AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Aangetekend
De Minister van Volksgezondheid, Welzijn en Sport
Dhr. dr. E.J. Kuipers
Postbus 20350
2500 EJ Den Haag

Datum
13 januari 2022

Ons kenmerk
z2021-17465

Contactpersoon

070 8888 500

Onderwerp
Nieuwe DPIA CoronaMelder

Geachte heer Kuipers,

Op 6 augustus 2020 heeft de Autoriteit Persoonsgegevens (AP) uw ambtsvoorganger geadviseerd inzake de voorgenomen inzet van de COVID19 notificatie-app (hierna: CoronaMelder).[1] De AP adviseerde uw ambtsvoorganger: "*niet te starten met de voorgenomen verwerking totdat u de in het advies genoemde maatregelen heeft getroffenen en adviezen in acht heeft genomen*".[2] In navolging daarop is uw ambtsvoorganger in oktober 2020 overgegaan tot het landelijk introduceren van CoronaMelder.

De AP heeft uw ministerie in 2021 een aantal malen vragen gesteld over de wijze waarop nadere invulling is gegeven aan de aanbevelingen van de AP. Aanbevelingen welke een randvoorwaarde zijn voor het rechtmatig uitvoeren van verwerkingen van persoonsgegevens in en rondom CoronaMelder. Uw ministerie heeft daarbij aangegeven dat het begin 2022 een vernieuwde Data Protection Impact Assessment (DPIA) aan de Tweede Kamer zal sturen.

Een DPIA dient te allen tijde actueel te zijn en het publiceren van een actuele DPIA is een goed voorbeeld van een transparante manier van omgaan met verwerkingen van persoonsgegevens. Een voorwaarde daarbij is dat een DPIA juist en volledig is. In dat licht is het naar de mening van de AP dan ook noodzakelijk om, in een geactualiseerde en in het eerste kwartaal van 2022 nog te publiceren DPIA, stil te staan bij alle adviezen die de AP heeft verstrekt. Zonder volledig te willen zijn wil de AP in het bijzonder

[1] Advies op voorafgaande raadpleging COVID19 notificatie-app van 6 augustus 2020, z2020-11824
[2] Brief van de Autoriteit Persoonsgegevens van 6 augustus 2020, z2020-11824

wijzen op enkele punten die naar de mening van de AP *extra* aandacht behoeven in een geactualiseerde DPIA.

De AP acht het noodzakelijk om in het bijzonder *extra* stil te staan bij de volgende punten en nauwkeurig te onderbouwen wat de huidige status is:

1. Noodzaak verwerking persoonsgegevens.
   Zowel in haar advies bij CoronaMelder[3] als in haar wetgevingsadvies[4] van 9 juni 2020 heeft de AP stilgestaan bij het beginsel van noodzakelijkheid. De AP heeft uw ambtsvoorganger in beide adviezen gewezen op de uitwerking van dit beginsel, dat onder ander vergt dat wordt aangetoond dat een verwerking moet voldoen aan de beginselen van proportionaliteit en subsidiariteit. Nu CoronaMelder al enige tijd in gebruik is heeft uw ministerie kunnen beoordelen in hoeverre CoronaMelder voldoet aan deze beginselen in relatie tot andere gebruikte methoden bij bron- en contactonderzoek.

   De AP is echter van mening dat bij tussentijdse verlengingen van de inzet van CoronaMelder deze motivatie te summier is en onvoldoende aangeeft waarom CoronaMelder noodzakelijk is. Het beginsel van noodzakelijkheid vergt immers een zwaardere toets dan de beantwoording van de vraag of een middel kan bijdragen aan een doel. Mede daardoor acht de AP het noodzakelijk om in een geactualiseerde DPIA nauwkeurig en op basis van cijfers en (internationale) ervaringen met vergelijkbaar functionerende notificatieapps duidelijk te maken waarom de inzet van CoronaMelder noodzakelijk is.

2. Beveiliging van de (backend) systemen rondom CoronaMelder.
   Ten tijde van haar advies heeft de AP niet kunnen adviseren over de uiteindelijke inrichting van de servers die de backend van CoronaMelder vormen. Aanleiding hiervoor was dat er tijdens de procedure een andere partij werd gekozen die deze backend server ging verzorgen. De AP heeft zich in algemene zin uitgelaten over het niveau van de beveiliging van de backend server dat noodzakelijk was om te voldoen aan de eisen uit, in het bijzonder art. 32 van, de Algemene Verordening Gegevensbescherming (AVG).

