To: 5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e .
(5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e [5.1.2e]
Cc: 5.1.2e)[5.1.2e @minvws.nl]
From: 5.1.2e)
Sent: Thur 2/25/2021 3:43:25 PM
Subject: RE: Mail tbv Coronamelder
Received: Thur 2/25/2021 3:43:25 PM

5.1.2e

Dank je wel.

groetjes

5.1.2e
5.1.2e

@ 5.1.2e @minvws.nl
06 5.1.2e

5.1.2e
@ 5.1.2e @minvws.nl
06 5.1.2e

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: donderdag 25 februari 2021 16:21
Aan: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e
< 5.1.2e >
CC: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: RE: Mail tbv Coronamelder

Fijn. Dank!

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: donderdag 25 februari 2021 15:54
Aan: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e
< 5.1.2e >
CC: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: FW: Mail tbv Coronamelder

Dag 5.1.2e

De AP heeft mij in onderstaande e-mail kort gevraagd om in een volgende rapportage over CoronaMelder aan de Kamer informatie op te nemen over de genomen maatregelen op het gebied van privacy en security na de invoering van CoronaMelder. Specifiek vraagt de AP onder andere aandacht voor het opvolgen van de bevindingen van de Noordbeek audit, afspraken met Apple en Google en blijvend actualiseren van de DPPIA CoronaMelder.

Ik zorg ervoor dat de aandachtspunten van de AP worden opgepakt en kom met een voorstel wat in een volgende rapportage meegenomen kan worden.

Vriendelijke groeten,

5.1.2e

Van: 5.1.2e . < 5.1.2e @autoriteitpersoonsgegevens.nl>

Verzonden: donderdag 25 februari 2021 09:40
Aan: 5.1.2e) < 5.1.2e @minvws.nl>
CC: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e .
< 5.1.2e @autoriteitpersoonsgegevens.nl>
Onderwerp: Mail tbv Coronamelder

Geachte heer 5.1.2e beste 5.1.2e

Ongeveer een half jaar geleden heeft de AP haar advies op de Voorafgaande Raadpleging COVID19 notificatie-app uitgebracht. Kortgezegd, ons advies inzake CoronaMelder. In dat advies constateerden wij met genoegen dat de door VWS zelf ontwikkelde app was ontworpen volgens de 'privacy-by-design'-standaard. Ook wezen wij destijds op het door VWS toegepaste principe van dataminimalisatie. Inmiddels is de destijds voorgenomen verwerking al geruime tijd operationeel.

De AP constateerde in haar advies ook dat er nog maatregelen noodzakelijk waren om aan de AVG te voldoen. De AP stelde in haar advies: "Wij adviseren om niet te starten met de voorgenomen verwerking totdat u de in het advies genoemde maatregelen heeft getroffen en adviezen in acht heeft genomen." Het betrof daarbij de volgende maatregelen en adviezen:

1. Creëren van een tijdelijk wettelijke basis als grondslag voor de verwerkingen die plaatsvinden.
   Inmiddels is door de Minister invulling gegeven aan een wettelijke regeling voor CoronaMelder.

2. Afspraken maken met Google en Apple inzake het door hen ontwikkelde Google Apple Exposure Notification framework.
   Daarbij verwees de AP onder andere naar het DP3T project en onzekerheden aangaande telemetrie die Google en of Apple mogelijk toepassen rondom het Google Apple Exposure Notification framework.
   Destijds gaf de Minister aan dat er, kortgezegd, overleg was met Google en Apple, ook in Europees verband. De AP wil nogmaals wijzen op de noodzaak tot het maken van afdoende en bindende afspraken in dit kader. De in het advies door de AP aangegeven punten vormen daarbij een kader, het is echter aan VWS om zorg te blijven dragen voor passende afspraken met Google en Apple waarbij wordt gereageerd op veranderende omstandigheden zoals nieuwe risico's of inzichten in de processen, procedures of werkwijzen van Google en Apple. We verwijzen daarbij graag nogmaals naar ons advies.

3. Inrichten van een backend server die dient te voldoen aan de AVG-standaarden.
   Ten tijde van ons advies bestond er nog onzekerheid aangaande de invulling van de backend. Wij hebben over de uiteindelijke operationele invulling dan ook niet volledig kunnen adviseren. Inmiddels is hier door VWS invulling aan gegeven door het CIBG in samenwerking met KPN een rol te laten vervullen. Met genoegen constateren we ook dat er door de Minister wordt gerapporteerd over de beveiliging van die backend server. Bijvoorbeeld in Kamerbrief met kenmerk 1810215-216877-PDC19. We hebben echter wel een aandachtspunt daarbij.

