Bijlage Advies Functionaris voor gegevensbescherming VWS DPIA COVID-19 Notificatie app

Contactgegevens: FG-VWS@minvws.nl
Datum advies: 7 juli 2020

Inleiding FG

De functionaris voor gegevensbescherming is binnen het ministerie verantwoordelijk voor onafhankelijk toezicht op toepassing en naleving van de Algemene verordening gegevensbescherming. En heeft tot taak organisatieonderdelen te adviseren op uit te voeren en de uitgevoerde gegevensbeschermingseffectbeoordeling - GEB, hierna te noemen DPIA. Onderstaand advies heeft betrekking op de DPIA COVID-19 notificatie-app, versie datum 20 juni 2020.

Advies

Als doel van de voorgenomen gegevensverwerkingen staat in de DPIA aangegeven: 'om de bron-contactopsporing van de GGD-en te ondersteunen met een app die gebruikers waarschuwt als zij risicovol contact hebben gehad met een op COVID-19 positief getest persoon. Hierdoor neemt kans toeneemt dat potentieel geïnfecteerde personen eerder in beeld komen en – daarmee – dat een exponentiële uitbraak van het virus sneller wordt afgeremd.'

Informatie over wie wel of niet besmet is (geweest) met COVID-19, en wie van dichtbij contact heeft met wie is privacygevoelige informatie. Een dergelijke voorgenomen gegevensverwerking vereist dan ook een zorgvuldige ontwikkeling, opzet en inrichting.

Een cruciaal punt hierin is de herleidbaarheid van de gegevens. In deze DPIA wordt ervan uitgegaan dat door te kiezen voor een methode van DP3T protocol[1], te werken met pseudonieme gegevens (op zich zelf staande codes welke niet zijn afgeleid van andere gegevens maar volledig willekeurig worden bepaald) en te kiezen voor een decentrale structuur (waarbij behalve het uitwisselen van sleutels bij mogelijke besmetting alles op de mobiele telefoon gebeurt) de gegevens binnen de app redelijkerwijs niet herleidbaar zijn tot geïdentificeerde of identificeerbare natuurlijke personen. Een scala aan maatregelen zijn doorgevoerd om deze herleidbaarheid uit te sluiten, zoals onder andere: inzet van DP3T protocol, cryptographische technologie, dataminimalisatie, vrijgeven van de broncodes van de opensource software.

De back-end in het geheel kan de zwakke schakel vormen in de keten. Het is dan ook van groot belang dat hier van een goede beveilig is voorzien en maatregelen worden getroffen om de herleidbaarheid tot het minimum te reduceren. Op weg naar de livegang wordt een brede inventarisatie gedaan op het gebied van informatiebeveiliging en privacybescherming zowel door interne als externe verificatieslagen om de kwaliteit en de beveiliging van de totale oplossing (app plus back-end) te toetsen. Het advies is om deze toetsen niet enkel op weg naar de livegang uit te voeren maar op frequente basis toetsen door extern deskundige partijen op de informatiebeveiliging en privacybescherming en de daarbij genomen maatregelen uit te laten voeren.

Men gaat ervan uit dat de API[2] en het systeem waarvan de API onderdeel uitmaakt zo zijn ontworpen en opgezet dat Apple en Google geen toegang kunnen hebben tot de gegevens die betrekking hebben op de gebruikers. Dit blijkt uit de documentatie die Apple en Google daarover hebben bekendgemaakt, zijnde een verklaring van zijde Apple en Google. Waarbij opgenomen staat dat zij garanderen dat zij geen gegevens in het kader van het gebruik van de notificatie-app voor eigen doeleinden zullen verwerken. Daarnaast speelt mee dat Google en Apple geen cloud backups maken van de DP3T-gegevens, de API een losse software laag betreft dat niet in het besturingssysteem geïntegreerd is en er fysieke toegang tot de telefoon moet zijn. Het is hiermee

[1] DP3T protocol: Decentraliced, Privacy-Preserving Proximity Tracing.

[2] API: Exposure Notification Application Programming Interface (API)

een theoretisch risico dat enkel met de inzet van niet legitieme middelen door Google en Apple te achterhalen is welk persoon besmet is geweest.

In de DPIA wordt kort de Europese interoperabiliteitsambities voor de verschillende nationale tracing apps aangehaald. Hierover staat opgenomen dat om de voorgenomen Europese interoperabiliteit van de verschillende nationale apps te kunnen waarborgen, te zijner tijd mogelijk een landcode moeten worden toegevoegd vanuit de app. Omdat uitbreiding mogelijke gevolgen op de privacy van de gebruiker met zich meebrengt is het advies om alvorens hiertoe over te gaan een DPIA op deze verbreding uit te voeren.

Ten tijde van het opstellen van de DPIA wordt nog gewerkt aan een wetsvoorstel waarin het direct of indirect verplicht gebruik van de app expliciet wordt verboden. Dit gelet op de risico's van stigmatisering en uitsluiting van besmette personen en in relatie tot vrijwilligheid.

De DPIA voldoet aan de eisen te stellen aan een DPIA en is van een gewenste robuustheid. En zijn de privacy beginselen als dataminimalisatie, privacy by design, opslagbeperking in de opzet van de notificatie-app voorzien. Daarnaast is de grondslag waarop de gegevensverwerking is gebaseerd helder verwoord. En zijn de verantwoordelijkheden in de DPIA nader omschreven. Waarbij de verwerkingsverantwoordelijkheid op twee niveaus is neergelegd. De Minister van VWS voor de gegevensverwerkingen in het kader van de inrichting en het beheer van de notificatieapp en de AVG-verplichtingen die daarbij horen. En wordt de GGD als verwerkingsverantwoordelijke aangemerkt voor wat betreft het uitvoering geven aan de informatieverstrekking aan en het voldoen aan de zgn. AVG-rechten van de betrokkenen. Het gaat dan onder meer om de plicht om gebruikers te informeren, het recht op inzage en het recht op rectificatie. Er heeft een juridische toets op deze structuur van verantwoordelijkheden plaatsgevonden. Er blijkt hiervoor gekozen te zijn omdat het onwenselijk wordt geacht om de minister ook in deze gevallen als verwerkingsverantwoordelijke te beschouwen, omdat hij dan juist persoonsgegevens ten behoeve van de notificatieapp zou gaan verwerken en zou hiermee een onnodige gegevensstroom voor het uitoefenen van de rechten van betrokkenen tot stand komen.

Door de opzet van de app en de te nemen maatregelen ten aanzien van privacy risico's zoals beschreven in deze DPIA en het feit dat de restrisico's door de verwerkingsverantwoordelijke zijn gewogen is het alles overziend aannemelijk dat de verwerking geen hoog risico zal opleveren.

Gezien de uitzonderlijke situatie waarvoor de notificatie-app tot stand is gekomen is het advies dat de effectiviteit (nut en noodzaak) van de inzet van de app periodiek wordt geëvalueerd. Dit om zo goed inzicht te houden of de inzet van de notificatie-app een aanvulling biedt in de bestrijding van het virus. Sluit voor het uitvoeren van de evaluatie in ieder geval aan bij het momentum van eerdere beëindiging of verlenging van het ontwerpwetsvoorstel Tijdelijke wet notificatieapplicatie.

Het kan niet genoeg benadrukt worden dat de inzet van een dergelijke notificatieapp een uiterst zorgvuldige ontwikkeling, opzet en inrichting vereist. Gezien het maatschappelijke belang wordt dan ook aangeraden om bij de Autoriteit Persoonsgegevens diens advies in te winnen.