   De AP neemt waar dat uw ambtsvoorganger stappen heeft gezet om de beveiliging van de verwerking goed in te richten. Zo is er een bug-bounty programma opgezet en bestaat de mogelijkheid om kwetsbaarheden snel te melden. Eventuele resultaten van deze initiatieven worden nu, voor zover de AP bekend, niet structureel gecommuniceerd.

   Uw ambtsvoorganger rapporteerde daarnaast over de beveiliging van de backend server. Bijvoorbeeld in de kamerbrief met kenmerk 1810215-216877-PDC19. Bij deze brief zijn een tweetal rapporten van Noordbeek Security bijgevoegd. In beide rapporten wordt aangegeven dat geen onderzoek is gedaan naar de 'werking' van de beheersingsmaatregelen. In het rapport "*ISAE*

[3] Advies op voorafgaande raadpleging COVID19 notificatie-app van 6 augustus 2020, z2020-11824
[4] Advies over het concept Tijdelijke wet maatregelen covid-19 van 9 juni 2020, z2020-09495

4401 rapport over assessment van de Backend van de CoronaMelder", is daarbij de volgende passage opgenomen: "*Wij adviseren de in dit rapport beschreven assessment op de opzet en bestaan van de Backend-omgeving en -processen in opbouw, te laten volgen door een volledige audit op het moment dat de omgeving en processen operationeel zijn. Dit dient een audit op opzet en werking te zijn. Hierbij wordt de operationele effectiviteit van de getroffen beheersmaatregelen getoetst*". In uw hierboven genoemde brief stelt u '*waar mogelijk*' aanbevelingen over te nemen en uit te voeren. Het is echter, ondanks een vraag hierover aan uw ministerie, voor de AP nog niet duidelijk welke verbeteringen uit de onderzoeken exact wanneer zijn doorgevoerd en welke aanbevelingen zijn overgenomen. In haar advies stelde de AP: "*Vanwege het ontbreken van een organisatie die de backend server host, zal de AP hier enkel kort ingaan op de situatie die voor de in de DPIA vermelde organisatie geldt. De standaarden betreffende technische en organisatorische maatregelen zoals vermeld in de DPIA waren voldoende voor de voorgenomen verwerking. Ook bij een nieuwe organisatie zullen de verwerkingsverantwoordelijken voldoende technische en organisatorische maatregelen moeten vastleggen om te voldoen aan de hoge standaarden die voor een verwerking als deze gelden. Vanzelfsprekend dient hier een verwerkersovereenkomst (artikel 28, derde lid van de AVG) te worden afgesloten. Dit geldt niet enkel voor de beveiliging, maar tevens voor de organisatorische maatregelen die waarborgen moeten bieden wanneer (bijzondere) persoonsgegevens worden verwerkt. Na de start van de verwerking dienen de verwerkingsverantwoordelijken de maatregelen te monitoren en waar nodig te versterken.*" [5]
De AP is van mening dat het, gezien de verplichting uit de AVG om een passend niveau van beveiliging van de verwerkingen te blijven waarborgen, wenselijk is om meer dan nu het geval is in detail stil te staan bij de in audits en onderzoeken gedane constateringen en aanbevelingen. Zowel als het gaat om de inhoudelijke risico's die worden gerapporteerd, waarbij dient te worden stilgestaan bij het moment van ontdekken en het moment van verhelpen van de risico's, als bij de aanbevelingen zoals het uitvoeren van een nieuwe audit naar opzet en werking.

Uiteraard dient daarbij, om het risico op inbreuken uit te sluiten, de situatie te worden voorkomen dat geconstateerde technische kwetsbaarheden worden gerapporteerd voordat deze zijn verholpen. Het kan daarvoor noodzakelijk zijn een periode van één a twee maanden 'achter te lopen' met het extern rapporteren van specifieke technische kwetsbaarheden of ervoor te kiezen dat die technische kwetsbaarheden alleen cijfermatig worden gerapporteerd, inclusief een datum waarop deze worden verholpen.

