor en na de geadviseerde maatregelen.

Bijlage 1: 112 Keten en 112 app Backend structuur

Bijlage 2:

(A)BIV

Kenmerk: **Afhankelijkheid**	
Definitie: Afhankelijkheid betreft het belang van informatie voor het uitvoeren van een proces.	
Kernvraag: • Welke informatie is onmisbaar voor het uitvoeren van het proces? • Om het proces door te laten gaan, wat is daar minimaal voor nodig en welke gegevens zijn daarvoor nodig? • … en heb je alternatieven als je die informatie onverhoopt moet missen?	
Niveaus:	
Aanvullend	Deze informatie bevestigt andere bronnen binnen het werkproces, informatie zal niet direct gemist worden.
Nuttig	Deze informatie ondersteunt het werkproces, informatie zal gemist worden. Het is wel mogelijk tijdelijk door te werken zonder de informatie. Het beschikbaar zijn van de informatie heeft echter wel een positieve invloed op de kwaliteit, efficiëntie, effectiviteit en kosten van het proces.
Noodzakelijk	Deze informatie is de pilaar waarop het werkproces rust. Informatie zal direct gemist worden, doorwerken zonder deze informatie betekent een gevoelige terugval in of uitval van het proces.

Kenmerk: **Beschikbaarheid**	
Definitie: Beschikbaarheid betreft het op het juiste moment toegankelijk zijn van informatie voor geautoriseerde gebruikers.	
Kernvraag: • Wat gebeurt er als de informatie niet beschikbaar is? • Wat gebeurt er als de onderliggende ICT-systemen of informatie niet beschikbaar is. • Heb je alternatieven of kan het probleem in het werk opgevangen worden en hoe moeilijk is dat? • Hoe ernstig is het als de informatie op moment X niet te verkrijgen is? En binnen welk termijn moet die informatie wel voorhanden zijn?	
Niveaus:	
Best effort	Er worden geen specifieke garanties voor dit werkproces gegeven over de toegang tot informatie. Dat wil zeggen: er wordt akkoord gegaan met datgene wat door de uitvoerende diensten geboden wordt.
Laag	Een mindere mate van garantie tot de toegang van de informatie is geaccepteerd. Het business proces is minder beïnvloed door uitval en kan een tijdelijke onderbreking opvangen.
Midden	Er dient een zekere mate van toegang tot de informatie gegarandeerd te worden. Uitval kan het business proces verstoren, de impact hiervan is behoorlijk maar te overzien.
Hoog	Er is een hoge mate van toegang tot de informatie gewenst. Uitval zou het business proces ernstig beïnvloeden, en de impact is kritiek.

Kenmerk: **Integriteit**	
Definitie: Integriteit betreft het vertrouwen dat een gegeven de juiste weergave is van de werkelijkheid en niet ongeoorloofd of onopgemerkt is veranderd.	
Kernvraag: • Hoe erg is het als de informatie niet juist is? • In hoeverre vertrouwt men erop dat de informatie correct is en niet ongemerkt gewijzigd is? • Wat gebeurt er als blijkt dat de gegevens mogelijk gewijzigd zijn? • Voor welke informatie is de integriteit essentieel voor het uitvoeren van het proces?	
Niveaus:	
Aannemelijk	De juistheid en volledigheid van de informatie wordt gegarandeerd door de professionaliteit van de collega's. Er is geen noodzaak aanvullende maatregelen te treffen om de juistheid en volledigheid te garanderen. Er is geen reden om aan te nemen dat de informatie onjuist of onvolledig is en er is geen reden om aan te nemen dat de informatie onbevoegd is gewijzigd.
Gecontroleerd	Juistheid en volledigheid zijn conform procedures, dan wel algemene professionaliteit, gecontroleerd. Er vindt continu controle op (onbevoegde) wijzigingen plaats en deze is ook reproduceerbaar
Onomstotelijk aantoonbaar	De integriteit van de informatie is van een zodanig niveau dat deze voldoet aan de eisen van dossierstukken*. **Er is hier gekozen om de term processtukken te wijzigen in dossierstukken, aangezien processtukken in de Wet-definitie zich beperkt tot stukken in belang van een rechtszitting (MVT, 'Wetboek van Strafvordering' Artikel 149a, tweede lid).*

Kenmerk:

Vertrouwelijkheid

Definitie:

Vertrouwelijkheid betreft de waarborg dat uitsluitend de juiste personen toegang hebben tot de desbetreffende informatie.

