GEB (gegevens beschermingseffect beoordeling) 1-1-2

<aanvulling titel>

10.2.e

Concept

Versie 1.3

Versie datum 12 november 2020

Rubricering Politie intern

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.

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	09-03-2018	Eerste versie, opgesteld t.b.v. Doorontwikkeling 1-1-2	
0.2	08-04-2018	Reviewopmerkingen d.d. 08-04-2018 Rob Dignum verwerkt	
0.3	16-10-2018	AML toegevoegd, hoofdstuk 4 ingevuld	
0.4	13-11-2018	GEB DO 112 gewijzigd in GEB 112; reviewcommentaar Rob Dignum, Marieke Ackerman op v0.3 verwerkt	
0.5	30-11-2018	Reviewopmerkingen 10.2.e op v0.4 verwerkt; toelichting op gebruik GMS webservice voor AML opgenomen; afbeeldingen met gegevensstromen toegevoegd in 1.3, beveiliging van verbindingen toegevoegd in hoofdstuk 4.	
1.0	04-12-2018	Finale reviewopmerkingen 10.2.e, 10.2.e verwerkt.	
1.1	18-02-2019	Google heeft een opt-out functie voor de burger toegevoegd aan de AML functionaliteit	
1.2	30-09-2019	AML functie voor IPhone actief. Paragrafen 1.1.6 en 1.2 hierop aangepast.	
1.3	04-11-2020	112 App toegevoegd	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1	09-03-2018	Intern MDC	
0.2	08-04-2018	Intern MDC	
0.3	16-10-2018	Commissie Gegevensverwerking meldkamerconvenant 10.2.e 10.2.e	 Dienstenmanager MDC Adviseur LMS
0.4	13-11-2018	10.2.e 10.2.e 10.2.e	Dienstenmanager MDC Adviseur LMS Privacyfunctionaris
0.5	30-11-2018	10.2.e 10.2.e	Dienstenmanager MDC Adviseur LMS
1.0	04-12-2018	10.2.e 10.2.e 10.2.e 10.2.e 10.2.e	Dienstenmanager MDC Adviseur LMS Privacyfunctionaris Sectorhoofd MDC Portefeuillehouder LMS
1.1	18-02-2019	10.2.e 10.2.e 10.2.e 10.2.e 10.2.e	Dienstenmanager MDC Adviseur LMS Privacyfunctionaris Sectorhoofd MDC Portefeuillehouder LMS
1.2	30-09-2019	10.2.e	Dienstenmanager MDC

		10.2.e	Adviseur LMS
		10.2.e	Privacyfunctionaris
		10.2.e	CIO LMS

Accordering

Functie: Portefeuillehouder LMS

Naam: Handtekening:

Datum:

Inhoudsopgave

1. Beschrijving kenmerken gegevensverwerking

1.1. Voorstel

Conform het Besluit 1-1-2 alarmcentrales is de Korpschef aangewezen als beheerder van de alarmnummers voor publieke diensten, bedoeld in artikel 11.10, eerste lid, van de Telecommunicatiewet. De korpschef is dus verantwoordelijk voor het beheer van de 1-1-2 alarmcentrale.

Naar aanleiding van enkele storingen in de 1-1-2 keten in 2012 is door de Inspectie VenJ een onderzoek uitgevoerd en zijn hieraan conclusies en voorgestelde verbetermaatregelen gekoppeld (1-1-2 onder de loep, Inspectie VenJ, maart 2013). In zijn beleidsreactie hierop heeft de minister van VenJ aangegeven verbetermaatregelen te treffen (Reactie op het rapport 1-1-2 onder de loep, Ministerie van Veiligheid en Justitie, 12 mei 2013, kenmerk 381281).

Onderdeel van die maatregelen zijn het onder eenduidige sturing brengen van het beheer van de 1-1-2 keten, het aanpassen van de systemen en infrastructuur, en het volledig uitbesteden van beheer en onderhoud van systemen en infrastructuur aan KPN. Dit wordt gerealiseerd door het programma Doorontwikkeling 1-1-2. Het resultaat van dit programma zou medio 2018 operationeel worden, dit is verschoven naar medio 2019.

Ter voorbereiding op de (nog niet vastgestelde) European Electronics Communications Code (EECC), die naar verwachting rond 2020 van kracht wordt en verplicht tot de invoering van 'handset derived location information', is de implementatie van AML (Advanced Mobile Location) gerealiseerd.

1.1.1. 1-1-2 Alarmoproep via mobiele telefonie

Noodoproepen van personen worden via hun mobile network operator (KPN/Vodafone/T-Mobile/Tele2[1]) en terminating provider KPN doorgerouteerd naar de 1-1-2 alarmcentrale. Het CLI (Calling Line Identification) wordt hierbij doorgegeven. Bij mobiele oproepen waarbij de CLI ontbreekt (b.v. bij SIMloze oproepen of in geval van roaming) wordt het IMEI doorgegeven. Tegelijkertijd worden door de mobile network operators de bijbehorende locatiegegevens (op basis van mastlocaties) verstrekt.

1.1.2. 1-1-2 Alarmoproep via vaste telefonie

Noodoproepen van personen worden via hun telefonieaanbieder en terminating provider KPN doorgerouteerd naar de 1-1-2 alarmcentrale. Hierbij wordt het CLI (Calling Line Identification) doorgegeven.

1.1.3. 1-1-2 Alarmoproep via eSMS

eSMS noodoproepen van personen worden via hun telefonieaanbieder en terminating provider KPN doorgerouteerd naar de 1-1-2 alarmcentrale.

1.1.4. E-Call

E-Call is de afkorting van 'Emergency call' (noodoproep) en staat voor een Europa-breed, op satellieten gebaseerd noodoproepsysteem in voertuigen. De E-Call noodoproep maakt gebruik van mobiele telefonie om een telefoonverbinding tot stand te brengen met het 112 alarmnummer na een ongeval. Daarbij wordt gebruik gemaakt van de door de ITU toegekende nummerreeksen voor eCall modems (zie ITU Operational Bulletin No. 1155-11 (http://www.itu.int/pub/T-SP-OB.1155-2018/en). Via de spraakverbinding verzendt het elektronische oproepsysteem in het voertuig gegevens met relevante informatie over de locatie van het ongeval (op basis van positiebepaling per satelliet) en het type voertuig.
Het boordsysteem bestaat uit een simkaart-achtige mobiele chip. Sensoren detecteren wanneer de auto hard wordt geraakt of wanneer de airbags worden geactiveerd. In dit geval stuurt het systeem een noodoproep en wordt de locatie van de auto doorgeven. Naast zo'n automatisch geactiveerde noodoproep kan deze ook met een knop handmatig worden ingeschakeld door de inzittende(n). Dankzij deze dataoverdracht is het mogelijk om de reddingsdiensten van extra informatie te voorzien.
Als een E-Call automatisch of handmatig wordt vastgesteld, worden de volgende gegevens eenmalig verzonden: noodoproeptype, chassisnummer van de auto, type brandstof, tijd, GPS-positie, voertuigrichting, de twee voorgaande GPS-posities en het aantal passagiers. De fabrikanten kunnen ook maximaal 94 bytes aan fabrikant-specifieke

[1] Tele2 maakt voor 1-1-2 oproepen gebruik van het mobiele netwerk van T-Mobile. In §1.3 wordt Tele2 daarom niet genoemd als network operator.

informatie toevoegen, bijvoorbeeld met betrekking tot het uitschakelen van de spanning van elektrische of hybride auto's.

Er zijn 2 varianten van eCall:

- Pan European eCall; Dit gratis systeem maakt direct verbinding met de 112-centrale. Alle nieuwe types personenauto's en lichte bedrijfsvoertuigen die na 1 april 2018 op de markt komen moeten dit systeem aan boord hebben.
- Third Party Service (TPS) eCall. Dit zijn noodoproepsystemen van autofabrikanten die al op de markt zijn. Hierbij gaat de noodoproep naar de alarmcentrale waar het automerk een contract mee heeft. Die gaat na of noodhulp nodig is. In dat geval geeft de alarmcentrale de oproep direct door aan de betreffende meldkamer.

De eigenaar van een auto kan zelf kiezen welke variant wordt gebruikt.

1.1.5. TotalConversation noodoproep

Total Conversation is een wereldwijde standaard die interoperabel functioneert: verschillende soorten en merken hardware en software kunnen via Total Conversation onderling met elkaar communiceren. De richtlijnen voor Total Conversation zijn vastgelegd in nationale en Europese regelgeving en in internationale richtlijnen.
Total Conversation bestaat uit beeld, tekst en geluid. Beeld is voor het aflezen van gebaren, lippen of gezichtsmimiek. Wanneer de tolkgebruikers niet kunnen gebaren of bij moeilijke namen en woorden, dan kunnen ze kiezen voor Real Time Text (RTT). Bij RTT wordt tekst meteen letter voor letter verzonden tijdens het typen, de ontvanger kan deze tekst meteen lezen terwijl het nog geschreven wordt. Geluid kan gebruikt worden als er zelf gesproken en/of geluisterd wordt.
Doven en slechthorenden kunnen een internetverbinding opbouwen met de 112 alarmcentrale vanaf hun computer, tablet of smartphone wanneer daarop de Total Conversation software is geïnstalleerd. Bij oproepen naar de 1-1-2 alarmcentrale wordt nog geen gebruik wordt gemaakt van de functionaliteit "beeld".

Noodoproepen via TotalConversation worden met vermelding van het SIP-adres via het openbare internet ontvangen op de 112 alarmcentrale.

1.1.6. AML (Advanced Mobile Location)

Advanced Mobile Location (AML) is een manier voor de 112 alarmcentrale om automatisch locatie-informatie vanuit een mobiel toestel te ontvangen bij noodoproepen.
Google biedt deze functie op Android telefoons vanaf OS versie 4.0. Google noemt dit Emergency Location Service (ELS). Google biedt de gebruiker van het mobiele toestel een opt-out mogelijkheid voor AML.
Apple levert deze functie op IPhones vanaf iOS versie 13. Apple biedt geen opt-out mogelijkheid.
Google en Apple slaan geen AML informatie op. Het AML bericht wordt ook niet via Google of Apple servers verstuurd. Google en Apple zijn hierdoor noch Verwerkingsverantwoordelijke, noch Verwerker, noch Ontvanger van de persoonsgegevens als bedoeld in de AVG.
In andere Operating systems (OS), zoals Microsoft Windows Mobile, BlackBerry, etc., is gebruik van lokalisatie en het automatisch versturen daarvan bij een noodoproep vooralsnog alleen mogelijk via een App (bron: TNO rapport Advanced Mobile location).

Bron: Google (https://crisisresponse.google/emergencylocationservice/how-it-works/)

Als een persoon (abonnee als bedoeld in artikel 1.1 van de Telecommunicatiewet en Betrokkene als bedoeld in de AVG) 112 belt met een mobiele telefoon, wordt automatisch de precieze locatie van de telefoon aan de 112 alarmcentrale en de benodigde hulpdienst in de regionale meldkamer doorgegeven. Als de locatievoorzieningen op de telefoon uitstaan, worden bij een noodoproep naar 112 automatisch de locatiediensten van het toestel ingeschakeld. Het toestel probeert dan aan de hand van WiFi-signalen en satellietnavigatiesystemen zoals GPS zijn locatie zo precies mogelijk te bepalen[2]. Indien deze niet beschikbaar zijn, gebruikt de mobiele telefoon de gegevens van de GSM-mast waarmee het in verbinding staat. Vervolgens stuurt het de beschikbare locatiegegevens door via SMS naar de SMS broker van de politie voor de 112 alarmcentrale. De locatie informatie wordt in de techniek gekoppeld aan de centralist die het gesprek in behandeling heeft. De SMS'jes worden alleen gestuurd gedurende het gesprek met 112. AML locatie informatie is dan ook aanvullende informatie.

De SMS is een zogenaamde dataSMS en is niet zichtbaar voor de burger in de outbox. De dataSMS wordt verstuurd op dezelfde manier als een gewone SMS volgens het store and forward principe. SMS'jes worden vanuit de mobiele telefoon naar de berichtencentrale (SMSC) van de Mobile Network Operator gestuurd. Deze SMSC slaat het bericht op en poogt (zonodig meerdere keren) het bericht af te leveren bij de SMS broker van politie (CM Telecom). Na een in te stellen tijd (standaard drie dagen) wordt het bericht gewist. In het SMS-systeem bestaat geen prioriteitsmechanisme waarmee aan noodroepen per SMS voorrang kan worden gegeven en is er geen gegarandeerde aflevering van de SMS. Er zijn dus vertragingen mogelijk. Naar verwachting zal er nooit sprake zijn van vertraging, omdat de ontvanger (shortcode politie) altijd aanstaat. De Mobile Network Operators (MNO's) of Mobile Virtual Netwerk Operators (MVNO's) zien de AML informatie in de SMS niet.

Aan de hulpdiensten is gevraagd hoe vaak ze een AML bericht willen ontvangen gedurende het 1-1-2 gesprek, dit is aan te geven bij Google. Dit betreft:

---

[2] Google: With ELS, when a call is made to a configured emergency number, the device automatically activates ELS to send location information. This happens via a high power location request that is registered with the Fused Location Provider. FLP analyses AGPS, cell tower triangulation, Wi-Fi hotspot proximity, Bluetooth, and a variety of sensor data potentially including magnetometer, barometer, and other sensors to derive highly accurate indoor and outdoor location as quickly as possible, with as little power consumption as possible.

- Report First Location: 1 SMS: de eerst beschikbare locatie versturen als die beschikbaar
- Sampling Delta: 1 SMS na 20 seconden
- Reporting delta: elke 60 seconden een update van de locatie

Google geeft aan dat tussen de 5 en 20 seconden een goede locatie beschikbaar is. Er is door de politie en KMar aangegeven dat een incident niet altijd statisch is, maar ook bewegend kan zijn. Daarom is het wenselijk om ook updates te ontvangen en is gekozen voor een reporting delta van elke 60 seconden een bericht.

