To: (10)(2e) [2)(2e) (10)(2e)][(10)(2e) @minvws.nl]
From: (10)(2e)
Sent: Fri 8/7/2020 9:22:45 AM
Subject: Opmerkingen advies AP
Received: Fri 8/7/2020 9:22:45 AM
z2020-11824 Kopie Advies op voorafgaande raadpleging COVID19notificatie-app.pdf
z2020-11824 Kopie Brief bij advies.pdf

Enkele delen van het advies zijn goed bruikbaar en maken het geheel beter, de samenvattende conclusie en onderliggende redenen zijn ons inziens juridisch onjuist en zullen we gemotiveerd weerleggen. Een van de kernpunt is dat huidige wetgeving geen voldoende grondslag biedt voor deze verwerking. Dit was reeds voor aangekondigd. Dat is onderbouwd en prima om in mee te gaan. Vervolg stelling van AP dat toestemming niet passend is, is slecht onderbouwd en de AP gaat voor het gemak volledig voorbij aan het feit dat deze grondslag in diverse andere landen staande praktijk is (die meer persoonsgegevens verwerken). Dat dit een van de mogelijke grondslagen is die in de AVG genoemd is doen zij wat mij betreft veel te gemakkelijk af. Van een gemeenschappelijk lezing van de AVG in de EU is blijkbaar geen sprake. Dit punt gaan we gemotiveerd weerleggen.

AP wil voor start van de verwerking een volledig afgeronde DPIA inclusief advies van FG-en. Dit is echt aanpoten. De landsadvocaat gaat hier het grootste gedeelte van het werk voor uitvoeren. We gaan alles inzetten om dit voor elkaar te krijgen.

Zie onderstaand alle punten. De LA analyseert ook nog het advies. Deze gaan we nog naast elkaar leggen om er zeker van te zijn dat we alles hebben. Komend weekend wordt hard doorgewerkt aan het aanpassen van de DPIA met als doel om dinsdagochtend een versie van de DPIA gereed te hebben die aan de FG-en die meedoen aan de proefperiode voor te leggen (Twente en Drente).

Punten opgemerkt uit eerste lezing advies:

- voor AP onduidelijk is wie de server gaat beheren.
  - Dit is al goed belegd. Het CIBG voert het beheer en wordt door KPN ondersteunt. Dit is reeds medegedeeld aan de AP zal worden beschreven in DPIA.
- Bij intrekken toestemming worden de RPI's die de telefoon van de gebruiker heeft uitgezonden en die door andere gebruikers zijn opgevangen niet verwijderd. Het recht op vergetelheid wordt daardoor niet toegepast. (zeer uitgebreid reageren).
  - niet juist. Dat dit niet kan in een privacy maatregel. Zoals duidelijk uiteengezet gaan we er zekerheidshalve vanuit dat de uitgezonden RPI's persoonsgegevens zijn. Dit omdat die in de hele keten inclusief melden besmetting en contact met de GGD in uitzonderlijke gevallen in een heel klein gedeelte van het proces mogelijk herleidbaar kunnen zijn. Als de gebruiker geen positieve test heeft gehad is hiervan geen sprake. Herleidbaarheid is dan uitgesloten en daarmee zijn het geen persoonsgegevens en in de AVG niet van toepassing. Recht op vergetelheid daarmee ook niet.
  - In het geval dat de persoon zich wel ziek heeft gemeld is….
- Niet alleen voor livegang (etische) toetsen, maar ook daarna
  - Prima idee, gaan we doen
- 4.2.1 risicobeoordeling gebeurt Apple google API. Dat komt niet overeen met DPIA.
  - Volgens ons niet, maar het gebeurt inderdaad in de DPIA. We zullen dit duidelijker beschrijven in de DPIA.
  - Bovendien wordt er met Europese samenwerking een codereview doen
- 4.2.1 bullets technisch nagaan. De TEKs brengens volgens mij geen betere bescherming, die worden namelijk niet gedeeld.
- 4.2.1 tweede fase van apple google volgen. Geen onderdeel van dit traject. Onzekere gebeurtenis en geen onderdeel van dit proces. Prima om te volgen maar als apart traject los hiervan.
- 4.3.1 tijdelijke wet kan oplossing bieden, maar is geen onderdeel van de officiele stukken. Daarom niet kunnen beoordelen. Vreemde argumentatie aangezien het vertrouwelijk is toegestuurd omdat het stuk bij de raad van state ligt. Is geen amvb maar wet
- 4.3.1 er moeten aanvullende afspraken gemaakt worden met apple google. Aangezien code openbaar is prima te zien hoe de api van google apple werkt. Nadere afspraken niet nodig, is ook niet iets dat andere landen hebben gedaan (navragen bij dirk Willem).
- 4.3.1 Effectiveit van de app niet bewezen doordat technologie nog niet eerder op deze manier is toegepast. Om te voldoen aan noodzakelijkheidvereiste moet bij voortdurend inzichten vanuit binnen en buitenland worden gewogen en geadresseerd.
  - Prima advies, wordt reeds (10)(2e) besproken
- Tijdigheid en verbod verplicht gebruik regelen.

