politie
brandweer
ambulance
koninklijke marechaussee

Notitie

Aan
Stuurgroep 112App

Van
10.2.e

E-mail
10.2.e @politie.nl

Datum
1 december 2020

Versie
0.1

Pagina's
6

Verantwoording van Veiligheid en Privacy van de 112NL-App

Deze notitie verantwoordt de maatregelen die in het project "112NL-app" zijn genomen om de privacy van burgers en de veiligheid te waarborgen.

Vanaf het begin is de insteek geweest om het maximale te doen aan bescherming van privacy en veiligheid. Het doel is dat een melder zonder aarzeling of twijfel gebruik kan maken van de 112NL-app. Met deze notitie willen wij verantwoorden welke maatregelen genomen zijn.

Gesprekspartners

- De **gegevensautoriteit** van de Politie heeft meegekeken vanuit een juridisch perspectief.
- Het **IB-kwartier** van de Politie heeft een risico-analyse gemaakt.
- **LMS** heeft een Gegevens-Effect-Beoordeling gemaakt.
- De 10.2.g heeft in functionele zin meegekeken vanuit het belang van inclusiviteit.
- **Security-specialisten van de Politie** hebben meegekeken om te zekeren dat de 112NL-app keten voldoet aan de beveiligingseisen van de Politie.
- 10.2.g heeft in 2018 een gebruikerstoets gehouden op basis van requirements om de bruikbaarheid al in het ontwerp te verankeren.
- **KPMG** heeft in het najaar van 2020 en het voorjaar van 2021 een tweetal penetratietests uitgevoerd om de veiligheid van de keten te waarborgen.
- **Google** heeft verantwoord dat er bij het vertalen geen informatie bij Google achterblijft, zodat deze gegevens niet achteraf gebruikt kunnen worden door Google (of anderen) voor nadere analyse.
- De **Dienst ICT** van de Politie bewaakt de veiligheid 24/7 alsof het een reguliere politie-applicatie betreft.
- Een **klankbordgroep** bestaande uit centralisten van 4 verschillende disciplines + de landelijke eenheid, senioren, CaCo's en functioneel beheer heeft op tweewekelijkse basis meegekeken met het project om vanuit gebruikerszijde input te leveren.

2 Uitgangspunten en kaders

Kaders

1 Juridische kaders
Bij aanvang van het project zijn de juridische kaders geïnventariseerd om inzicht te krijgen in de na te volgen regelgeving. (1)

2 Tactisch Normenkader
De baseline van de beveiliging is het tactisch normenkader (TNK) van de Baseline Informatiebeveiliging Rijksdienst (3), om aan ISO 27001 en ISO 27002 te voldoen.

3 NCSC richtlijnen
Het ontwerp volgt de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Justitie en Veiligheid (4), om de 112NL-app minder kwetsbaar te maken tegen misbruik en cybercrime.

4 Gegevenseffectbeoordeling (GEB)
Onder de AVG en de Wpg is de LMS verplicht om een GEB (eng: data protection impact assessment, DPIA) uit te voeren. De LMS gebruikt dit instrument om vooraf de privacyrisico's in kaart te brengen en om maatregelen te kunnen nemen om de voorziene risico's te verkleinen.

Uitgangspunten

5 Privacy by design
In het Project Initiatie Document (2) is het thema privacy geaddresseerd en geborgd in de persoon van de privacyfunctionaris.

6 Security by design
In het Project Initiatie Document (2) is het thema security geaddresseerd en geborgd door deelname van het Informatiebeveiligingskwartier van de Politie. Het IB-kwartier heeft het ontwerp geanalyseerd op risico's en deze zijn voorafgaand aan de live-gang geanalyseerd en gemitigeerd.

7 Gebruiker centraal
Privacy en Veiligheid zijn er voor de burgers, voor de centralisten, voor hulpverleners, en ook voor de LMS en haar convenantpartners. Zij moeten het vertrouwen krijgen/hebben dat het uiterste is gedaan.

3 Projectactiviteiten

Wat heeft de LMS gedaan om de 112-NL app veilig te maken en de privacy van gebruikers te garanderen?