Kernvraag:

- Wat gaat er mis als onbevoegden toegang hebben tot de informatie?
- In welke mate moet erop toegezien worden dat de informatie alleen ter beschikking komt aan de juiste persoon en wat zijn de consequenties als die ter beschikking komt bij de verkeerde persoon?
- Welke zorgen heb je als de informatie breder toegankelijk wordt?
- Wat is de consequentie als jouw gegevens bij het grote publiek bekend wordt?
- Welke informatie zou niet bij welke groep/persoon mogen komen en wat zou er dan mis kunnen gaan?

Niveaus		**Rubricerings-regeling**
Niet Vertrouwelijk	**Geen tot zeer geringe schade**	
Politie Intern	**Nadelig voor betrokkenen**	
Politie Confidentieel	**Schade voor betrokkenen**	
Politie Geheim	**Ernstige schade voor betrokkenen**	
Politie Zeer Geheim	**Zeer ernstige schade voor betrokkenen**	

Kwalificeerbaarheid van de Kans en Impact

Kans / Frequentie	
Kwalitatief	*Kwantitatief*
Zeer Klein (ZK)	groter dan 5 jaar
Klein (K)	eens in de 5 jaar
Middel (M)	jaarlijks
Groot (G)	maandelijks
Zeer Groot (ZG)	wekelijks

Impact		
Kwalitatief	*Aspect*	*Kwantitatief*
Verwaarloosbaar (V)	**Beschikbaarheid**	Verwaarloosbaar.
	Schade	Verwaarloosbaar
	Exclusiviteit	Betreft openbare informatie.
	Escalatie	Geen.
Minimaal (Min)	**Beschikbaarheid**	Incidenteel maar de beschikbaarheid blijft binnen de afspraak (SLA).
	Schade	Schending van privacy van personen, doordat naam, adres en/of andere gevoelige gegevens openbaar worden, danwel het bekend worden van gegevens, waardoor de uitvoering van de politietaak kan worden aangetast en waarvan de gevolgen lastig zijn te herstellen.
	Exclusiviteit	'Politie Intern'
	Escalatie	Verantwoordelijke specialist wordt ter verantwoording gevraagd.
Gemiddeld (Mid)	**Beschikbaarheid**	Structureel maar de beschikbaarheid blijft binnen de afspraak (SLA).
	Schade	Openbaarmaking van gegevens, waardoor de uitoefening van de dienstverlening en/of taken van de politie, de ketenpartners en/of in het partnerdomein van de politie zodanig in gevaar komen, dat de gevolgen daarvan nauwelijks herstelbaar zullen zijn.
	Exclusiviteit	'Politie Zeer Vertrouwelijk'
	Escalatie	Verantwoordelijke diensteigenaar wordt ter verantwoording gevraagd.
Maximaal (Max)	**Beschikbaarheid**	Structureel en de beschikbaarheid loopt buiten de afspraak (SLA).
	Schade	Openbaarmaking van gegevens, waardoor de uitoefening van de taken van de politie zodanig in gevaar komen, dat deze onherstelbaar zullen zijn.
	Exclusiviteit	'Politie Geheim'
	Escalatie	Verantwoordelijke hoofdcommissaris wordt ter verantwoording gevraagd.
Catastrofaal (C)	**Beschikbaarheid**	Structureel en meerdere services / diensten zijn voor lange tijd niet meer bruikbaar.
	Schade	Openbaarmaking van gegevens, waardoor de uitoefening van de taken van de politie zodanig in gevaar komen, dat deze onherstelbaar zullen zijn en mensenlevens in het geding zijn (infiltranten, informanten en beschermde getuigen).
	Exclusiviteit	'Politie Zeer Geheim'
	Escalatie	Verantwoordelijke minister wordt ter verantwoording gevraagd.