  - Goed advies, wordt uitgewerkt.
- Uitleggen in welke gevallen een beroep op artikel 11 van toepassing is:
  - In alle gevallen. Zal uitgebreid uit worden gelegd.
- 4.4.2 uitleg telemetrie google play services
  - Brenno geeft uitleg
- 4.4.3 Ingaan op verzoek toestemming locatiegegevens bij google. AP verwijst naar advies begeleidingscommissie.
  - Gemotiveerd van afwijken
- 4.4.4 Niet alle voorgenomen maatregelen reeds uitgevoerd.
  - AP specificeert niet welke, maar de bevinding is in basis juist. Diverse tests die zijn genoemd worden nog uitgevoerd en zijn inderdaad niet gedaan. Dit verloopt echter wel volgens planning.
- 4.4.4 "Tevens is de rapportage van de broncode-kwaliteit niet aangetroffen in de publieke opslagplaats van de broncode (code-repository) en is de broncode summier becommentarieerd."
  - Dit is in basis juist, Brenno maakt reactie. Wordt namelijk nog uitgevoerd.
- Daarnaast is er bij de beoordeling opgemerkt dat er geen code-review wordt gedaan in de publieke broncode. Dit draagt niet bij aan de transparantie van de ontwikkeling van de notificatie-app.
  - Onjuist dit gebeurt wel
- 4.5 voorgenomen evrwerking is nog in ontwikkeling
  - Juist
- In DPIA enkel technische risico's benoemd
  - Niet geheel juist, maar heeft de AP in zijn vragen ook benoemd. Als antwoord op de vragen tevens een lijst van risico beoordeling conform overweging 75 AVG. Ap lijkt deze niet mee te nemen.
- 5 inleiding nietszeggend
- Noemen van dag van de besmetting brengt mogelij risico tot identificatie emt zich mee. In DPIA onvoldoende onderbouwd risico,
- Enkel verbod opnemen in wet geen maatregel onder AVG
  - Volgens mij onjuist. Als iets illegaal is (gemaakt) door middel van een wet dan hoef je het in beginsel niet mee te nemen als risico en daarmee ook geen maatregel te nemen. Het verbod is namelijk de maatregel
  - Er wordt echter een meldplicht ingericht en het verbod zal worden gehandhaafd als de Staten Generaal het wetsvoorstel waarin het verbod in wordt geregeld aanneemt.
- 5.2 opnemen als tekst dat we goed bezig zijn
  - PDCA cyclus toezeggen
- 5.3 wetgeving moet eerst geregeld worden voordat grondslag er is.
  - Wetgeving niet op tijd gereed, noodzaak te hoog om te wachten. Wordt overgestapt op expliciete toestemming
- 5.3 afspraken moeten gemaakt worden met GGD-en voor verdeling verantwoordelijkheden (vast te leggen over de verdeling van taken, omgang met persoonsgegevens, en de waarborgen voor betrokkenen.)
  - Deze overeenkomst is in voorbereiding en wordt gesloten
- Uitvoering rechten van betrokkene moet goed belegd zijn
  - Dit wordt goed ingeregeld en hier worden goede afspraken over gemaakt.
- Back-end server moet aan zelfde standaard voldoen als beschreven maatregelen belastingdienst.
  - Een andere partij betekent op nuance andere uitvoering van de maatregelen. Hetzelfde niveau van maatregelen wordt toegepast.
- 5.5 onvoldoende duidelijk of en zo aj welke persoonsgegevens apple en google verwerken in het framawork
  - Apple en google verwerken geen persoonsgegevens in het framework, zij treden enkel op als software leverancier.
- Onvoldoende duidelijk of zij doel en middelen bepalen en daarmee verwerkignsverantwoordelijke zijn.
  - Zowel bij het ministerie als bij apple en google is die onduidelijkheid er niet. Apple en google bepalen geen doel en middelen en zijn geen verwerkingsverantwoordelijke. Zij zijn enkel software leverancier.
- AP noemt meermaals de tweede fase en ook dat het advies hier niet over gaat.
  - Het ministerie deelt het standpunt van de AP dat deze verwerking niet over de tweede fase gaat en zal op die opmerkingen voor deze verwerking niet meenemen.
  - Als apple en google in de toekomst zelfstandig gegevens gaat verwerken in dezelfde context in het de taak van de AP om hierop toe te zien.
- Ontbreken van afspraken met apple en google is onvoldoende om als verwerking van het geheel van start kunnen gaan.
  - Sterk aandachtspunt: apple en google nogmaals benaderen voor statement geen verwerking van persoonsgegevens in eerste fase.
  - Nagaan of duidelijk genoeg omschreven in licentie anders vervolgactie nemen. Benadrukken at het enkel om eerste fase gaat.
- Op grond van de ontvangen informatie en het voorgaande concludeert de Autoriteit Persoonsgegevens dat de