Bij Apple wordt eenmaal een AML bericht verzonden. In een Apple AML bericht worden IMSI en IMEI deels afgeschermd

Tijdeli ke situatie
Bij de implementatie van AML in Nederland zal de locatieinformatie in eerste instantie alleen naar de regionale meldkamers verstuurd worden (via de GMS Webservice) en pas in tweede instantie ook naar de 1-1-2 alarmcentrale (dit is een wijziging in programma Doorontwikkeling 112 die pas na live-gang van Doorontwikkeling 112 kan worden geïmplementeerd). Hier geldt een afwijkende vorm van verwerking:
De daadwerkelijke noodoproepen worden vanuit de 112 alarmcentrale doorgerouteerd naar (verstrekt aan) de regionale meldkamer van de hulpverleningsdienst(en). De gegevens worden daarbij als melding vastgelegd in GMS.
Alle SMS berichten die worden verstuurd naar shortcode 1662 worden beschouwd als AML bericht en via de SMS broker doorgerouteerd naar de GMS Webservice.
Wanneer een AML bericht kan worden gematcht aan een melding in GMS, wordt de AML informatie toegevoegd aan de GMS melding.
In alle overige gevallen wordt de AML informatie niet doorgerouteerd of gekoppeld aan andere gegevens. Dit geldt dus zowel voor 112 misbruikgesprekken (die worden niet als melding in GMS vastgelegd) als voor SMS berichten die onbedoeld, niet door de AML functionaliteit maar door de betrokkene, zijn verstuurd naar shortcode 1662.

In de tijdelijke situatie vindt ten behoeve van beheer- en verdere ontwikkeldoeleinden analyse plaats van de mate waarin noodoproepen worden voorzien van AML gegevens.
De GMS webservice houdt hiertoe een logbestand bij. Dit bestand wordt elke 24 uur verzonden naar de 112 beheerorganisatie en daar opgeslagen in een datawarehouse. Op de GMS webservice wordt de logging na verzenden verwijderd.
De 112 beheerorganisatie analyseert dagelijks geautomatiseerd de ontvangen loginformatie en genereert beheerrapportages. Van noodoproepen worden de loggegevens in het datawarehouse na 2 maanden de identificerende gegevens verwijderd, van misbruikoproepen na 6 maanden, en van overige oproepen binnen 24 uur. In de beheerrapportages worden geen identificerende gegevens vermeld.

1.1.7. 1-1-2 App

Met 1-1-2 App wordt hier bedoeld: De app voor mobiele Android en iOS toestellen, bedoeld voor noodoproepen, die de Politie/LMS beschikbaar stelt aan het publiek. Vergelijkbare apps van derden vormen nadrukkelijk geen onderdeel van deze GEB.

De 112App is onderdeel van het programma 'Het nieuwe melden' dat is gestart op basis van de uitkomsten van een onderzoek dat TNO heeft uitgevoerd in opdracht van het Ministerie van Justitie en Veiligheid.
Uit vervolgonderzoek door Berenschot in opdracht van het Ministerie van Justitie en Veiligheid blijkt dat burgers behoefte hebben aan een 112App.

De 112App kan alleen worden gebruikt op mobiele telefoons die AML ondersteunen.

Met de 112App verbetert de meldkamer de dienstverlening voor een grotere groep mensen (gehoor- en spraak beperkten, niet-Nederlandstaligen) en breidt de dienstverlening uit met nieuwe middelen (chat, foto's, video's). Daarmee wil LMS de bereikbaarheid verbeteren en oproepen sneller bij de juiste discipline-centralist bezorgen.

De 112App is ook nodig om de 112-keten geschikt te maken voor het aansluiten van andere apps zoals Signcall of KNRM.

Wanneer vanuit de 112App een noodoproep wordt geplaatst realiseert de app het opzetten van een 112 alarmoproep via mobiele telefonie (zie § 1.1.1) inclusief AML (zie § 1.1.6) met parallel daaraan het uitwisselen van informatie door

de app. Aanvullend aan AML worden locatiegegevens door de 112App verstuurd gedurende de 112 oproep indien de locatie wijzigt of indien een nauwkeuriger positie is bepaald.
Een melder die direct 112 belt, terwijl de 112App is geïnstalleerd, kan alsnog de 112App openen om beelden te kunnen uploaden of te chatten.
De 112App draagt bij aan het verkorten van de aannametijd doordat gesprekken naar 112, die gestart zijn vanuit deze app, een discipline keuze bevatten vanuit de melder. In veel gevallen kan het gesprek zonder tussenkomst van een 112-centralist naar een geschikte post worden gerouteerd.
Deze app biedt bovendien extra functionaliteiten zoals het communiceren met tekst en het kunnen opvragen van beelden bij de melder.
De communicatie met tekst is waardevol, bijvoorbeeld in het geval iemand een spraak/hoor beperking heeft. Bovendien kan de getypte tekst vanuit verschillende talen vertaald worden naar het Nederlands, waardoor de communicatie met de centralist extra ondersteund wordt.
Het opvragen van beelden (foto's of korte filmpjes) bij melder kan helpen bij het inzicht krijgen in de incidentlocatie en -omgeving. Daarmee kan vooraf nog betere afstemming van benodigde noodhulpinzet worden bereikt.

Indien gebruik wordt gemaakt van de vertaalfunctie van de chat worden woorden, zinsdelen en hele zinnen naar Google translate verzonden. Met Google is contractueel afgesproken dat Google deze gegevens NIET opslaat en uitsluitend vertaalt. (Is dit inderdaad afgesproken? welke overeenkomst?)

Alle datacommunicatie (met uitzondering van file upload) tussen de app met de centralist vindt plaats met de GMS webserver. File upload vindt plaats van de app naar een upload server in het politienetwerk (buiten GMS om). Een URL wordt door de uploadserver naar de GMS webserver verzonden. Communicatie tussen de app en de GMS weberserver of de uploadserver vindt plaats via het publieke internet.

1.2. Persoonsgegevens

Zoals bij Gegevensverwerkingen wordt toegelicht, wordt voor de afhandeling van noodoproepen naar de 112 alarmcentrale gebruik gemaakt van een keten van infrastructuren en partijen.
Hieronder wordt uitsluitend de gegevensverwerking door de 112 alarmcentrale weergegeven. De verwerkingen door de toeleverende partijen (telefonieaanbieders, internet aanbieders, eCall TSP's, Stichting 10.2.g , 10 2 g , 10.2.g) tot aan het punt van aflevering aan de 112 alarmcentrale, en de verwerkingen door de hulpverleningsdiensten na verstrekking door de 112 alarmcentrale, valt onder de verantwoordelijkheid van de desbetreffende partijen, en wordt hier buiten beschouwing gelaten.[3]

Betrokkene	**Categorie persoonsgegevens**	**Persoonsgegevens**
Personen die gebruik maken van het 112 alarmnummer (zowel via vaste telefonie als mobiele telefonie)	Algemeen	CLI (telefoonnummer), IP-adres Naam, adres, woonplaats, postcode metagegevens gespreksafhandeling (CLI, centralistwerkplek, gespreksduur, doorverbindgegevens) Aard gesprek (hulpverlening, misbruik, prioritair)
	Gevoelig	Locatiegegevens
	Bijzonder - gezondheid, ras, seksuele geaardheid	Kan voorkomen in gesprek en gespreksopname
	Strafrechtelijk	Kan voorkomen in gesprek en gespreksopname
Personen die gebruik maken van eSMS	Algemeen	CLI (telefoonnummer), IP-adres metagegevens gespreksafhandeling (CLI, centralistwerkplek, gespreksduur, doorverbindgegevens) Aard gesprek (hulpverlening, misbruik, prioritair)

[3] Tot het moment van implementatie van de Europese richtlijn COM(2016) 590 in de Telecommunicatiewet wordt AML niet geleverd op basis van wetgeving maar op verzoek van de beheerder 112 alarmcentrale namens de hulpdiensten. Zie § 1.9.1.

	Bijzonder - gezondheid, ras, seksuele geaardheid	Kan voorkomen in gesprek en gespreksopname
	Strafrechtelijk	Kan voorkomen in gesprek en gespreksopname
Aanvullend bij 1-1-2 melding via Smartphone met AML bericht[4]	Algemeen	CLI (telefoonnummer), IMEI-nummer, SIM-kaartnummer (IMSI), cel-, netwerk- en operatorcode[5] [6] Datum en tijd van positiebepaling, verzending en ontvangst van het AML bericht[7]. Volgens AML standaard: https://www.etsi.org/deliver/etsi_tr/103300_103399/103393/01.01.01_60/tr_103393v010101p.pdf"
	Gevoelig	Locatiegegevens (lengte- en breedtegraad, hoogte, verdieping[8], straal / nauwkeurigheid) Volgens AML standaard: https://www.etsi.org/deliver/etsi_tr/103300_103399/103393/01.01.01_60/tr_103393v010101p.pdf"
Auditief beperkte personen die via Total-Conversation gebruik maken van het 112 alarmnummer	Algemeen	SIP-adres Naam, adres, woonplaats metagegevens gespreksafhandeling (SIP-adres, centralistwerkplek, gespreksduur, doorverbindgegevens)
	Bijzonder - gezondheid, ras, seksuele geaardheid	Kan voorkomen in gesprek en gespreksopname
	Strafrechtelijk	Kan voorkomen in gesprek en gespreksopname
Eigenaar en/of inzittende(n) van voertuig dat een eCall noodoproep initieert	Algemeen	IMEI, nummer uit ITU nummerreeks eCall MSD (Minimum set of data zoals gedefinieerd in EN-norm 15722): voertuig locatie informatie, time stamp, voertuigrichting, aantal passagiers met vastgemaakte autogordel, voertuig identificatie nummer (VIN) en andere voor noodhulpdiensten relevante informatie. Eucaris voertuig-gegevens: i) fabrikant (en model, indien beschikbaar); ii) identificatienummer van het voertuig; iii) registratienummer; iv) datum van eerste registratie; v) type brandstof en/of type aandrijving; vi) signalering van diefstal[9]. metagegevens gespreksafhandeling (CLI, centralistwerkplek, gespreksduur, doorverbindgegevens)
	Bijzonder - gezondheid, ras, seksuele geaardheid	Kan voorkomen in gesprek en gespreksopname
	Strafrechtelijk	Kan voorkomen in gesprek en gespreksopname
1-1-2 centralist	Gevoelig - stelselmatige monitoring	metagegevens gespreksafhandeling (CLI, centralistwerkplek, gespreksduur, doorverbindgegevens) Overige gebruikershandelingen Voicelogs van gesprekken
	Gevoelig – accountinfo	Gebruikersnamen, wachtwoorden en/of andere inloggegevens

[4] Pas na live gang van DO112 worden AML gegevens door de 112 alarmcentrale opgeslagen. Voordien worden ze opgeslagen in de GMS Webservice en haar data warehouse. Zie hiervoor de GEB GMS.
[5] IMSI en cel-, netwerk- en operatorcode zijn niet zichtbaar voor de 1-1-2 centralist
[6] In een Apple AML bericht worden IMSI en IMEI deels afgeschermd
[7] Alleen datum en tijd van het bericht zal worden getoond aan de 1-1-2 centralist
[8] Hoogte en verdieping zit wel in de standaard, maar wordt nog niet doorgeven en ook niet gepresenteerd aan de 1-1-2 centralist.
[9] Signalering van diefstal wordt niet door de 112 applicatie getoond aan de 112 centralist, maar wel via GMS doorgegeven aan de hulpverleningsdienst(en).

1-1-2 supervisor, 1-1-2 beheerder	Gevoelig - stelselmatige monitoring	Gebruikershandelingen
	Gevoelig – accountinfo	Gebruikersnamen, wachtwoorden en/of andere inloggegevens
Personen die gebruik maken van de 112App	Algemeen	Via spraakverbinding (mobiele telefonie): CLI (telefoonnummer), IP-adres Naam, adres, woonplaats, postcode metagegevens gespreksafhandeling (CLI, centralistwerkplek, gespreksduur, doorverbindgegevens) Aard gesprek (hulpverlening, misbruik, prioritair) Via app: Naam van de melder, voorkeurstaal chat log
	Gevoelig	Via spraakverbinding (mobiele telefonie): Locatiegegevens AML locatiegegevens Via app: Locatiegegevens
	Bijzonder - gezondheid, ras, seksuele geaardheid	Via spraakverbinding (mobiele telefonie): Kan voorkomen in gesprek en gespreksopname Via app: Indicatie gehoor/spraakbeperking,
	Strafrechtelijk	Via spraakverbinding (mobiele telefonie): Kan voorkomen in gesprek en gespreksopname Via app: Kan voorkomen in chat en chatlog

1.3. Gegevensverwerkingen

Noodoproepen van (voertuigen van) personen worden via hun telefonieaanbieder doorgerouteerd naar de 1-1-2 alarmcentrale. Tegelijkertijd worden door de telefonieaanbieders de bijbehorende locatiegegevens verstrekt (mobiele

