Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

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)

Nr. 11 **AMENDEMENT VAN DE LEDEN VERHOEVEN EN VAN DER GRAAF**

Ontvangen 2 september 2020

De ondergetekenden stellen het volgende amendement voor:

In artikel I, onderdeel A, wordt aan artikel 6d een lid toegevoegd, luidende:

9. Onze Minister draagt ervoor zorg dat het in het tweede lid, onderdeel 4, bedoelde ip-adres van gebruikers zo snel mogelijk wordt gescheiden van de overige gegevens. Teneinde herleidbaarheid uit te sluiten is het verboden dit gegeven voorts aan andere gegevens, waaronder de gegevens bedoeld in het tweede lid, te koppelen.

Toelichting

Dit amendement beoogt het wettelijk regelen van niet-herleidbaarheid. Dit amendement volgt daarmee de tweede aanbeveling van Privacy Management Partners, die in opdracht van het Ministerie van VWS een tweede opinie gaven over de DPIA. Het is van groot belang de privacy van de gebruikers van de CoronaMelder zo adequaat mogelijk te beschermen. Dit is ook zeer belangrijk bij de privacy van geïnfecteerde gebruikers. Het is een goede zaak dat gegevens zo veel mogelijk decentraal verwerkt worden. Echter zijn er nog enkele waarborgen die genomen kunnen worden in de omgang met persoonsgegevens, zoals een wettelijk verbod op herleidbaarheid.

De in de CoronaMelder gebruikte Temporary Exposure keys (TEKs) en Diagnosis keys (DKs) zijn naar hun aard anoniem, maar zijn in combinatie met de IP-adressen in de back end wel herleidbaar tot een gebruiker. De TEKs en de DKs zijn aan te merken als persoonsgegevens omdat ze voldoen aan de volgende criteria: de unieke codes worden steeds gekoppeld aan een datum; de TEKs zijn samen met een bij de GGD op naam bekende autorisatiecode geüpload; de IP-adressen worden zeven dagen bewaard door het CIBG (met als doel het beveiligen van de CIBG infrastructuur tegen aanvallen van buitenaf).

Afspraak is dat het CIBG IP-adressen en overige gegevens apart zal opslaan. Deze afspraak lijkt niet te voldoen als adequate waarborg voor het tegengaan van gebruik van de gegevens door de overheid voor

kst-35538-11
ISSN 0921 - 7371
's-Gravenhage 2020

andere doeleinden. Het CBIG is namelijk een uitvoeringsorganisatie van het Ministerie van VWS, en onder de AVG niet gescheiden van de Minister. Een wettelijk verbod op herleidbaarheid kan ertoe dienen om extern gehandhaafd te kunnen worden, als beter alternatief op een interne afspraak tussen Ministerie en een daaronder vallende uitvoeringsorganisatie.

Als het verboden is om de IP-adressen te koppelen dan wel te laten koppelen aan de TEK's van de gebruiker, dan zal dit ook betekenen dat TEK's en DK's in de backend niet langer zijn aan te merken als persoonsgegevens en dus niet onder de AVG vallen. Dit lost twee eerder geconstateerde problemen op, zoals het feit dat het praktisch gezien onmogelijk is voor besmette gebruikers om hun toestemming in te trekken en het feit dat het Ministerie van VWS zich bij de uitoefening van inzage, correctie of verwijderingsrechten van de betrokkene steeds moet beroepen op art. 11 AVG, waardoor de AVG-rechten van de betrokkenen in de praktijk betekenisloos zijn.

Verhoeven
Van der Graaf