   De Minister stelt in die brief: "*Informatiebeveiliging en privacybescherming CoronaMelder*
   Ook na landelijke introductie van CoronaMelder blijf ik mogelijke risico's voor de informatiebeveiliging en privacybescherming intensief bewaken en onderzoeken. Op mijn verzoek heeft het IT Audit en adviesbureau Noordbeek daarom onderzoek uitgevoerd op deze aspecten van de app. Hiertoe hebben zij onder andere de hardware en backendomgeving beoordeeld. De bevindingen tonen ook nu geen kritieke risico's aan. De constateringen en aanbevelingen zoals genoemd in de rapportages (zie bijlage 5 en 6) neem ik waar mogelijk over en worden uitgevoerd."

   Bijgevoegd bij de brief zijn inderdaad twee rapporten van Noordbeek Security. In die rapporten staan, zonder dat we willen suggereren volledig te zijn, een aantal punten die mogelijk verbetering behoeven. Kortgezegd stelt Noordbeek in één rapport dat de BIO-classificatie te laag is ingezet en daarbij acht Noordbeek Security het verstandig niet slechts op "*onze huidige beperkte steekproef binnen deze assessment*" te bouwen maar die uit te breiden. Daarnaast signaleren ze geen risico's inzake accountbeheer voor beheeraccounts en systeemaccounts maar ook : "*Wij missen echter een geaccordeerd overzicht van alle accounts in de Backend-omgeving, met een toelichting waarvoor deze zijn bedoeld en welke specifieke instellingen daarbij nodig zijn. Tevens hebben wij geconstateerd dat de relevante omgevingen ten tijde van ons onderzoek nog werden opgebouwd, waardoor geen volledige oordeelsvorming mogelijk was.*"
   In het algemeen stelt Noordbeek Security verder geen onderzoek te hebben gedaan naar de werking van maatregelen en daarbij onder: "*Volledige audit op de operationele Backend-omgeving*
   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."

Uit de door de minister aan de Kamer gezonden brief in combinatie met de datering van de assessments van Noordbeek Security en de introductiedatum van CoronaMelder, kan de indruk ontstaan dat er ten tijde van het operationeel worden van de verwerking, en mogelijk daarna, nog aanpassingen in de beveiliging noodzakelijk waren. De Minister geeft immers in januari 2021 aan "waar mogelijk" aanbevelingen over te nemen. Aanbevelingen die Noordbeek Security in december rapporteerde en mogelijk deels voortvloeien uit interviews die al hebben plaatsgevonden (augustus/september 2020) voor de (landelijke) introductie van CoronaMelder. (Bijlage A Overzicht van interviews en waarnemingen, ISAE 4401 rapport over assessment van de Backend van de CoronaMelder). Daarnaast waarschuwt Noordbeek Security zelf in beide rapporten voor de beperkte zekerheid die met de door hen uitgevoerde assessments wordt geboden. De verwerkingen die op de backend plaatsvinden dienen echter te allen tijde te voldoen aan de AVG en, ten aanzien van de beveiliging (waarbij verwerkers worden ingezet), in het bijzonder aan de artikelen 24, 26/28 en 32 AVG.

Mogelijk kan bij een volgende rapportage meer in detail aandacht worden geschonken aan de wijze waarop bij de (landelijk) introductie van CoronaMelder invulling is gegeven aan de bovenstaande adviezen van de AP. Met name ten aanzien van de afspraken met Google en Apple en de staat van de beveiliging van de backend, in het bijzonder in het licht van de adviezen van de AP en Noordbeek Security ten aanzien van de maatregelen die werden geadviseerd voor de (landelijke) introductie van CoronaMelder.

We hebben destijds geadviseerd op basis van een door VWS opgestelde DPIA. In dat verband is het ook goed om te wijzen op de noodzaak tot het actueel houden van die door VWS opgestelde DPIA.

Met vriendelijke groet,

5.1.2e

Secretariaat: 5.1.2e || M 5.1.2e
Bezuidenhoutseweg 30, 2594 AV Den Haag
Postbus 93374, 2509 AJ Den Haag

AUTORITEIT
PERSOONSGEGEVENS

5.1.2e