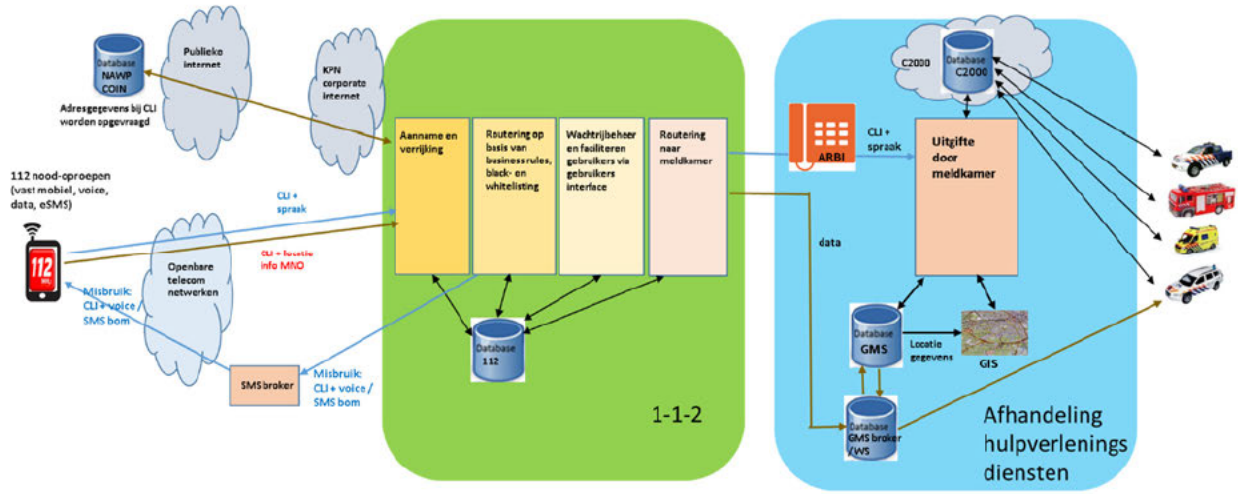
telefonie) of worden op basis van het telefoonnummer de bijbehorende NAW-gegevens opgevraagd in de 110.2.g database. Bij mobiele telefonie zijn de locatiegegevens momenteel gebaseerd op mastgegevens en daarmee indicatief. Na implementatie van AML wordt door het mobiele toestel automatisch de locatie doorgegeven indien 112 wordt gebeld.
De daadwerkelijke noodoproepen worden, verrijkt met informatie, gerouteerd naar de relevante hulpdienst(en) in de meldkamer voor de betreffende regio. Daarbij worden alle relevante gegevens doorgegeven aan GMS (Gemeenschappelijk Meldkamer Systeem).[10]

Bij een eCall worden automatisch aanvullende voertuiggegevens uit de RDW EUCARIS database opgevraagd.
Tevens kan de 112 centralist handmatig, op basis van een kenteken, aanvullende gegevens over een voertuig opvragen in de RDW EUCARIS database. Dit gebeurt in het geval van een "Samaritan call", waar de melder een ongeval van een ander voertuig meldt.
Bij een oproep via TotalConversation wordt het SIP-adres verstrekt, en kan de 1-1-2 centralist aanvullende gegevens opgevragen in de Berengroep database (dit gebeurt niet automatisch).
Voor eSMS en TotalConversation oproepen wordt ook de bemiddeling tussen de beller en de hulpdienst gedaan door de 1-1-2 centralist, waardoor de inhoud van de noodhulpvraag door de 1-1-2 centralist wordt vastgelegd en aan de hulpdienst verstrekt.
Bij een oproep via de 112App wordt door de app een mobiele spraak alarmoproep geïnitieerd (inclusief AML) en worden parallel daaraan gegevens naar GMS verzonden. Ook de chatgegevens worden in GMS opgenomen. Bij uploaden van foto's/filmpjes worden deze op een (niet-GMS) fileserver opgeslagen. De URL's van de foto's/filmpjes worden door de fileserver naar GMS verstuurd. Aanvullend aan de AML-functie worden door de app locatiegegevens voor een langere duur doorgestuurd naar GMS.

Oproepen die zijn gemist worden teruggebeld.
Oproepen die geen daadwerkelijke noodoproepen zijn, worden als zodanig gemarkeerd. Aansluitingen die herhaaldelijk misbruik maken van het alarmnummer kunnen worden bestookt met voice- of SMS bommen.
Ten behoeve van het functioneren van de alarmcentrale worden diverse beheerrapportages gegenereerd

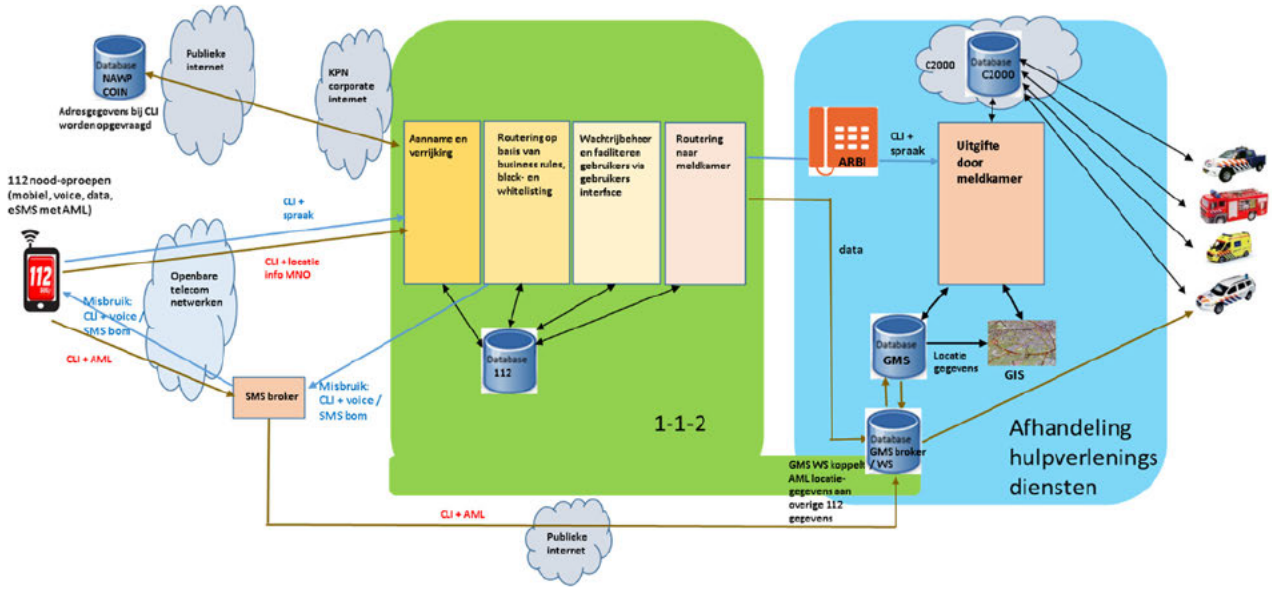
1.3.1. 1-1-2 Alarmoproep via mobiele en vaste telefonie

Zonder AML:

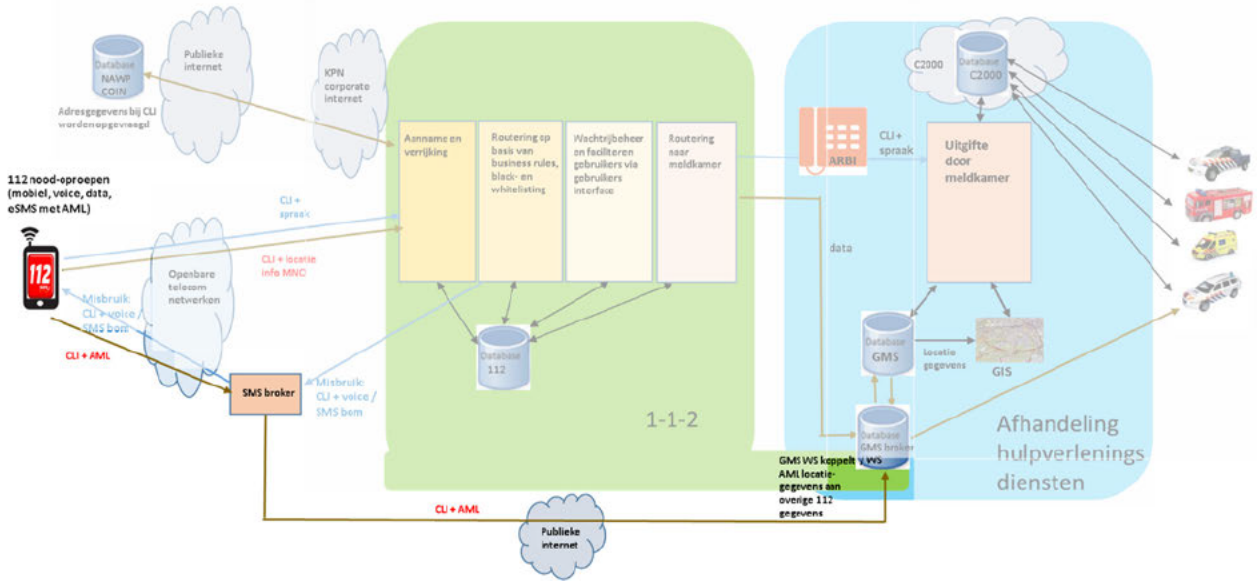


Alarmoproep via mobiele telefonie **met AML**:

[10] Voor AML geldt dat de gegevens binnen komen (via de SMS Broker) bij de GMS Webservice; die stuurt de informatie vervolgens door naar het GMS van de betreffende hulpdienst en (na live gang DO 112) de 1-1-2 alarmcentrale.



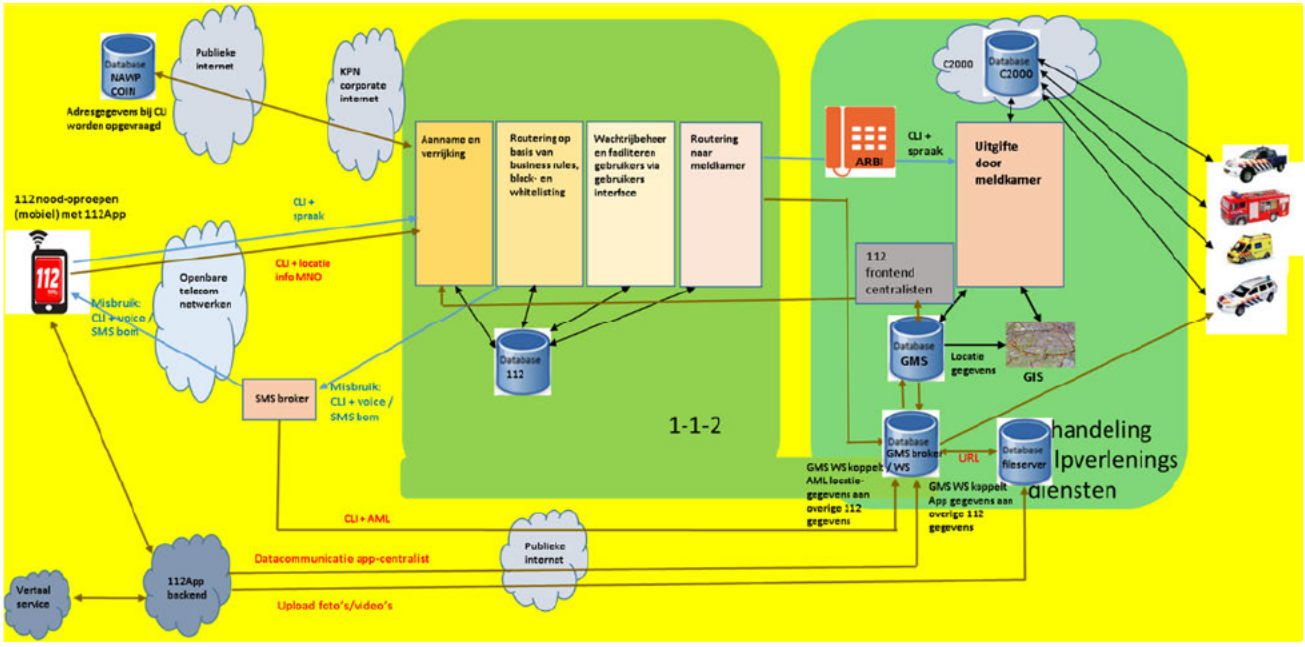
In onderstaande figuur wordt het verschil tussen de situatie met vs zonder AML verduidelijkt.



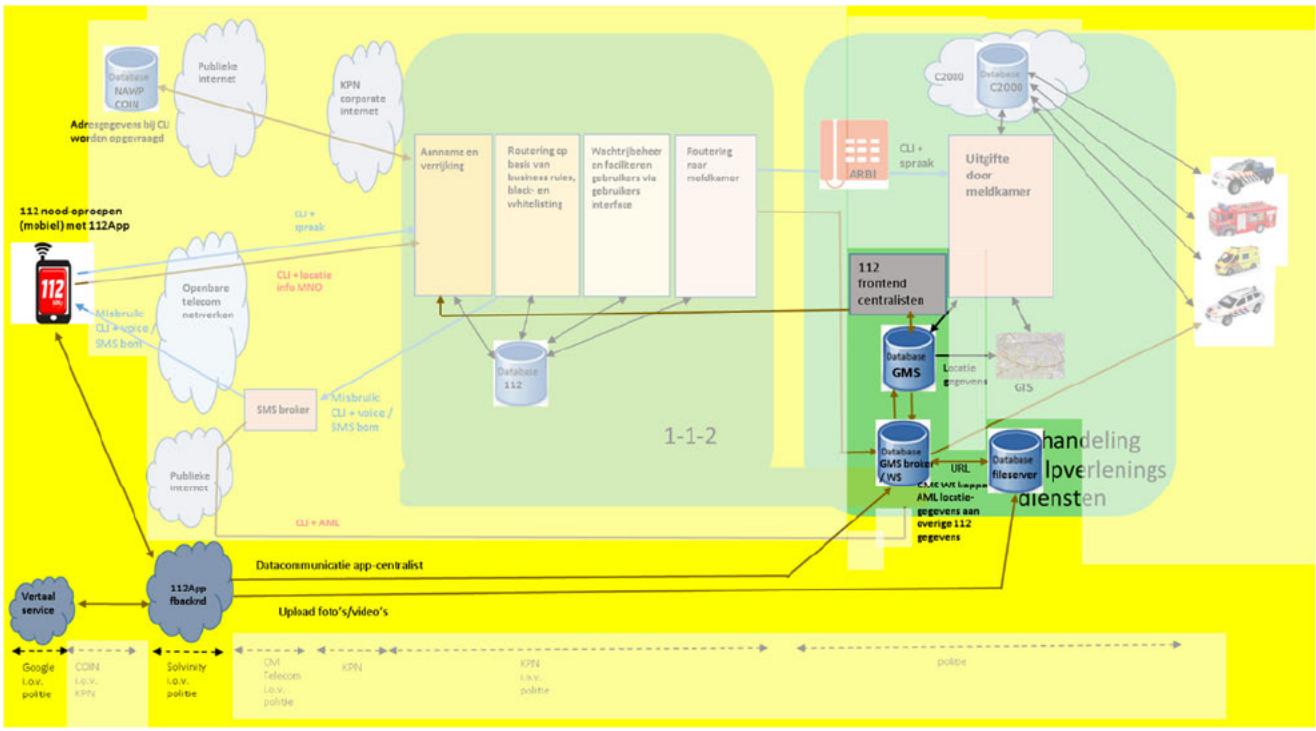
Ontvangen	• Mobiele telefonie: Noodoproepen van personen worden via hun mobile network operator doorgerouteerd naar de 1-1-2 alarmcentrale. Tegelijkertijd worden door de mobile network operators (KPN/Vodafone/T-Mobile) de bijbehorende locatiegegevens verstrekt, alsmede IMSI (International Mobile Subscriber Identity) en IMEI (International Mobile Equipment Identity). De standaard door de MNO verstuurde locatiegegevens zijn gebaseerd op mastlocatie; bij gebruik van AML worden daarnaast locatiegegevens gebaseerd op GPS verstuurd. Dan wordt ook SIMkaartnummer meegestuurd. • Vaste telefonie: Noodoproepen van personen worden via hun telefonieaanbieder en terminating provider KPN doorgerouteerd naar de 1-1-2 alarmcentrale.
Opvragen	De gesprekshistorie van het bellende nummer (CLI) wordt opgevraagd in de 1-1-2 database. De bij het CLI behorende NAW-gegevens worden opgevraagd in de 10.2.g database.
Vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen,	De oproep wordt gerouteerd naar een 1-1-2 centralist met de juiste skill en werkplek. De 1-1-2 centralist heeft de oproep en bijbehorende gegevens nodig voor de uitvoering van zijn taak. De ontvangen gegevens, de metagegevens van de gespreksafhandeling en de gespreksopname (voicelog) worden vastgelegd.