voorgenomen verwerking COVID-19 notificatie-app zoals beschreven ten minste inbreuk zou maken op artikelen 5, 6, 9, 32 en 35 van de AVG.
    - Verzamelconclusie op basis van voorgaande en volgende.
- 6 maatregelen
- 6.1.1Afspraken maken over verwerkingsverantwoordelijkheden met apple google
    - Geen afspraak over verwerkingsverantwoordelijkheden, maar wel proberen bevestiging enkel softwareleverancier. AP brengt geen redenen aan om aan te nemen dat apple google wel persoonsgegevens zouden verwerken.
    - Geheel gaat enkel over fase 1. Geen afspraken nodig over latere fase
- 6.1.2 Heldere afspraken maken over beeindiging app en toepassing api stopt
    - Deze is er al. Dit is echter niet enkel gelinkt aan de nederlandse app. Gebruikers kunnen ook andere apps downloaden. Minister enkel inspraak over inzet nederlandse app.
- 6.1.3 verwijdering gegevens na verwijdering app.
    - niet automatisch verwijderd, maar volledig in control door gebruiker en na uiterlijk 1 dagen alsnog verwijderd.
- 6.1.4 wederom toch noemen tweede fase
    - Gaat deze app niet over. In seperaat traject behandelen. Eigenstandige rol van de AP
- 6.2 zonder passende wetgeving app niet mogelijk
    - Onjuiste stelling. Huidige wettelijk taak van de minister niet specifiek genoeg. De AP is hier onvolledig. De AVG biedt de mogelijk om op basis van expliciete toestemming dergelijk gegevens te verwerken. Minister heeft reeds voldoende waarborgen genomen om op basis van deze expliciete toestemming te starten. Diverse aanbevelingen van de AP zullen worden overgenomen.
- 6.2 verbod verplicht gebruik moet wettelijk verankert worden.
    - is juist en is reeds in voorbereiding. Geen belemmering om te starten gezien de uitgebreide mogelijkheden in de app en api om gegevens te verwijderen wanneer het de gebruiker wil. Overal blijkt vrijwilligheid en eigen regie van de gebruiker uit.
- 6.3. backend server moet goed beveilig zijn en er moet verwerkersok gesloten worden met partij.
    - Fijn dat AP de beschreven maatregelen als afdoende beschouwd. Wij nemen de aanbeveling eerder uit het advies graag over dat we continu de beveiliging zullen blijven testen. Hetzelfde niveau van beveiliging wordt gehanteerd uitvoering is op nuance verschillend en zal opnieuw beschreven worden.
    - Verwerkersovk wordt gesloten met KPN
- 7.1 tijdigheid moet geadresseerd worden
    - Juist dit moet nader uitgewerkt worden. einddatum kan, maar heeft in eerste instantie niet de voorkeur
- 7.1 DPIA moet volledig klaar en met advies van de FG klaar zijn om te kunnen starten met verwerking
    - Dit is nagenoeg onmogelijk
    - Hiervoor moeten ook alle FG's van alle GGD-en advies geven binnen een week inclusief FG VWS.
    - 7.1 WJZ en LA vragen extra stuk 7.1 uitbreiding DPIA
- 7.2 afspraken maken tussen verwerkingsverantwoordelijken
    - Reeds in voorbereiding
- 7.3 risico google play store en telemetrie mitigeren
    - Mogelijk of voldoende extra uitleg geven? vraag aan Brenno
- 7.3 aanpassing geldigheid TEKs
    - Vanuit het oogput van invloed op de betrokkene geen goed idee. Hiermee wordt het dataverkeer 6-12 keer vergroot. Er worden door de verkorting van de geldigheid namelijk 6-12 keer meer TEKs aangemaakt in de 14 dagen waarin de TEKs bewaard blijven en daarmee in geval van besmetting geupload worden én de download wordt 6 tot 12 keer zo groot om dezelfde reden.
- 7.3 techniek shared secrets toepassen op RPI's – vraag om mee te nemen in doorontwikkeling app.
    - Onbekend met techniek (vraag Brenno)
- 7.3 laatste 5 bullets:
    - 1 Wordt aangepast in versie 11 van android. Deels opgelost met deze update deels geen showstopper omdat het een administratief veschil van mening is en hiermee geen aanvullende geen aanvullende gegevens worden verwerkt.
    - 2 uitschakelen van maken van screenshots wordt bekeken om toe te voegen aan wensenlijst. Geen reden om niet van start te gaan.
    - 3 traject voor verified built in gang gezet (loopt reed bij LA)
    - 4 publiceren van code review en uitslagen zullen we doen
    - Onduidelijk wat gewenst wordt.

Algemene opmerking:

- De AP gaat vrij ver in de reikwijdte van de beoordeling. Het toezicht ziet op toepassing van de AVG/privacy, niet op het gehele proces van het bouwen van de app.
- Nergens in het advies wordt de bijzondere omstandigheden van de DPIA meegewogen. Privacy is een risico afweging, de AP geeft hier geen blijk van. Bijzondere omstandigheid benadrukken in DPIA.