1 Requirements opstellen voor privacy (5) om deze requirements te kunnen toetsen in de testfase.
2 Aanpassen van de GEB voor de dienst 112 ten behoeve van de 112NL-app (6) om de privacyrisico's in de context van de gehele 112 dienstverlening te kunnen beoordelen.
3 Uitlopen van de NCSC-checklist (7).
4 Het uitvoeren van een risico-analyse (8)
5 Overleg met de 10.2.g rond het thema inclusiviteit, om vast te stellen of het ook voor gehoor- en spraakbeperkte mensen voldoende bescherming biedt.
6 Gebruikerstoets (10.2.g 2018), om de bruikbaarheid al in het ontwerp te verankeren.
7 Penetratietest (KPMG, okt/nov 2020), om de veiligheid van de keten te testen.
8 Penetratietest (KPMG, dec/jan 2020-21), om de veiligheid van de keten te testen.
9 Publiekstest (december 2020), om kinderziektes vroegtijdig op te lossen.
10 Het vertrouwen in de privacybescherming van Google is gebaseerd op een onderzoek van uit het project 10.2.e), die heeft kunnen vaststellen dat Google geen gegevens van de vertaling bewaart. Dit is ingesteld op een dashboard dat bij de Politie in beheer is 10.2.e). De vertaling wordt alleen gebruikt als de burger daar expliciet toestemming voor heeft gegeven.
11 Centralisten hebben in een klankbordgroep meegekeken tijdens het ontwerp en de bouw, zodat hun zorgen ten aanzien van veiligheid en privacy ook tijdens het traject geaddresseerd zijn.

4 Borging

- Bij elke nieuwe feature wordt een publiekstest uitgevoerd om kinderziektes uit te sluiten en om aanpassingen te kunnen doen op basis van gebruikerservaring in het veld.
- De Politie bewaakt de veiligheid permanent om het vertrouwen van het publiek in de app 112NL te bewaren.

5 Hoe respecteert de 112-NL app de belangen van de burger?

- De 112-NL app slaat in de smartphone de minimale persoonsgegevens op die noodzakelijk zijn om de app te laten functioneren.
- De LMS houdt geen register bij van mensen die de 112-NL app gebruiken, en bewaart dus geen gegevens over deze gebruikers.
- Gegevens die tijdens een noodoproep worden verstrekt (onboarding-gegevens, de eventuele chat, het gesprek, de eventuele foto's/videos van de melder) worden alleen bij de meldingsgegevens opgeslagen. Deze gegevens worden op precies dezelfde manier behandeld als de meldingsgegevens uit een regulier 1-1-2 telefoongesprek zonder 112-NL app.
- Alleen een centralist kan gegevens die tijdens een melding worden verstrekt doorgeven aan de hulpverleners in het veld: brandweer, ambulance, politie, marechaussee. De centralist is daarvoor opgeleid en bevoegd.
- Medische gegevens, die de meldkamer verwerkt tijdens het gebruik van de 112-NL app, vallen onder het medisch beroepsgeheim van de centralist en de hulpverleners.
- Het vertalen van de chat is optioneel. De vertaling wordt verzorgd door Google Translate. Google slaat niets van en niets over de vertaalde gegevens op.
- Alle gegevens worden versleuteld overgedragen, om het "meekijken" door kwaadwillende derden te voorkomen.

6 Bronvermeldingen

1. 10.2.e **.** *Juridische analyse van privacy issues in de 112-NL app keten.* sl : LMS, 2020.
2. 10.2.e **;** 10.2.e **.** *Project Initiatie Document (PID) 112App-keten.* LMS. sl : LMS, mei 2020.
3. **BZK, Min.** *Baseline Informatiebeveiliging Rijksdienst, Tactisch Normenkader (TNK).* sl : Rijksoverheid, 2012.
4. **NCSC.** *ICT-beveiligingsrichtlijnen voor webapplicaties.* Den Haag : sn, 2015.
5. 10.2.e **.** *Projectarchitectuur tbv de 112-NL app.* sl : LMS, 2020.
6. 10.2.e **.** *GEB (gegevensbeschermingseffectbeoordeling) 1-1-2.* sl : LMS, 2020.
7. 10.2.e **.** *Verantwoording van security aspecten van de 112NL-app ten aanzien van de de NCSC-richtlijnen.* sl : LMS, 2020.
8. 10.2.e **.** *Risico-analyse en IB advies.* sl : LMS, 2020.