gebruiken, raadplegen, combineren, afschermen	De gespreksopname kan worden beluisterd door de afhandelende 1-1-2 centralist en de 1-1-2 supervisor. Oproepen die geen daadwerkelijke noodoproepen zijn, worden als zodanig gemarkeerd, zodat aansluitingen die herhaaldelijk misbruik maken van het alarmnummer kunnen worden bestookt met voice- of SMS bommen. Ten behoeve van het functioneren van de alarmcentrale worden diverse beheerrapportages gegenereerd. AML locatiegegevens worden via de SMS broker gerouteerd naar de GMS webservice. De GMS webservice analyseert of ontvangen AML locatiegegevens kunnen worden gematched met een door de 112 centralist naar de hulpverleningsdienst doorgerouteerd, en daardoor in GMS vastgelegde, melding. Als dit het geval is worden de AML locatiegegevens toegevoegd aan de melding in GMS.
verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen	Oproepen die daadwerkelijke noodoproepen zijn, worden doorgerouteerd naar de relevante hulpdienst(en) in de meldkamer voor de betreffende regio. Daarbij worden alle relevante gegevens doorgegeven aan GMS. Misbruikgesprekken worden gerapporteerd aan de daartoe aangewezen opsporingsambtenaren. Deze opsporingsambtenaren sporen de beller op, waarschuwen de beller of gaan over tot vervolging. Doel hiervan is het voorkomen van verminderde bereikbaarheid van de 112 alarmcentrale voor daadwerkelijke noodhulpoproepen als gevolg van misbruikgesprekken. Beheerrapportages worden verstrekt aan de procesverantwoordelijken.
wissen of vernietigen	Telecommunicatiewet artikel 11.10, zevende lid, bepaalt de maximale termijn gedurende welke de nummers en gegevens mogen worden bewaard: a. twee maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van een verzoek om hulpverlening in een noodsituatie; b. zes maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van misbruik van een alarmnummer voor publieke diensten; c. 24 uur in alle overige gevallen. Na verloop van deze termijn worden de gegevens automatisch gewist.

1.3.2. 1-1-2 Alarmoproep via 112App



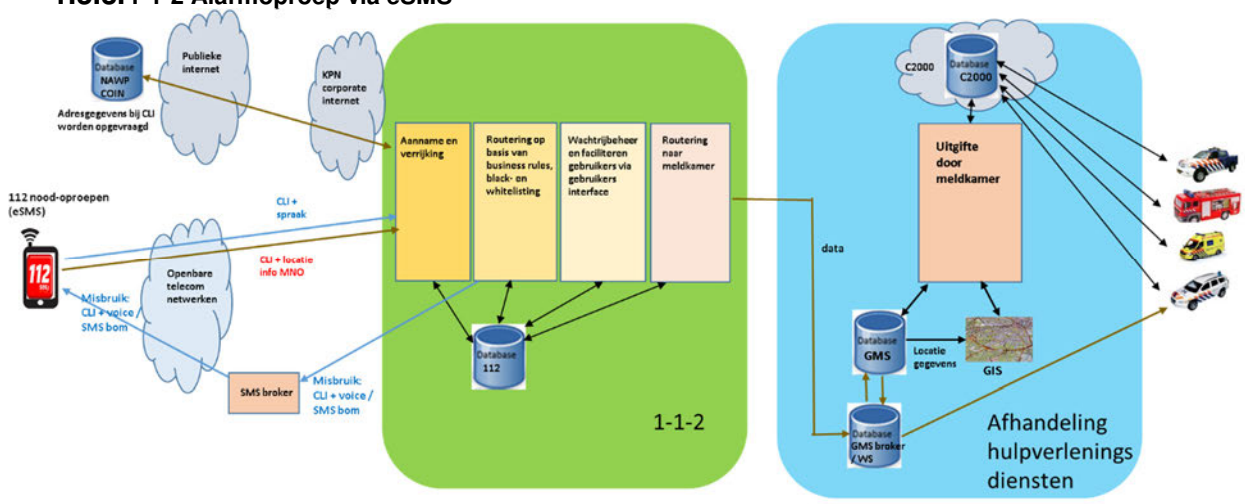
In onderstaande figuur wordt het verschil tussen de situatie met 112App vs alarmoproep via mobiele telefonie met AML verduidelijkt.



Ontvangen	• Mobiele telefonie: Noodoproepen van personen worden via hun mobile network operator doorgerouteerd naar de 1-1-2 alarmcentrale. Tegelijkertijd worden door de mobile network operators (KPN/Vodafone/T-Mobile) de bijbehorende locatiegegevens verstrekt, alsmede IMSI (International Mobile Subscriber Identity) en IMEI (International Mobile Equipment Identity). De standaard door de MNO verstuurde locatiegegevens zijn gebaseerd op mastlocatie; bij gebruik van AML worden daarnaast locatiegegevens gebaseerd op GPS verstuurd. Dan wordt ook SIMkaartnummer meegestuurd. • 112App: Aanvullend aan bovenstaande worden van de app de volgende gegevens ontvangen: Naam, voorkeurstaal, locatiegegevens. Optioneel: chat, foto/video
Opvragen	De gesprekshistorie van het bellende nummer (CLI) wordt opgevraagd in de 1-1-2 database. De bij het CLI behorende NAW-gegevens worden opgevraagd in de 10.2.g database.
Vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, gebruiken, raadplegen, combineren, afschermen	De oproep wordt gerouteerd naar een 1-1-2 centralist met de juiste skill en werkplek. De 1-1-2 centralist heeft de oproep en bijbehorende gegevens nodig voor de uitvoering van zijn taak. De ontvangen gegevens, de metagegevens van de gespreksafhandeling en de gespreksopname (voicelog) worden vastgelegd. De gespreksopname kan worden beluisterd door de afhandelende 1-1-2 centralist en de 1-1-2 supervisor. Oproepen die geen daadwerkelijke noodoproepen zijn, worden als zodanig gemarkeerd, zodat aansluitingen die herhaaldelijk misbruik maken van het alarmnummer kunnen worden bestookt met voice- of SMS bommen. Ten behoeve van het functioneren van de alarmcentrale worden diverse beheerrapportages gegenereerd. AML locatiegegevens worden via de SMS broker gerouteerd naar de GMS webservice. De GMS webservice analyseert of ontvangen AML locatiegegevens kunnen worden gematched met een door de 112 centralist naar de hulpverleningsdienst doorgerouteerd, en daardoor in GMS vastgelegde, melding. Als dit het geval is worden de AML locatiegegevens toegevoegd aan de melding in GMS. Gegevens (m.u.v. foto/video) van de 112App worden via de 112App backend en publiek internet verzonden naar de GMS webservice. De GMS webservice analyseert voor welke meldkamer en hulpdienst de oproep is bestemd en routeert de gegevens naar de betreffende GMS omgeving. Daarnaast routeert de GMS webserver de gegevens via de 112 frontend naar het 112 systeem. Het 112 systeem analyseert of de inkomende

	spraakoproep kan worden gematched met een inkomende 112App oproep en routeert dan het gesprek zonder tussenkomst van een 112 centralist naar de betreffende meldkamer / hulpdienst. De spraakoproep wordt echter gerouteerd naar een 112 centralist indien het oproepende nummer voorkomt op de misbruiklijst, het gesprek wegens drukte niet kan worden gerouteerd naar de beoogde meldkamer of bij calamiteiten. De centralist heeft inzage in de van de 112App ontvangen keuzes en locatiegegevens. De via de 112App ontvangen foto's/video's worden opgeslagen op een uploadserver. De uploadserver stuurt een bericht met de CLI en een URL per foto/video naar de GMS webserver. De webserver analyseert deze berichten en voegt de informatie toe aan de gegevens in GMS.
verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen	Oproepen die daadwerkelijke noodoproepen zijn, worden doorgerouteerd naar de relevante hulpdienst(en) in de meldkamer voor de betreffende regio. Daarbij worden alle relevante gegevens doorgegeven aan GMS. Misbruikgesprekken worden gerapporteerd aan de daartoe aangewezen opsporingsambtenaren. Deze opsporingsambtenaren sporen de beller op, waarschuwen de beller of gaan over tot vervolging. Doel hiervan is het voorkomen van verminderde bereikbaarheid van de 112 alarmcentrale voor daadwerkelijke noodhulpoproepen als gevolg van misbruikgesprekken. Beheerrapportages worden verstrekt aan de procesverantwoordelijken. Indien in de 112App een andere taalvoorkeur dan Nederlands is opgegeven en er gebruik wordt gemaakt van de chatfunctie worden de chatberichten door de 112App backend verzonden naar een vertaalservice (Google translate) en worden de vertaalde berichten verzonden naar de oproepende partij c.q. de centralist. Zowel de 112App backend als de vertaalservice houden geen informatie vast.
wissen of vernietigen	Telecommunicatiewet artikel 11.10, zevende lid, bepaalt de maximale termijn gedurende welke de nummers en gegevens mogen worden bewaard: a. twee maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van een verzoek om hulpverlening in een noodsituatie; b. zes maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van misbruik van een alarmnummer voor publieke diensten; c. 24 uur in alle overige gevallen. Na verloop van deze termijn worden de gegevens automatisch gewist. De van de 112App ontvangen data valt niet onder de werking van de Telecommunicatiewet. Hier worden de bewaartermijnen van GMS gehanteerd. Voor de op de uploadserver opgeslagen foto's/video's wordt een bewaartermijn van ….. gehanteerd.

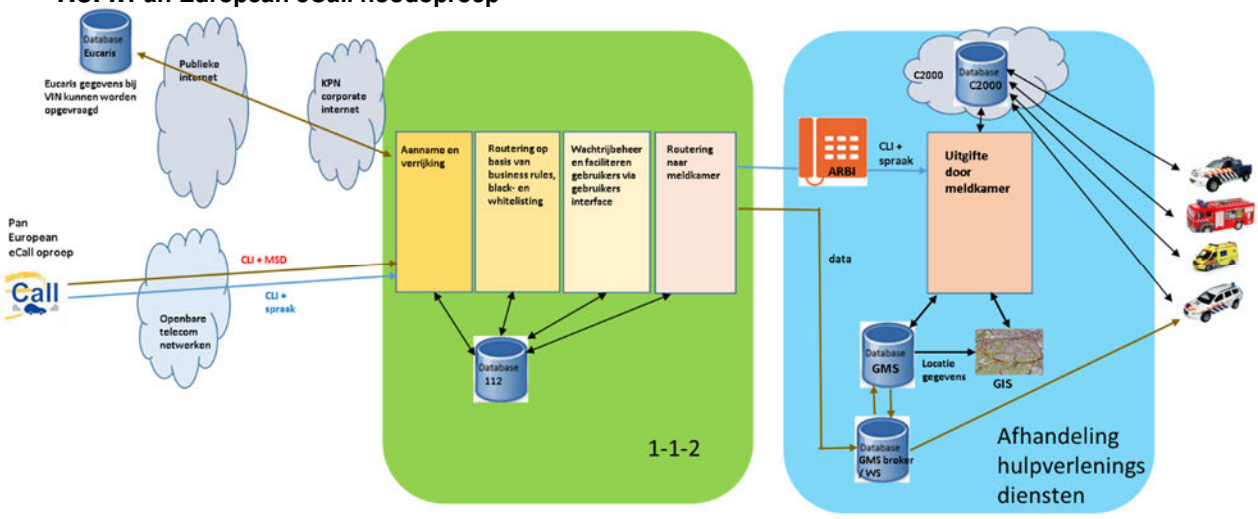
1.3.3. 1-1-2 Alarmoproep via eSMS



Ontvangen	Noodoproepen van personen worden via hun telefonieaanbieder en terminating provider KPN doorgerouteerd naar de 1-1-2 alarmcentrale.

