Vergaderjaar 2020 – 2021

35 538 Tijdelijke bepalingen in verband met de inzet van een notificatieapplicatie bij de bestrijding van de epidemie van covid-19 en waarborgen ter voorkoming van misbruik daarvan (Tijdelijke wet notificatieapplicatie covid-19)

S BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 28 april 2021

CoronaMelder maakt gebruik van het Google Apple Exposure Notification (GAEN) framework om ontmoetingen te detecteren en gebruikers een melding te geven als ze in contact zijn geweest met iemand die achteraf besmet bleek. Het framework maakt gebruik van steeds wisselende willekeurige codes die worden uitgewisseld wanneer twee telefoons dichtbij elkaar zijn. Zo kan worden vastgesteld of iemand in contact is geweest met iemand die achteraf besmet bleek. Dit is een privacyvriendelijke manier om ontmoetingen bij te houden.

CoronaMelder wordt voortdurend getest op veiligheid en het voldoen aan de privacyvoorwaarden. Daartoe is ook een data protection impact assesssment (DPIA) uitgevoerd waarin privacyrisico's staan beschreven en de maatregelen die zijn genomen om deze te voorkomen. Hieronder valt ook het risico dat eigen en ontvangen codes worden verzameld en ingezien door anderen. Dit moet niet mogelijk zijn op de telefoon. De ontwikkelaars van het framework, Google en Apple, moeten hiertegen beveiligen.

Op telefoons die gebruik maken van het Google Android operating systeem blijkt dit niet afdoende geborgd. Het probleem doet zich voor op alle Google Android toestellen, omdat dit framework een integraal onderdeel van het besturingssysteem is. Het maakt daarbij niet uit of de eigenaar CoronaMelder heeft gedownload.

De willekeurige codes worden gelogd in het algemene systeemlogbestand van de telefoon. Dit is een serieus te nemen fout omdat vooraf geïnstalleerde standaard applicaties die met de telefoon worden meegeleverd hier toegang toe kunnen hebben. Daarmee is denkbaar dat deze apps bijvoorbeeld kunnen vaststellen of de telefoon behoort tot iemand die eerder als besmet is gemeld in CoronaMelder of welke ontmoetingen met besmette personen hebben plaatsgevonden. Hiervoor moeten willekeurige codes wel eerst gecombineerd worden met andere databronnen, wat in strijd is met de Tijdelijke wet notificatieapplicatie covid-19. Dit probleem doet zich voor zover nu bekend niet voor bij Apple telefoons en Google heeft mij vandaag gemeld geen bewijs te hebben dat eerder genoemde apps daadwerkelijk data hebben verzameld en gebruikt.

Het betreft een probleem in het framework van Google en raakt daarmee alle gebruikers. Zo'n 40 landen hebben een notificatieapplicatie ontwikkeld, die gebruik maakt van dit framework. In Nederland is dat CoronaMelder. Google is in ieder geval sinds afgelopen februari op de hoogte van

de fout in de software. Nederland is op 22 april via het Europese eHealth Netwerk op de hoogte gesteld van het probleem. Mijn ministerie is na ontvangst van de melding direct een technisch onderzoek gestart om de gevolgen van dit probleem nader in kaart te brengen. Daarnaast hebben wij maandag 26 april de Autoriteit Persoonsgegevens op de hoogte gesteld van dit mogelijke datalek van Google. Er is de afgelopen dagen intensief overleg gevoerd met andere lidstaten in het Europese eHealth Network.

Het door Nederland uitgevoerde onderzoek heeft vandaag laten zien dat het inderdaad zo is dat gegevens van gebruikers gelezen kunnen worden door onbevoegde partijen. Nederland heeft Google donderdag 22 april 2021 van haar initiële bevindingen op de hoogte gesteld. Daarna zijn zij meermalen op de hoogte gesteld van de aangetoonde misbruikmogelijkheden. Google meldt dat de bevinding bekend is en ook opgelost maar dat het enige tijd kan duren voordat alle telefoons van deze oplossing zijn voorzien. Daarbij bleken ze nog niet op de hoogte van de mogelijkheden voor misbruik die door onze experts aan hen zijn gemeld.

Ik vind het huidige antwoord van Google onvoldoende bevredigend. Het gaat hier om een serieus te nemen bevinding waarbij door onbevoegde partijen zou kunnen worden vastgesteld dat de eigenaar van een telefoon zich besmet heeft gemeld of met welke besmette personen contact is geweest. Ook al is er, aldus Google, nog geen reden aan te nemen dat een dergelijk misbruik al zou hebben plaatsgevonden.

De oplossing van het probleem ligt bij Google. Vandaag heeft Google mij gemeld dat een deel van het probleem is opgelost en de overige risico’s de komende dagen worden weggenomen. In de tussentijd kan ik wel de gevolgen van het mogelijke datalek beperken. Daarom worden de komende 48 uur vooralsnog geen codes van Nederlandse gebruikers van CoronaMelder die zich besmet hebben gemeld gedeeld met andere gebruikers van CoronaMelder. Deze tijd wordt gebruikt om te onderzoeken of Google daadwerkelijk het lek heeft gedicht.

De GGD blijft wel mensen helpen die anderen willen waarschuwen over een positieve testuitslag. Zodra Google dit probleem heeft opgelost, ontvangen CoronaMelder gebruikers weer meldingen en worden de nog niet gepubliceerde willekeurige codes alsnog gepubliceerd.

Ik blijf over dit incident in intensief contact met de andere lidstaten en met Google. Tot slot heb ik vandaag een formele datalekmelding gedaan bij de Autoriteit Persoonsgegevens. Ik zal gezien het belang van deze kwestie de Autoriteit Persoonsgegevens blijven informeren over de voortgang.

de minister van Volksgezondheid,
Welzijn en Sport,

Hugo de Jonge