3. Afspraken met Google en Apple betreffende het Google Apple Exposure Notification framework.
De AP adviseerde onder andere : "*Schriftelijke contractuele afspraken te maken met Google en Apple, in lijn met mogelijk al bestaande afspraken op Rijksniveau, aangaande de werking van het Google Apple Exposure Notification framework in fase 1. Dit omhelst ook garanties en waarborgen aangaande de stelling van Google en Apple dat zij geen persoonsgegevens verwerken of gaan verwerken in het Google Apple Exposure Notification framework.*"[6]
De AP benadrukt dat het hier niet alleen ging om de zogenaamde API maar juist ook om de software die Google en Apple ontwikkelden en beheren. Mede in het licht van de stelling dat Google en Apple geen persoonsgegevens zouden verwerken. Daarbij dient te worden stilgestaan

[5] Advies op voorafgaande raadpleging COVID19 notificatie-app van 6 augustus 2020, z2020-11824, p. 19
[6] Advies op voorafgaande raadpleging COVID19 notificatie-app van 6 augustus 2020, z2020-11824, p. 18

bij de mogelijkheid van telemetrie die door Google en Apple wordt bijgehouden en de mogelijkheid dat meegeleverde applicaties van telefoonleverancier door instellingen toegang tot de gegevens op de telefoon krijgen. De AP heeft gesuggereerd deze aspecten ook internationaal te bespreken en waar mogelijk aan te sluiten bij initiatieven om gezamenlijk nadere afspraken te maken met Google en Apple.

Het is de AP niet duidelijk of, en zo ja welke, afspraken er additioneel zijn gemaakt naar aanleiding van het advies van de AP.

4. Beoordeling van de risico's in de DPIA.
Tijdens de procedure die uitmondde in het advies van de AP heeft de AP op 16 juli 2020 opmerkingen gemaakt bij zowel de methode die werd gehanteerd, als de in de methode opgenomen inschattingen van de kans en impact van voorvallen. De AP stelde onder andere dat:
" b. Binnen de risicoanalyse lijkt terminologie door elkaar te lopen. Het bruto risico is het product van kans en impact voordat mitigerende maatregelen worden getroffen. Het netto risico is het restrisico. Deze begrippen worden niet consequent gebruikt…
… c. Bij de inschatting van de risico's, onderdeel impact, lijkt geen gewicht te zijn toegekend aan de gewenst brede adaptatie van de app en de mogelijkheid dat ongewenste verwerkingen de rechten en vrijheden van een groot aantal natuurlijke personen raakt. Daar speelt bijvoorbeeld mee de mogelijkheid dat een aanval eenvoudig kan worden opgeschaald…
… d. Bij de inschatting van de risico's, onderdeel kans, lijkt de kans dat een gerichte aanval wordt uitgevoerd vaak relatief laag te worden ingeschat terwijl wordt beoogd de app binnen heel Nederland te gaan gebruiken. Dit laatste brengt met zich dat op veel fysieke plaatsen kan worden getracht aanvallen uit te voeren die, indien ze succesvol zijn, mogelijk leiden tot waardevolle informatie over bewegingspatronen van, en mogelijke ziekteverschijnselen bij mensen.."[7]
Inmiddels heeft uw ministerie na een jaar inzet van CoronaMelder een beter onderbouwd cijfermatig beeld van de risico's. Dit mede in het licht van incidenten die zich hebben voorgedaan. Het gaat daarbij zowel om de bruto risico's, de risico's die bestaan zonder mitigerende maatregelen, als de netto risico's, de resterende risico's na het nemen van mitigerende maatregelen. Dit vergt een in de geactualiseerde DPIA op te nemen nieuwe beoordeling van zowel het soort risico's dat zich kan voordoen, als uw inschattingen behorende bij deze risico's.

De AP adviseert u, naast het verwerken van deze punten in de DPIA, deze ook expliciet te adresseren bij het aanbieden van de DPIA aan de Tweede Kamer.

Openbaarmaking van deze brief

De AP is voornemens deze brief, indien daar aanleiding toe is, openbaar te maken, bijvoorbeeld op de website www.autoriteitpersoonsgegevens.nl.

[7] Brief van de Autoriteit Persoonsgegevens van 6 augustus 2020, z2020-11824 p. 2

Datum
13 januari 2022

Ons kenmerk
z2021-17465

Afsluitend

Indien u vragen heeft aangaande deze brief kunt u daarvoor contact opnemen met de in deze brief genoemde contactpersoon.

Een kopie van deze brief zal tevens ter informatie worden verstrekt aan uw Functionaris voor de Gegevensbescherming (FG).

Hoogachtend.
Autoriteit Persoonsgegevens,

Monique Verdier
vicevoorzitter