	Voor eSMS oproepen wordt ook de bemiddeling tussen de beller en de hulpdienst gedaan door de 1-1-2 centralist, waardoor de inhoud van de noodhulpvraag (gesprekscontent) wordt ontvangen van de beller.
Opvragen	De gesprekshistorie van het bellende nummer (CLI) wordt opgevraagd in de 1-1-2 database.
Vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, gebruiken, raadplegen, combineren, afschermen	De oproep wordt gerouteerd naar een 1-1-2 centralist met de juiste skill en werkplek. De 1-1-2 centralist heeft de oproep en bijbehorende gegevens nodig voor de uitvoering van zijn taak. De ontvangen gegevens, de metagegevens van de gespreksafhandeling en de uitgewisselde berichten worden vastgelegd. De communicatie kan worden geraadpleegd door de afhandelende 1-1-2 centralist en de 1-1-2 supervisor. Oproepen die geen daadwerkelijke noodoproepen zijn, worden als zodanig gemarkeerd, zodat aansluitingen die herhaaldelijk misbruik maken van het alarmnummer kunnen worden bestookt met voice- of SMS bommen. Ten behoeve van het functioneren van de alarmcentrale worden diverse beheerrapportages gegenereerd.
verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen	Bij oproepen die daadwerkelijke noodoproepen zijn, wordt door de 1-1-2 centralist bemiddeld tussen de melder en de relevante hulpdienst in de meldkamer voor de betreffende regio. Misbruikgesprekken worden gerapporteerd aan de daartoe aangewezen opsporingsambtenaren. Beheerrapportages worden verstrekt aan de procesverantwoordelijken.
wissen of vernietigen	Telecommunicatiewet artikel 11.10, zevende lid, bepaalt de maximale termijn gedurende welke de nummers en gegevens mogen worden bewaard: a. twee maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van een verzoek om hulpverlening in een noodsituatie; b. zes maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van misbruik van een alarmnummer voor publieke diensten; c. 24 uur in alle overige gevallen. Na verloop van deze termijn worden de gegevens automatisch gewist.

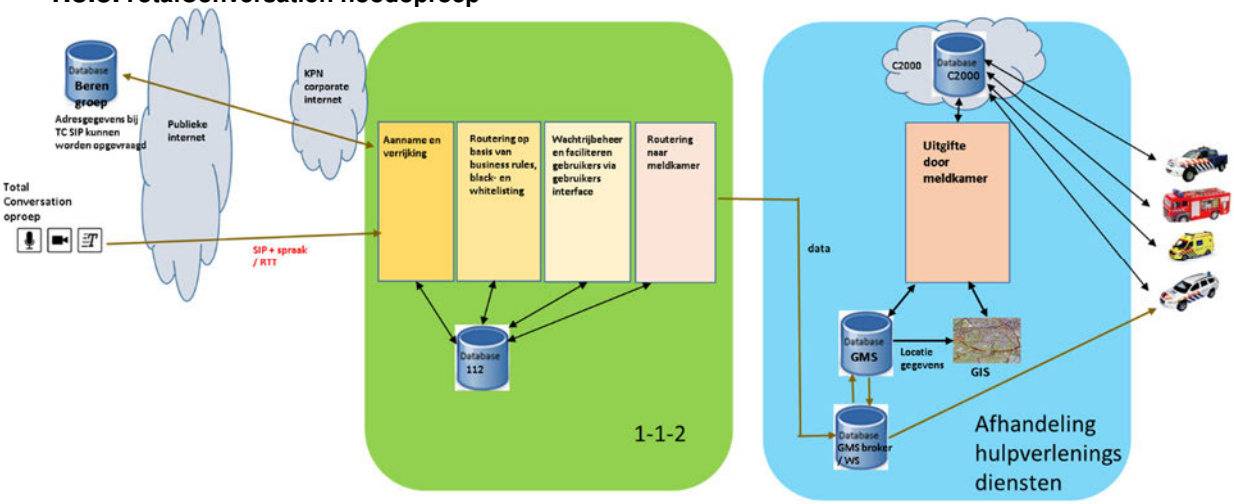
1.3.4. Pan European eCall noodoproep



Ontvangen	Noodoproepen van voertuigen worden door de mobile network operators via terminating provider KPN doorgerouteerd naar de 1-1-2 alarmcentrale. Tegelijkertijd worden door de mobile network operator de locatiegegevens en eCall MSD (Minimum Set of Data) doorgegeven.

Opvragen	Van het in de MSD vermelde voertuig worden automatisch op basis van het VIN (voertuig identificatie nummer), of handmatig op basis van een kenteken (in het geval van een “Samaritan call”), aanvullende gegevens over het voertuig opgevraagd in de RDW EUCARIS database
Vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, gebruiken, raadplegen, combineren, afschermen	De oproep wordt gerouteerd naar een 1-1-2 centralist met de juiste skill en werkplek. De 1-1-2 centralist heeft de oproep en bijbehorende gegevens nodig voor de uitvoering van zijn taak. De ontvangen gegevens, de metagegevens van de gespreksafhandeling en de gespreksopname (voicelog) worden vastgelegd. De gespreksopname kan worden beluisterd door de afhandelende 1-1-2 centralist en de 1-1-2 supervisor. Ten behoeve van het functioneren van de alarmcentrale worden diverse beheerrapportages gegenereerd.
verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen	Oproepen die daadwerkelijke noodoproepen zijn, worden doorgerouteerd naar de relevante hulpdienst in de meldkamer voor de betreffende regio. Daarbij worden alle relevante gegevens doorgegeven aan GMS. Misbruikgesprekken worden gerapporteerd aan de daartoe aangewezen opsporingsambtenaren. Beheerrapportages worden verstrekt aan de procesverantwoordelijken.
wissen of vernietigen	Telecommunicatiewet artikel 11.10, zevende lid, bepaalt de maximale termijn gedurende welke de nummers en gegevens mogen worden bewaard: a. twee maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van een verzoek om hulpverlening in een noodsituatie; b. zes maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van misbruik van een alarmnummer voor publieke diensten; c. 24 uur in alle overige gevallen. Na verloop van deze termijn worden de gegevens automatisch gewist.

1.3.5. TotalConversation noodoproep



Ontvangen	Noodoproepen via TotalConversation worden met vermelding van het SIP-adres via het openbare internet ontvangen. Voor TotalConversation oproepen wordt ook de bemiddeling tussen de beller en de hulpdienst gedaan door de 1-1-2 centralist, waardoor de inhoud van de noodhulpvraag (spraak, tekst, beeld) wordt ontvangen van de beller.
Opvragen	De bij het SIP-adres behorende NAW gegevens kunnen worden opgevraagd in de Berengroep database. De gegevens worden alleen getoond indien de oproeper gebruiker is van de nWise Total Conversation applicatie en toestemming heeft gegeven aan Berengroep om deze gegevens te verstrekken aan de 1-1-2 alarmcentrale.

Vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, gebruiken, raadplegen, combineren, afschermen	De oproep wordt gerouteerd naar een 1-1-2 centralist met de juiste skill en werkplek. De 1-1-2 centralist heeft de oproep en bijbehorende gegevens nodig voor de uitvoering van zijn taak. De ontvangen gegevens, de metagegevens van de gespreksafhandeling en de communicatie (spraak, tekst, beeld) worden vastgelegd. De communicatie kan worden teruggekeken door de afhandelende 1-1-2 centralist en de 1-1-2 supervisor. Ten behoeve van het functioneren van de alarmcentrale worden diverse beheerrapportages gegenereerd.
verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen	Bij oproepen die daadwerkelijke noodoproepen zijn, wordt door de 1-1-2 centralist bemiddeld tussen de melder en de relevante hulpdienst in de meldkamer voor de betreffende regio. Beheerrapportages worden verstrekt aan de procesverantwoordelijken.
wissen of vernietigen	Telecommunicatiewet artikel 11.10, zevende lid, bepaalt de maximale termijn gedurende welke de nummers en gegevens mogen worden bewaard: a. twee maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van een verzoek om hulpverlening in een noodsituatie; b. zes maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van misbruik van een alarmnummer voor publieke diensten; c. 24 uur in alle overige gevallen. Na verloop van deze termijn worden de gegevens automatisch gewist.

1.3.6. Voor de 1-1-2 centralist zichtbare actuele informatie van de oproep

Afhankelijk van het soort oproep is een subset van onderstaande overzicht zichtbaar

- Oproeptype (= Telefonische alarmoproep, eCall, Total Conversation-oproep of eSMS-bericht)
- Tel.nr.: CLI van de beller / voertuig
- IMEI: IMEI van de beller (indien eCall of AML)
- Tijd: datum / starttijd oproep
- Bestemming: door beller aangekozen tel.nr. (DNIS)
- Op witte-lijst: indicatie op Witte-lijst ja/nee[11]
- Reden Witte-lijst: reden dat CLI op de Witte-lijst staat
- Op grijze-lijst: indicatie op Grijze-lijst ja/nee
- Naam: volledige naam van de abonnee
- Adres: volledig adres van de abonnee
- Postcode: postcode van de abonnee
- Woonplaats: woonplaats van de abonnee
- Provider: provider naam waarvan de beller gebruik maakte
- Positie: GPS X-coördinaat ‘latitude’ van de beller (vanuit de Locatie Service)
- Positie: GPS Y-coördinaat ‘longitude’ van de beller (vanuit Locatie Service)
- Positie betrouwbaar: indicator die aangeeft of de doorgegeven positie betrouwbaar is (uit MSD)
- Type voertuig: vertaald naar een label, zoals ‘bus’, ‘passagiersvoertuig’ of ‘vrachtwagen’ (uit MSD)
- VIN: voertuig identificatie nummer (uit MSD)
- Tijdstip van incident (uit MSD)
- Positie: GPS X-coördinaat ‘latitude’ van het voertuig (uit MSD)
- Positie: GPS Y-coördinaat ‘longitude’ van het voertuig (uit MSD)
- Aantal passagiers in het voertuig (uit MSD)
- Land: land waaruit voertuig afkomstig is (EUCARIS)
- Kenteken: kenteken van het voertuig (EUCARIS)

[11] Witte en grijze list wordt toegelicht in § 1.8

- Kleur: kleur van het voertuig (EUCARIS)
- Merk: merkbeschrijving van het voertuig (EUCARIS)
- Type: voertuig typebeschrijving (EUCARIS)
- Brandstof: bestaat uit één of meer brandstof soorten, en worden gescheiden weergegeven door het karakter ‘,’ (EUCARIS)
- Locatiegegevens (lengte- en breedtegraad, straal / nauwkeurigheid)
- Datum en tijd van positiebepaling.

1.3.7. Voor de 1-1-2 centralist zichtbare historische informatie

- Tijd: datum / starttijd oproep
- Centralist: centralist die het contact afgehandeld heeft (volledige naam)
- IMEI: IMEI van de beller
- Misbruik: indicator misbruik (ja / nee)
- Reden misbruik
- Noodhulp: indicator noodhulp (ja / nee)
- Noodhulpdienst: naar welke noodhulpdienst is doorverbonden (organisatie code)
- Opmerking: ingevuld op verschijningsraam ‘doorverbinden’
- GPS X-coördinaat ‘latitude’ (vanuit de Locatie Service)
- GPS Y-coördinaat ‘longitude’ (vanuit de Locatie Service)
- GPS X-coördinaat ‘latitude’ (uit MSD)
- GPS Y-coördinaat ‘longitude’ (uit MSD)
- Transcript: indicator transcript aanwezig (alleen voor oproeptype ‘eSMS’)
- AML locatie[12]

1.3.8. Terugluisteren van voicelogs

Een 1-1-2 centralist kan in zijn nawerktijd via een knop zijn meest recente gesprek terugluisteren. En daarnaast beschikt hij over een functionaliteit om op basis van zoekcriteria gespreksopnames te zoeken en terug te luisteren. Een Senior kan deze gespreksopnames ook exporteren naar een bestand ten behoeve van trainingsdoeleinden, afhandeling van klachten, of verstrekking aan de wettelijke opsporingsinstanties.

1.4. Verwerkingsdoeleinden

- Aannemen van noodoproepen, bemiddelen van bepaalde typen noodoproepen tussen oproeper en benodigde hulpdienst, en verstrekken met het oog op hulpverlening in noodsituaties aan publieke diensten belast met hulpverleningstaken;
- Verstrekken met het oog op bestrijding van misbruik van het alarmnummer voor publieke diensten.
- Analyse van gegevens ten behoeve van beheerdoeleinden.

1.5. Betrokken partijen

Zoals bij Gegevensverwerkingen wordt toegelicht, wordt voor de afhandeling van noodoproepen naar de 112 alarmcentrale gebruik gemaakt van een keten van infrastructuren en partijen.
Hieronder wordt uitsluitend de gegevensverwerking door (en bezien vanuit de optiek van) de 112 alarmcentrale weergegeven. De verwerkingen door de toeleverende partijen (telefonieaanbieders, internet aanbieders, eCall TSP’s, stichting 10.2.g , 10 2 g , 10.2.g) tot aan het punt van aflevering aan de 112 alarmcentrale, en de verwerkingen door de hulpverleningsdiensten na verstrekking door de 112 alarmcentrale, valt onder de verantwoordelijkheid van de desbetreffende partijen, en wordt hier buiten beschouwing gelaten.
Voor AML wordt gebruik gemaakt van de GMS webservice. Hiervoor wordt verwezen naar de GEB GMS.

Rol	Partij, gegevens, toegang tot gegevens door
Verantwoordelijke	De korpschef van politie (opgedragen middels Besluit 1-1-2 alarmcentrales)

[12] Na livegang van DO 112

	Toegang tot de gegevens: 1-1-2 centralisten, supervisors en beheerders; beperkingen op basis van autorisatiemodel
Verwerker	CM Telecom Ontvangt namens politie de AML SMS berichten en stuurt die door naar de GMS webservice. Toegang tot uitsluitend de inhoud van de AML SMS berichten (CLI + tekst) door de daartoe binnen CM Telecom geautoriseerde medewerkers
Verwerker	KPN Toegang tot de gegevens door de daartoe binnen KPN geautoriseerde medewerkers
Verwerker	112App backend: 10.2.g De 112Backend wordt gehost bij 10.2.g . De backend houdt geen gegevens vast. Toegang tot de backend uitsluitend door de daartoe binnen 10.2.g geautoriseerde medewerkers.
Verwerker	112App vertaalservice: Google Bij niet-Nederlandse taalvoorkeur worden chatberichten door de 112App backend aangeboden aan Google translate. Er is contractueel overeengekomen dat Google uitsluitend vertaalt en geen verdere verwerkingen doet. Checken
Subverwerkers KPN	CM Telecom Afhandeling van SMS bommen en voice bommen; SMS centrale voor eSMS. Toegang tot uitsluitend de inhoud van de SMS berichten (CLI + tekst) door de daartoe binnen CM Telecom geautoriseerde medewerkers
	nWise Betreft beheer van de TotalConversation applicatie Toegang tot de via TotalConversation uitgewisselde communicatie door de daartoe binnen nWise geautoriseerde medewerkers
Verstrekkers	Betrokkene (c.q. eCall boordsysteem): inhoud van de communicatie Toegang tot deze informatie door betrokkene, afhandelende 1-1-2 centralist en de 1-1-2 supervisor
	KPN als terminating provider voor telefonie, eCall en eSMS oproepen CLI / IMEI van alle oproepen eCall MSD (Minimum set of data zoals gedefinieerd in EN-norm 15722): voertuig locatie informatie, time stamp, voertuigrichting, aantal passagiers met vastgemaakte autogordel, voertuig identificatie nummer (VIN) en andere voor noodhulpdiensten relevante informatie. Toegang tot de informatie alleen voor daartoe binnen KPN geautoriseerde medewerkers
	Mobile network operators CLI, locatiegegevens Toegang tot informatie door de daartoe geautoriseerde medewerkers
	10.2.g NAW gegevens van bevraagd CLI Toegang tot NAW gegevens door de daartoe geautoriseerde medewerkers
	10.2.g Naam, adres, woonplaats Toegang tot gegevens door de daartoe geautoriseerde medewerkers
	RDW Eucaris voertuig-gegevens van bevraagd VIN of kenteken/landcode: i) fabrikant (en model, indien beschikbaar); ii) identificatienummer van het voertuig; iii) registratienummer; iv) datum van eerste registratie; v) type brandstof en/of type aandrijving; vi) signalering van diefstal. Toegang tot gegevens door de daartoe geautoriseerde RDW medewerkers
Ontvangers	Daadwerkelijke noodoproep: de aangewezen hulpverleningsdiensten (politie, KMar, regionale ambulancevoorziening, regionale brandweer) CLI / IMEI, locatiegegevens, NAW gegevens, eCall MSD en voertuiggegevens Toegang tot gegevens door: meldkamercentralist
	Misbruikoproepen: de in de Telecommunicatiewet aangewezen opsporingsambtenaren (politie, Ministerie van JenV) CLI / IMEI, oproephistorie

	Beheerrapportages: 1-1-2 procesverantwoordelijken

1.6. Belangen bij de gegevensverwerkingen

Melder	Het zo spoedig mogelijk ontvangen van adequate noodhulp
Politie: 112 alarmcentrale (politie)	Voldoen aan de middels Besluit 1-1-2 alarmcentrales opgedragen wettelijke taak.
Politie: dienst ICT / MDC	Leveren van Dienst 112 aan de 112 alarmcentrale Leveren van dienst GMS Webservice aan de 112 alarmcentrale voor verwerking van AML berichten
Hulpverleningsdiensten (politie, KMar, regionale ambulancevoorziening en/of regionale brandweer)	Leveren van noodhulp aan betrokkenen conform de opgedragen wettelijke taken
Telefonie aanbieders	Aanbieden van noodoproepen van abonnees met bijbehorende gegevens aan de 112 alarmcentrale conform wet- en regelgeving Aanbieden van gegevens van noodoproepen aan de 112 alarmcentrale conform overeengekomen uitvoeringsafspraken
KPN	Leverancier van de 112 functionaliteit op basis van overeenkomst met politie
Pan European eCall	Aanbieden van noodoproepen van abonnees met bijbehorende gegevens aan de 112 alarmcentrale conform wet- en regelgeving
10.2.g	Verstrekken van NAW gegevens behorende bij oproepende CLI's op basis van uitvoeringsovereenkomst met KPN
10.2.g	Verstrekken van NAW gegevens behorende bij TotalConversation oproepen op basis van overeenkomst met politie
RDW	Verstrekker van Eucaris gegevens op basis van wetgeving en verstrekkingsovereenkomst met politie
10.2.g	SMS centrale voor eSMS en SMS-bommen op basis van overeenkomst met KPN SMS broker voor AML op basis van overeenkomst met politie
nWise	Leverancier van en onderhoudspartij voor TotalConversation op basis van overeenkomst met KPN
10.2.g	Leverancier van 112App backend dienst op basis van overeenkomst met politie
Google	Leverancier van 112App vertaalservice. Op basis van overeenkomst met politie? Niet duidelijk

1.7. Verwerkingslocaties

Locatie	Verwerking
Nederland	Gespreksafhandeling 1-1-2 centralisten (locatie Landelijke eenheid van Politie) Vastlegging en bewerking (KPN datacenters) Verstrekking aan meldkamers (meldkamerlocaties) Verstrekking aan opsporingsambtenaren Verstrekking door telefonieproviders Verstrekking door 10.2.g Verstrekking door RDW Verzending door 10.2.g
Duitsland	Verstrekking door 10.2.g
Zweden	Onderhoud aan TotalConversation applicatie
Binnen EU (land niet gespecificeerd)	Verwerking 112App backend 10.2.g)

Verwerkingslocatie Google?

1.8. Technieken en methoden van de gegevensverwerkingen

De 1-1-2 centralisten nemen oproepen aan en bepalen of dit noodhulpoproepen of misbruikoproepen zijn.
Noodhulpoproepen worden door de centralist doorgezet naar de betreffende hulpverleningsdiensten.
Misbruikoproepen worden door de centralist als zodanig gemarkeerd.
Er is steeds sprake van menselijke tussenkomst, behalve bij oproepen van CLI's die op de zwarte lijst staan.

Er wordt gecontroleerd of het oproepende CLI op een permanente of tijdelijke witte of zwarte lijst staat, of belt vanuit een in de grijze lijst gemarkeerd gebied.
Bij een oproep van een CLI op de zwarte lijst wordt een misbruik (preventie)-actie opgestart die kan bestaan uit het spelen van een automatische meldtekst of het verbreken van de telefoonverbinding. Wanneer de beller (onlangs) al eerder misbruik belpogingen heeft gedaan, dan wordt een misbruik (preventie)-actie opgestart die kan bestaan uit het versturen van een SMS-bom (een aantal geautomatiseerde SMS-berichten) of het versturen van een voice-bom (een aantal geautomatiseerd terugbelberichten).
Bij een oproep van een CLI op de witte lijst wordt de oproep direct met hoge prioriteit in de wachtrij geplaatst.
Bij een oproep van een locatie binnen een gebied op de grijze lijst wordt een meldtekst die specifiek is voor het gemarkeerde gebied afgespeeld, waarna de beller naar een grijze-lijst gerelateerde systeemwachtrij, een noodhulpdienst of een specifiek telefoonnummer wordt gerouteerd.
Bij eCall wordt de zwarte lijst niet gehanteerd.
Bij een eSMS oproep van een CLI dat op de zwarte lijst staat zal een misbruik (preventie)-actie gestart worden die bestaat uit het terugsturen van een SMS-bericht met een geconfigureerde melding.
CLI's die op een tijdelijke zwarte of witte lijst zijn geplaatst, worden automatisch na 1 uur weer van die lijst verwijderd.

Er is verder geen sprake van geautomatiseerde besluitvorming, profilering, big data of nieuwe technologieën.
De implementatie van eCall en AML als zodanig is overigens wel een nieuwe technologie, maar deze ligt buiten de scope van de 112 alarmcentrale.

1.9. Juridisch en beleidsmatig kader

1.9.1. Wet- en regelgeving

Conform het Besluit 1-1-2 alarmcentrales is de Korpschef aangewezen als beheerder van de alarmnummers voor publieke diensten, bedoeld in artikel 11.10, eerste lid, van de Telecommunicatiewet. De korpschef is dus verantwoordelijk voor het beheer van de 1-1-2 alarmcentrale.

Conform artikel 11.10, eerste lid, van de Telecommunicatiewet dient de provider bij een noodoproep gelijktijdig het telefoonnummer, de naam, en de beschikbare adres-, postcode- en woonplaatsgegevens van de abonnee, dan wel de locatie van de openbare betaaltelefoon, door te geven.
Conform artikel 11.10, tweede lid, dient de provider, indien hij locatiegegevens kan verwerken, deze ook gelijktijdig door te geven.

Artikel 11.10, derde lid, bepaalt dat de verstrekte nummers, en NAW / locatiegegevens moeten worden vastgelegd met het oog op de hulpverlening in noodsituaties of de bestrijding van het misbruik van het alarmnummer.
Ook bepaalt artikel 11.10, derde lid, dat de korpschef de verantwoordelijke is in de zin van artikel 1, onderdeel d, van de Wet bescherming persoonsgegevens voor deze vastlegging.

Artikel 11.10, vierde lid, bepaalt dat verstrekking van nummers en gegevens alleen is toegestaan met het oog op de hulpverlening in noodsituaties of de bestrijding van het misbruik van een alarmnummer voor publieke diensten. De korpschef is verantwoordelijke in de zin van artikel 1, onderdeel d, van de Wet bescherming persoonsgegevens voor deze verstrekkingen.

Conform artikel 2 van het Besluit 1-1-2 alarmcentrales zijn de gemeentelijke en regionale brandweerkorpsen, de Regionale Ambulancevoorzieningen, bedoeld in artikel 4 van de Tijdelijke wet ambulancezorg, en de politie aangewezen als publieke diensten belast met hulpverleningstaken, bedoeld in artikel 11.10, vijfde lid, van de Telecommunicatiewet. Artikel 11.10, vijfde lid, bepaalt dat verstrekking van nummers en gegevens alleen aan deze partijen mag plaatsvinden.

Telecommunicatiewet artikel 11.10, zesde lid, bepaalt dat verstrekking van nummers en gegevens met het oog op de bestrijding van het misbruik van het alarmnummer alleen is toegestaan aan degene die op grond van artikel 141 of 142 van het Wetboek van Strafvordering is belast met de opsporing van strafbare feiten.

Artikel 11.10, zevende lid, bepaalt de maximale termijn gedurende welke de nummers en gegevens mogen worden bewaard:
a. twee maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van een verzoek om hulpverlening in een noodsituatie;
b. zes maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van misbruik van een alarmnummer voor publieke diensten;
c. 24 uur in alle overige gevallen.

EU gedelegeerde verordening nr. 305/2013 bepaalt in artikel 2, lid c en d, en artikel 3, tweede lid, dat de door de autoriteiten aangewezen eCall alarmcentrale de eCalls behandelt overeenkomstig de nationale regelgeving inzake de verwerking van noodoproepen.
Artikel 2, lid j, bepaalt dat de doorgezonden informatie moet voldoen aan de vereisten zoals gedefinieerd in EN-norm 15722.
Artikel 3, vijfde en zesde lid, bepaalt dat de locatie, de wijze van activering van de eCall (handmatig of automatisch) en andere relevante data aan de juiste noodhulpdienst(en) of dienstverleningspartner(s) verstrekt kunnen worden.
Artikel 3, zevende lid, bepaalt dat het, in voorkomend geval, afhankelijk van de nationale procedures en wetten, toegestaan is om de eCall-alarmcentrale en de relevante noodhulpdienst(en) of dienstverleningspartner(s) toegang te geven tot de in nationale databanken en/of andere relevante bronnen opgeslagen kenmerken van het voertuig, met als doel informatie te verkrijgen die nodig is voor de behandeling van een eCall, met name met het oog op de interpretatie van het voertuigidentificatienummer (VIN) en de presentatie van aanvullende relevante informatie, meer bepaald voertuigtype en -model.
Artikel 6, eerste lid bepaalt dat de alarmcentrales, inclusief de eCall-alarmcentrales, worden beschouwd als voor de verwerking van gegevens verantwoordelijken in de zin van artikel 2, onder d), van Richtlijn 95/46/EG[13], en dat de verwerking van persoonsgegevens in het kader van de behandeling van eCalls door de alarmcentrales, de noodhulpdiensten en de dienstverleningspartners plaatsvindt overeenkomstig de Richtlijnen 95/46/EG en 2002/58/EG[14] en dat de naleving van deze voorschriften ten aanzien van de voor gegevensbescherming bevoegde nationale autoriteiten wordt aangetoond.
Artikel 7, tweede lid, bepaalt dat de behandeling van 112-oproepen, de ruwe MSD die samen met de eCall worden ontvangen, en de MSD-inhoud die aan de eCall-centralist wordt gepresenteerd, gedurende een bepaalde periode bewaard moet worden overeenkomstig de nationale regelgeving. Deze gegevens worden opgeslagen overeenkomstig de artikelen 6, 13 en 17 van Richtlijn 95/46/EG. Deze artikelen in de Richtlijn 95/46/EG, de algemene gegevensverordening, zijn verwerkt in de bepalingen in artikelen 6-11 van de Wbp[15].
De bepalingen in de Richtlijn 2002/58/EG zijn verwerkt in de Telecommunicatiewet.

Conform artikel 2, lid 2, sub IV van het Verdrag betreffende een Europees voertuig- en rijbewijsinformatiesysteem (EUCARIS) is een doel van EUCARIS: Partijen of derde partijen ter beschikking te staan die gegevens wensen uit te wisselen op basis van EU-wetgeving of een bilaterale of multilaterale overeenkomst anders dan dit Verdrag. Hierdoor kunnen EUCARIS gegevens worden verstrekt voor de uitvoering van de eCall regelgeving.

Conform artikel 43 lid 1 van de Wegenverkeerswet 1994 verstrekt de Dienst Wegverkeer gegevens uit het kentekenregister aan overheidsorganen, voor zover zij aangeven deze gegevens nodig te hebben voor een goede uitoefening van hun publieke taak.

VERORDENING (EU) 2015/758 geeft in Artikel 6 voorschriften inzake bescherming van de privacy en gegevensbescherming aan de fabrikanten van eCall boordsystemen.

---

[13] Door het vervangen van Richtlijn 95/46/EG door Verordening 2016/679 (AVG) is dit nu de verwerkingsverantwoordelijke in de zin van artikel 4 onder 7) van de Verordening 2016/679. Dit is nog niet aangepast in de EU gedelegeerde verordening nr. 305/2013.
[14] Door het vervangen van Richtlijn 95/46/EG door Verordening 2016/679 (AVG) is dit nu overeenkomstig de Verordening 2016/679 (AVG) en Richtlijn 2002/58/EG (e-Privacy richtlijn). Dit is nog niet aangepast in de EU gedelegeerde verordening nr. 305/2013.
[15] Door het vervangen van Richtlijn 95/46/EG door Verordening 2016/679 (AVG) is de Wbp vervallen en is dit nu overeenkomstig de artikelen 5, 23 en 24-31 van de Verordening 2016/679 (AVG). Dit is nog niet aangepast in de EU gedelegeerde verordening nr. 305/2013.

RICHTLIJN 2002/22/EG (Universeledienstrichtlijn), Telecommunicatiewet art. 9.1 lid f, Besluit universele dienstverlening en eindgebruikersbelangen art. 2.3a, 2.3b, 2.3c en Regeling universele dienstverlening en eindgebruikersbelangen art 2.7 schrijven voor dat auditief beperkten gelijkwaardig toegang moeten hebben tot het alarmnummer 1-1-2 en dat hiervoor een bemiddelingsdienst kan worden aangewezen. Uit de beantwoording van kamervragen door de minister van VWS d.d. 9-10-2013 (kenmerk ah-tk-20132014-376) en kamerbrief 620265 d.d. 24 februari 2015 van de minister van VenJ kan worden afgeleid dat KPN Teletolk middels aanbesteding is aangewezen voor deze bemiddelingsdienst.
TotalConversation is de applicatie waarmee gelijkwaardige toegang wordt gerealiseerd.

Besluit universele dienstverlening en eindgebruikersbelangen art. 4.3 en Regeling universele dienstverlening en eindgebruikersbelangen art 4.6 geven specificaties m.b.t. de kwaliteit van de door de providers aan de alarmcentrale aan te leveren gegevens.
Deze regelingen stellen minimale eisen aan de nauwkeurigheid van locatiegegevens, geen maximale eisen), en sluiten daarmee AML niet uit.

AML wordt geïmplementeerd conform (concept) European Electronics Communications Code (EECC), overweging 259 en 260, en artikel 102 5e lid. Na vaststelling van deze Europese richtlijn dienen de nationale overheden deze te implementeren in hun nationale telecommunicatiewetgeving. In Nederland wordt dit (in de ontwerptekst voor de consultatie) verwerkt door aanpassing van Tw art. 11.10.

EECC overweging 20 geeft aan dat het begrip noodcommunicatie alle persoonlijke communicatiediensten waarmee de noodhulpdiensten kunnen worden bereikt moet bestrijken, en niet alleen die via telefonie. Overwegingen 137 en 138 betreffen Europese harmonisatie hiervan. Overweging 255 noemt een aantal voorbeelden: Noodhulpcommunicatie is een communicatiemiddel dat niet alleen spraakcommunicatie omvat, maar ook SMS, berichten, video of andere vormen van communicatie. Dit kan de wettelijke basis vormen voor de 112 app, alhoewel deze overweging of de implementatie ervan niet als zodanig is opgenomen in de ontwerptekst Telecommunicatiewet (noch art 7.7 of 11.10, noch elders)..

Uit praktische overwegingen heeft de beheerder 1-1-2 alarmcentrale zelf besloten een overeenkomst af te sluiten met de Berengroep voor het kunnen opvragen van adresgegevens van doven en slechthorenden die contact opnemen met 1-1-2. Deze overeenkomst is niet gebaseerd op regelgeving.

Uit oogpunt van verbetering van het noodhulpproces heeft de beheerder 1-1-2 alarmcentrale zelf besloten een 112App te ontwikkelen en daartoe overeenkomsten af te sluiten met een leverancier voor het hosten van de 112App backend en met een leverancier van een vertaalservice voor de chatberichten.

Politiewet 2012
Conform Politiewet 2012 artikel 4 zijn een aantal politietaken opgedragen aan de KMar. Conform artikel 5 kan de minister van JenV regels stellen aan de samenwerking tussen politie en KMar.
Deze regels zijn gesteld in de Samenwerkingsregeling politie-Koninklijke marechaussee. Conform artikel 1 lid 3 kan deze samenwerking pas plaatsvinden na goedkeuring van het bevoegd gezag (i.c. de ministers van JenV en Defensie).
Alhoewel de KMar niet is genoemd als hulpverleningsdienst als bedoeld in artikel 11.10, vijfde lid, van de Telecommunicatiewet, kan deze wel als zodanig worden beschouwd op basis van bovenstaande.

1.9.2. Beleid

Routeringsbeleid
Dit houdt in dat de 1-1-2 centralist de burger zal vragen wie hij/zij wil spreken: politie, brandweer of ambulance? en vervolgens zal doorverbinden met de gevraagde hulpdienst in de regionale meldkamer.
Afgesproken is dat de landelijke 1-1-2 centrale bij piekbelasting of storingen burgers met een noodhulpmelding doorverbindt met een centralist van de gevraagde hulpverleningsdienst in een andere regionale meldkamer. Als er bijvoorbeeld sprake is van piekbelasting voor de politie in de regionale meldkamer A zal de landelijke 1-1-2 centrale de burger doorverbinden naar de politie in de regionale meldkamer B.
De brandweer, politie, KMar en ambulancevoorziening hebben binnen hun eigen kolom (landelijk) onderling afgestemd naar welke meldkamerlocatie de burger in eerste instantie doorverbonden zal worden. Bij grotere

piekbelasting of technische storing kunnen burgers binnen dezelfde kolom naar iedere meldkamerlocatie waar capaciteit vrij is doorverbonden worden, als de burger maar geholpen wordt.

Een eCall wordt volgens hetzelfde protocol afgehandeld als een “gewone” 1-1-2 melding van een auto ongeluk. Dit houdt in dat de 1-1-2 centralist de burger zal vragen wie hij/zij wil spreken: politie, brandweer of ambulance? en vervolgens zal doorverbinden met de gevraagde hulpdienst in de regionale meldkamer. In de regionale meldkamer dient de eCall gedeeld te worden met de overige hulpdiensten indien daar aanleiding toe is conform standaard protocol.
Hierop is één uitzondering: als het een automatische eCall betreft en de burger niet in staat is om de vraag van de 1-1-2 centralist te beantwoorden, zal de melding doorverbonden worden met het politie deel binnen de regionale meldkamer.

Routeringsbeleid bij gebruik van de 112App
Doelstelling van de 112App is dat een alarmoproep zonder tussenkomst van een 112 centralist direct naar de juiste hulpverleningsdienst kan worden gerouteerd. Het routeringsbeleid bij gebruik van de app is dus afwijkend van bovenstaande.
De GMS webservice analyseert voor welke meldkamer en hulpdienst de oproep is bestemd en routeert de gegevens naar de betreffende GMS omgeving. Daarnaast routeert de GMS webserver de gegevens via de 112 frontend naar het 112 systeem. Het 112 systeem analyseert of de inkomende spraakoproep kan worden gematched met een inkomende 112App oproep en routeert dan het gesprek zonder tussenkomst van een 112 centralist naar de betreffende meldkamer / hulpdienst. De spraakoproep wordt echter gerouteerd naar een 112 centralist indien het oproepende nummer voorkomt op de misbruiklijst, het gesprek wegens drukte niet kan worden gerouteerd naar de beoogde meldkamer of bij calamiteiten.

1.10. Bewaartermijnen

Conform Telecommunicatiewet artikel 11.10, zevende lid :
a. twee maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van een verzoek om hulpverlening in een noodsituatie;
b. zes maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van misbruik van een alarmnummer voor publieke diensten;
c. 24 uur in alle overige gevallen.

De van de 112App ontvangen data valt niet onder de werking van de Telecommunicatiewet.
Het chat-verkeer(in- en uitgaande berichten) wordt in de vorm van een integrale chat-sessie opgeslagen in GMS als deel van de melding. Hier worden de bewaartermijnen van GMS gehanteerd. Dit houdt in dat elke hulpverleningsdienst voor de eigen incidenten de bewaartermijn instelt.
De 112App Back-end vernietigt de chat na afloop van de sessie, zodat de chat alleen in GMS is opgeslagen.
De met de Google vertaalservice uitgewisselde gegevens worden door Google normaliter na 7 dagen en bij een verstoring na 14 dagen verwijderd.

Voor de op de uploadserver opgeslagen foto’s/video’s is nog geen bewaartermijn bepaald en geïmplementeerd. De uploadfunctionaliteit zal pas voor het publiek beschikbaar worden gemaakt nadat deze termijn is bepaald en verwerkt in een bijgewerkte versie van deze GEB.

2. Beoordeling rechtmatigheid gegevensverwerkingen

2.1. Rechtsgrond

De gegevensverwerking dient te voldoen aan minimaal één van de rechtsgronden, genoemd in Verordening 2016/679 (AVG) artikel 6, lid 1.
De gegevensverwerking is primair gebaseerd op:

> c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

en secundair op:

> e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
> d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

2.2. Bijzondere persoonsgegevens

Verwerking van bijzondere categorieën van persoonsgegevens is conform AVG artikel 9 lid 1 verboden, tenzij wordt voldaan aan één van de voorwaarden van artikel 9, lid 2.

Doel van de verwerking is uitsluitend het aannemen van oproepen, bemiddelen van bepaalde typen oproepen tussen beller en hulpdienst, verrijken met voor de hulpverleningsdiensten relevante informatie, en doorzetten van het gesprek naar de relevante hulpverleningsdienst(en). De verrijking is uitsluitend conform hetgeen beschreven in hoofdstuk 1.

Bij aanname van alle typen oproepen met uitzondering van eSMS en TotalConversation vraagt de centralist uitsluitend aan de oproeper welke hulpdienst deze wil spreken. Het proces is er dus op gericht om geen inhoudelijke informatie over de reden van de oproep te ontvangen. Het is echter mogelijk dat de oproeper ongevraagd bijzondere, strafrechtelijke of andere gevoelige gegevens verstrekt, die dan worden opgeslagen in de voicelog.
Bij aanname van eSMS en TotalConversation bemiddelt de 1-1-2 centralist tussen de beller en de benodigde hulpdienst en neemt dus steeds kennis van de inhoud van de hulpvraag. Deze wordt ook gelogd. De inhoud kan alle categorieën persoonsgegevens bevatten.

Gezien het doel van het 1-1-2 nummer, waarbij elke seconde telt, wordt niet voorzien in de informatieplicht of om expliciete toestemming voor verwerking van deze gegevens gevraagd.

De verwerking is toegestaan op basis van de volgende verbodsuitzonderingen in de AVG atikel 9 lid 2:
a. de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden (waarbij de toestemming blijkt doordat melder de bijzondere persoonsgegevens zelf vertrekt);
c. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;

In aanvulling hierop is de verwerking van gezondheidsgegevens toegestaan op basis van Uitvoeringswet AVG artikel 23, lid 1, sub a.

Voorts is de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen conform Uitvoeringswet artikel 31 toegestaan indien deze geschiedt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht. Politie is één van deze organen.

De 1-1-2 alarmcentrale taak wordt uitgevoerd door politieambtenaren. Deze zijn gescreend en hebben een geheimhoudingsplicht.

2.3. Doelbinding

Primair:

- Ten behoeve van het aannemen van oproepen, bemiddelen van oproepen tussen beller en hulpdienst, verrijken met voor de hulpverleningsdiensten relevante informatie, en doorzetten van het gesprek naar de relevante hulpverleningsdienst(en).

Secundair:

- Ten behoeve van het bestrijden van misbruik van het 1-1-2 alarmnummer.
- Ten behoeve van beheer en bedrijfsvoering van de 1-1-2 alarmcentrale
- Ten behoeve van de behandeling van klachten van betrokkenen aangaande de afhandeling van de noodoproep

De secundaire doelen zijn ondersteunend aan, en daardoor geheel verenigbaar met, het primaire doel.

2.4. Noodzaak en evenredigheid

2.4.1. Proportionaliteit

Er worden niet meer gegevens verwerkt dan noodzakelijk is voor een zo goed en snel mogelijke noodhulpverlening, de bestrijding van misbruik van het 112 nummer, en het beheer van deze bedrijfsprocessen.

2.4.2. Subsidiariteit

Het eventueel verwerken van minder gegevens heeft nadelige gevolgen voor de snelheid en/of kwaliteit van de noodhulpverlening, en is daarmee niet in het belang van de betrokkenen en de hulpdiensten.

2.5. Rechten van de betrokkenen

De politie heeft een privacy verklaring gepubliceerd op https://www.politie.nl/algemeen/privacy.html.
Voor de uitoefening van rechten door betrokkenen kan het algemene proces binnen de politie worden gevolgd. Betrokkenen kunnen zich wenden tot elke willekeurige politie eenheid. Afhandeling wordt daarna intern doorgerouteerd.

Op de website van de rijksoverheid worden burgers geinformeerd over het gebruik van 1-1-2. Een feitelijke privacyverklaring maakt hier geen deel van uit.

3. Beschrijving en beoordeling risico's voor de betrokkenen

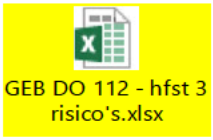
In het hieronder ingevoegde document worden de risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen gespecificeerd. Hierbij is rekening gehouden met de aard, omvang, context en doelen van de gegevensverwerkingen.

Er wordt hierbij ingegaan op:
a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
b. de oorsprong van deze gevolgen;
c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Risico's:
- Vernietiging en verlies (beschikbaarheid)
- Wijziging (integriteit)
- Ongeoorloofde toegang en verstrekking (vertrouwelijkheid)

Mogelijke gevolgen voor betrokkene:
- De gegevensverwerking kan leiden tot:
    - discriminatie, stigmatisering en uitsluiting;
    - (blootstelling aan) identiteitsdiefstal of -fraude;
    - financiële verliezen;
    - reputatie- of anderszins relationele schade;
    - verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
    - ongeoorloofde ongedaanmaking van pseudonimisering;
    - of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;
- wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
- wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;
- wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

NB Bovenstaande opsomming is overgenomen uit het Model gegevensbeschermings-effectbeoordeling rijksdienst (PIA); niet alle gevolgen hoeven van toepassing te zijn voor 1-1-2. De voor 1-1-2 relevante gevolgen zijn benoemd in onderstaande overzicht.



4. Beschrijving voorgenomen maatregelen

Hieronder worden de maatregelen om de hiervoor beschreven risico's van de gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Politie
De 1-1-2 alarmcentrale is ingericht in een beveiligde politielocatie en uitsluitend toegankelijk voor de daartoe geautoriseerde medewerkers. Medewerkers zijn gescreend en hebben een geheimhoudingsplicht.
Het 1-1-2 platform is gekoppeld aan GMS via het beveiligde interne politienetwerk. De maatregelen voor GMS worden toegelicht in de GEB GMS.

Voor dit geheel is het politie beveiligingsbeleid van kracht. Dit beleid is gebaseerd op de Regeling Informatiebeveiliging Politie, zie https://wetten.overheid.nl/BWBR0008599/2017-12-15 en is intern politie uitgewerkt in diverse beleidsregels. Deze interne beleidsregels mogen niet extern gepubliceerd worden, en worden hier derhalve niet toegelicht.

KPN
Het 1-1-2 platform is gehuisvest in beveiligde datacenters van KPN en is beveiligd conform het hoogste niveau (kritisch) van de KPN Security Policy.

KPN heeft haar securitybeleid gepubliceerd in een app voor professionals, zie https://overons.kpn/nl/nieuws/2016/kpn-publiceert-securitybeleid-in-app-voor-professionals.

In de contracteringsfase is de KPN security policy door de politie beoordeeld en adequaat bevonden. Specifieke afspraken met betrekking tot de 112 dienstverlening zijn vastgelegd in een jaarlijks te reviewen Informatiebeveiligingsplan Dienst 1-1-2.
Hierin is o.a. vastgelegd dat de Dienst 1-1-2 gekwalificeerd is als vitale en kritieke dienst, en er daarom een aantal aanvullende maatregelen gelden ten opzichte van de standaard KPN Security Policy.
Dit beveiligingsplan is geclassificeerd als vertrouwelijk en wordt hier derhalve niet verder toegelicht.

Verbindingen

- Het door KPN beheerde 112 platform is via het beveiligde KPN netwerk en een beveiligde partnerkoppeling verbonden met het beveiligde politienetwerk. De berichtuitwisseling van het 112 platform naar GMS vindt plaats op basis van HTTPS en SOAP.
- De oproepen worden vanuit de netwerken van de telefonieaanbieders via vaste verbindingen aangeboden aan het 112 platform.
- De mastlocatiegegevens worden door de telefonieaanbieders via vaste verbindingen aangeboden aan het 112 platform.
- SMS- en voicebommen worden vanuit het 112 platform doorgerouteerd naar CM Telecom via vaste verbindingen en vervolgens via de netwerken van de telefonieaanbieders naar de betrokkenen gerouteerd.
- De AML locatiegegevens worden via de netwerken van de mobiele telefonieaanbieders aangeboden aan de SMS broker, en door de SMS broker aan de GMS webservice aangeboden via een internetkoppeling met gebruik van SSL en Rijksoverheid PKI certificaten met tweezijdige certificaatverificatie.

.

Telefonieaanbieders
De telefonieaanbieders dienen conform de Telecommunicatiewet, het Besluit beveiliging gegevens telecommunicatie en het Besluit continuïteit openbare elektronische communicatienetwerken en –diensten zorg te dragen voor passende beveiligingsmaatregelen.

10 2 g
10 2 g voldoet aan de 15027001 en ISAE3402 (of gelijkwaardige) standaards. De gebruikte beveiligingsproducten zijn voor zover mogelijk gecertificeerd volgens de Common Criteria tegen een niveau dat algemeen haalbaar wordt

geacht in de markt maar minimaal EAL-niveau 2. In verband met ontwikkelingen en doorlooptijd van de certificering door Common Criteria is 10.2.g gerechtigd om een nieuwe - nog niet gecertificeerde -versie van de gebruikte beveiligingsproducten te gebruiken indien zij dit redelijkerwijs nodig acht en zij aangeeft dat naar haar inschatting deze nieuwe versie tenminste aan dezelfde vereisten voldoet en mogelijk zelfs verbeteringen kent.
Tevens geldt voor sommige door 10.2.g gebruikte beveiligingsproducten dat deze (nog) niet door Common Criteria gecertifieerd zijn. In deze gevallen zal 10.2.g onderbouwen dat zij van mening is dat deze beveiligingsproducten voldoen aan de industrie standaarden en bij een eventuele certificering door Common Criteria aan de vereisten hiervan zou voldoen. Laatstgenoemde beveiligingsproducten zullen slechts na voorafgaande goedkeuring van de Politie welke toestemming de Politie niet op onredelijke gronden zal weerhouden of vertragen - worden toegepast.
In de praktijk betekent dit bijvoorbeeld dat er gebruik wordt gemaakt van versleutelde verbindingen (HTTPS) en dat netwerk segmentatie wordt toegepast waarbij het verkeer wordt gecontroleerd door firewalls.

De organisatorisch en technische beveiligingsmaatregelen omvatten in ieder geval:
a. Maatregelen om te waarborgen dat enkel bevoegd Personeel van 10.2.g toegang heeft tot de Persoonsgegevens en/of Politiegegevens voor het doel dat is uiteengezet in Bijlage 1 van de Verwerkersovereenkomst;
b. Maatregelen waarbij 10.2.g zijn Personeel en Hulpleveranciers uitsluitend toegang geeft tot Persoonsgegevens en/of Politiegegevens via op naam gestelde accounts, waarbij het gebruik van die account adequaat gelogd wordt en waarbij de betreffende account alleen toegang geven tot die Persoonsgegevens en/of Politiegegevens waartoe de toegang noodzakelijk is;
c. Maatregelen om de Persoonsgegevens en/of Politiegegevens te beschermen tegen onopzettelijk of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking;
d. Maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van Persoonsgegevens en/of Politiegegevens in de systemen die worden ingezet voor het verlenen van de diensten aan de Politie;
e. Maatregelen om de tijdige beschikbaarheid van de gegevens te garanderen die benodigd zijn voor het uitvoeren van de Overeenkomst.

Google
Er is voor de vertaalservice geen overeenkomstafgesloten met Google. De Google Cloud Platform voorwaarden voor gegevensverwerking en –beveiliging zijn van toepassing:
“ Google will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the “Security Measures”). The Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google’s systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Google may update the Security Measures from time to time provided that such updates do not result in the degradation of the overall security of the Services.”

5. Oordeel en advies

5.1. 112App

5.1.1. Fasering oplevering

De 112App wordt gefaseerd opgeleverd. Er wordt een pilot uitgevoerd voordat de eerste publieksversie live gaat. Naderhand zal de functionaliteit stapsgewijs uitgebreid worden.
Op dit moment zijn nog niet alle details bekend voor de eerste publieksversie.
Deze versie van de GEB kan als gereed worden beschouwd voor de pilot versie; voorafgaand aan de eerste publieksversie en elke versie daarna zal de GEB moeten worden bijgewerkt met de dan relevante informatie.

5.1.2. Rechtsgrond

Vanuit het project 112App is aangegeven dat er op grond van Europese regelgeving druk is om de 112App op te leveren.

Het is niet precies duidelijk welke regelgeving dit is: EECC overweging 20 geeft aan dat het begrip noodcommunicatie alle persoonlijke communicatiediensten waarmee de noodhulpdiensten kunnen worden bereikt moet bestrijken, en niet alleen die via telefonie. Overwegingen 137 en 138 betreffen Europese harmonisatie hiervan. Overweging 255 noemt een aantal voorbeelden: Noodhulpcommunicatie is een communicatiemiddel dat niet alleen spraakcommunicatie omvat, maar ook SMS, berichten, video of andere vormen van communicatie. Dit kan de wettelijke basis vormen voor de 112 app, alhoewel deze overweging of de implementatie ervan niet als zodanig is opgenomen in de ontwerptekst wijzigingswet Telecommunicatiewet inzake de Telecomcode (noch art 7.7 of 11.10, noch elders).

De EECC vormt als zodanig geen wettelijke basis; de EECC dient door de EU lidstaten via nationale wetgeving geïmplementeerd te worden.

Alhoewel de verwerking van persoonsgegevens op basis van rechtsgronden AVG art. 6 lid d en e prima te verdedigen is, is de legitimiteit natuurlijk nog groter wanneer de verwerking plaatsvindt op basis van een wettelijke verplichting (AVG art. 6 lid c). **Het is zaak om hier helderheid in te verkrijgen.**

5.1.3. Bewaartermijn

In de pilotversie in eerste publieksversie wordt de bewaartermijn van de chatlog bepaald door de bewaartermijn in GMS te configureren. Het project geeft aan dat de disciplines dit zelf doen.

Het volstaat niet om het bij deze constatering te laten. **De LMS heeft als ICT leverancier een zorgplicht, en dient er nadrukkelijk op te wijzen, en ook te bewaken, dat de disciplines die bewaartermijn daadwerkelijk en juist instellen.**

Zie voor jurisprudentie over de zorgplicht bijvoorbeeld https://www.juridict.nl/juridict-nieuwsartikel/zorgplicht-ict-leverancier-bij-schade-door-ransomware/

5.1.4. Vertaalservice

Voor de vertaalservice wordt Google translate gebruikt. Het project heeft geen overeenkomst met Google kunnen overleggen op basis waarvan afspraken zijn gemaakt die de persoonsgegevens voldoende beschermen.

De standaard voorwaarden van Google zijn van toepassing. Volgens die voorwaarden treft Google de nodige beveiligingsmaatregelen. Volgens de voorwaarden voor gegevensbeveiliging en –verwerking is de AVG van toepassing indien de verwerking plaatsvindt in de EEA of de UK. Het is echter niet duidelijk of de verwerking inderdaad plaatsvindt.
Volgens de zelfde voorwaarden kan ook “Non-European Data Protection Law” van toepassing zijn. De vraag hierbij is of letterlijk wordt bedoeld dat niet Europese wetgeving ten aanzien van databescherming van toepassing kan zijn, of dat heir eigenlijk wordt bedoeld dat niet Europese wetgeving die een negatieve impact heeft op databescherming van toepassing kan zijn.

Op basis van Amerikaanse wetgeving (Patriot Act) en daaraan gerelateerde wetgeving zoals de Foreign Intelligence Surveillance Act (FISA), Executive Order 12333 en Presidential Policy Directive 28 heeft de overheid verregaande mogelijkheden om verbindingen af te luisteren en bedrijven te dwingen om persoonsgegevens te verstrekken.

Op basis van de CLOUD Act kunnen Amerikaanse autoriteiten bij Amerikaanse clouddienstverleners gegevens vorderen die in een ander land zijn opgeslagen. Dus ook indien de verwerking door Google plaatsvindt binnen de EEA. Zie bijvoorbeeld https://www.ictrecht.nl/blog/mag-de-amerikaanse-overheid-persoonsgegevens-vorderen-bij-eu-bedrijven-onder-de-cloud-act

In juli 2020 is door het Europese hof van justitie bepaald dat, gelet op de Amerikaanse wetgeving, de Privacy Shield overeenkomst tussen EU en USA onvoldoende waarborgen biedt ter bescherming van persoonsgegevens, en daarom ongeldig is verklaard in het zogenoemde "Schrems II arrest". Als gevolg hiervan is verwerking van persoonsgegevens door Amerikaanse partijen of op Amerikaans grondgebied uitsluitend toegestaan nadat aanvullende beschermingsmaatregelen zijn getroffen.

Een technische maatregel kan zijn versleuteling van data, waarbij de dienstverlener niet de mogelijkheid heeft om de data te ontsleutelen. In het geval van de Google vertaaldienst is dit niet realiseerbaar: de vertaalservice kan dan niet functioneren.

Er zullen daarom voldoende contractuele en organisatorische maatregelen getroffen moeten worden. Voor informatie en duiding zie bijvoorbeeld https://iapp.org/news/a/a-break-down-of-edpbs-recommendations-for-data-transfers-post-schrems-ii/?mkt_tok=eyJpIjoiTkRKalpUY3lZV1ZpTURZMCIsInQiOiJPTDdyYytHTDRVR0xMRG1rU0NsZTdjR3dZR1dVTmVlTUFLTm9JRk85SllPQjZIaDl3XC9nc1l0Q3ZNcTlXNGJUalFUUk5EWTZaakprTXB5aTFQSCs4RnN5ZERSV0xCTGJoMHg4RFFqTXl2QksxaDRIeCt4XC9LRGdTdVdwXC9Dd2l3MCJ9

Als organisatorische maatregelen noemt de EDPB o.a. dataminimalisatie en het conformeren aan internationale beveiligingsstandaarden.

Als contractuele maatregelen noemt de EDPB:
Transparantieverklaring van de dienstverlener, met daarin in ieder geval het geverifieerd niet aanwezig zijn van een beckdoor waardoor de overheid toegang tot de data zou kunnen hebben, audits ter verificatie of persoonsgegevens aan de overheid zijn verstrekt, het informeren van de klant wanneer de dienstverlener door wetswijzigingen niet langer kan voldoen aan haar eigen commitment of de vereiste bescherming van persoonsgegevens, het via rechtszaken betwisten van de vordering tot gegevensverstrekking, het informeren van de klant voorafgaand aan het uitvoering geven van een verzoek tot gegevensverstrekking, en een "warrant canary" (het continu informeren van de klant dat er geen verzoek tot gegevensverstrekking is ontvangen tot het moment dat dat verzoek wel is ontvangen; dit is noodzakelijk omdat in bepaalde gevallen het de dienstverlener niet is toegestaan om de klant te informeren over zo'n verzoek tot verstrekking), en/of het informeren van betrokkenen en/of het verzoeken om expliciete toestemming van betrokkenen voorafgaand aan verstrekking.

De Google transparantieverklaring benoemt alleen de volgende zaken:

- Betwisten of specifieker maken van vordering;
- informeren van de klant indien dat is toegestaan;
- Indien de klant bezwaar maakt (bij een Amerikaanse rechtbank) pas verstrekken indien de rechtbank zo besluit.

Google lijkt hiermee onvoldoende contractuele waarborgen te leveren, waardoor de verwerking niet geheel voldoet aan de AVG.