To: 5.1.2e [5.1.2e @cuccibu.nl]; 5.1.2e [5.1.2e @joanknecht.nl]; 5.1.2e , 5.1.2e [5.1.2e @ggdghor.nl]; 5.1.2e)[5.1.2e @minvws.nl]
Cc: 5.1.2e - 5.1.2e 5.1.2e @dpa.nl]; 5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e . (5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e @ggdghor.nl'[5.1.2e @ggdghor.nl]
From: 5.1.2e
Sent: Tue 11/17/2020 9:46:13 AM
Subject: Re: Concept DPIA App oplossing 2
Received: Tue 11/17/2020 9:46:23 AM

5.1.2e

5.1.2e en ik werken samen dus dit is het.

Wat betreft punt 6: dat staat niet zo in de DPIA en de verplichtende basis moet eerst uit onderzoek blijken. Daarna moet nog eens gaan blijken of het kan en langs welke route. Een voorschot nemen op wankele juridische basis zou dat proces zelfs kunnen frustreren (argument doelredenering).

Ik stel voor dat we de lijn van 5.1.2e volgen.

Hartelijke groet,

5.1.2e

Op 17-11-2020 om 09:27 schreef 5.1.2e :

> Goedemorgen 5.1.2e
>
> Dank voor de terugkoppeling. Hieronder op enkele punten kort alvast een toelichting.
> @ 5.1.2e Ik vroeg mij af of hier reeds ook feedback vanuit jou kant in is opgenomen? Dit i.v.m. de planning zodat ik weet of ik rekening moet houden met nog een terugkoppeling.
>
> Met vriendelijke groet,
>
> 5.1.2e
>
> cuccibu
> Reduce Risk, Create Value
>
> 5.1.2e @cuccibu.nl / +31 (0) 5.1.2e
>
> **Cuccibu B.V.**
> +31 (0) 85 303 29 84
> Boutenslaan 195C, 5654 AN, Eindhoven ,
> Olof Palmestraat 16, 2616 LR, Delft
> www.cuccibu.nl
>
> **Van:** 5.1.2e 5.1.2e >
> **Verzonden:** dinsdag 17 november 2020 00:56
> **Aan:** 5.1.2e < 5.1.2e @cuccibu.nl>; 5.1.2e < 5.1.2e @joanknecht.nl>; 5.1.2e < 5.1.2e @ggdghor.nl>
> **CC:** 5.1.2e < 5.1.2e @minvws.nl>; 5.1.2e - 5.1.2e < 5.1.2e @dpa.nl>; 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e < 5.1.2e @minvws.nl>; 5.1.2e @ggdghor.nl' < 5.1.2e @ggdghor.nl>
> **Onderwerp:** Re: Concept DPIA App oplossing 2

Beste 5.1.2e

De DPIA heb ik de afgelopen week helemaal doorgewerkt en er zijn veel problemen die uit het document blijken. Ik vrees dan ook niet dat de DPIA morgen naar de GGD'en zal kunnen.

Ik begin met het meest ernstige probleem: er zijn meerdere risico's aangeduid als hoog-hoog dus hoog. Dit betekent dat AVG verplicht tot het houden van een voorafgaand raadpleging en daarmee riskeert de GGD GHOR **maanden vertraging**. Afgaande op de tekst zou dan een verwerkingsverbod mij niet verbazen. Het lijkt mij van het grootste belang om de risico's fors te verkleinen.

Er zijn nogal wat problemen. Ik heb ze zo uitgebreid mogelijk in notities beschreven. Ik wil de belangrijkste punten langslopen:

1. Een DPIA moet de risico's voor betrokkenen in kaart en welke maatregelen de verwerkingsverantwoordelijke moet nemen om de risico's te verkleinen. Deze DPIA beschrijft veel zaken, maar nauwelijks risico's en maatregelen. Daarvoor wordt naar andere mensen verwezen voor de inkleuring. Normaliter zoek je daar gezamenlijk na en is het geen invuloefening. 5.1.2e heeft de eerste stap gezet bij de kickoff, waar door het proces is gelopen. Vervolgens vraag je - zie ook hieronder - of mensen zelf maatregelen inkleuren. Daarmee wordt de wereld omgedraaid: we matchen maatregelen op risico's. Het moet juist zijn dat er maatregelen uit de DPIA vloeien die worden geïmplementeerd, zodat de restrisico's zo klein mogelijk worden.
2. De hele procesbeschrijving kan veel helderer. Het is voor mij soms lastig te volgen wat er nu wordt gemaakt. Dit gaat een buitenstaander (bijvoorbeeld een toezichthouder) niet duidelijk zijn. Dat kan tot ongelukkige misverstanden leiden. Precies hebben we bij de kickoff het proces in kaart gebracht. Ik zie dat eigenlijk nauwelijks terug. Het gevolg is dat het totaalplaatje vaag is.
3. De GGD GHOR staat neergezet als verwerkingsverantwoordelijke. Dat vind ik juridisch niet overtuigend. Uit DPIA blijkt niet dat zij een mandaat om doel en middelen te bepalen voor de verwerking. Als ze dat wel doen, vraag ik me af hoe dat juridisch te regelen is. Zij spelen in de Wpg geen rol en zij zijn zeker geen bestuursorgaan (Afdeling Bestuursrecht Raad van State - 5.1.2e . Kortom in die rol roept dat op zijn zachtst gezegd vraagtekens op. Het lijkt mij dat een vereniging zaken doet ten behoeve van de leden. Ze bepalen misschien middelen, maar zeker geen doel. Kortom dat maakt ze toch echt verwerker.
4. Er wordt gesteld dat er geen sprake zou zijn van een grootschalige verwerking zonder dit te onderbouwen. De unieke positie van de GGD bij infectiebestrijding is op zichzelf al reden om te twijfelen aan die stellingname. Maar daarbij is er sprake van grote aantallen mensen bij infectieziekten. Alleen COVID-19 is voldoende om dit een grootschalige verwerking te noemen. Ik denk dat je dit bij een toezichthouder niet gaat drooghouden. De extra beschreven maatregelen zijn wel iets om te overwegen. Daarnaast wijs ik opnieuw dat de minister juist de privacy zo goed wil borgen. Kortom weer een reden om geen shortcut te nemen. Klopt dit is in de nieuwe versie van dit weekend al reeds aangepast.
5. Informatiebeveiliging. Op dit moment krijgt informatiebeveiliging in de DPIA nauwelijks aandacht. Zo wordt niet aangesloten bij standaarden, zoals de BIO (niveau 2+) en de NEN7510. Wil je aansluiten bij de Wpg om daarmee de rechtmatigheid (rechtsgrond) in te kleden dan hoort daar ook echt informatiebeveiliging een plek te krijgen. Dat doe je niet met losse maatregelen. We weten dat onze toezichthouder (begrijpelijkerwijs) hecht aan een goede PDCA-cycle (en die vloeit uit genoemde standaarden). Ik zie dat nergens terug.
6. Zelf schrok ik behoorlijk van de redenering dat er in de DPIA dat er geen verplichting was in de wet om mee te werken met BCO ("Het verstrekken van de persoonsgegevens van de contacten is niet expliciet opgenomen in de wet, maar blijkt op grond van het hierboven gestelde impliciet uit art. 35 lid 1 jo 37 Wpg jo. 6 lid 2 sub c Wpg"). Maar via een u-bocht wordt deze toch geconcludeerd uit de bevoegd om andere maatregelen te nemen. Los van het rechtszekerheidsbeginsel uit de algemene beginselen van behoorlijk bestuur schuurt dit met onze democratische rechtsstaat. De juridische redenering vond ik niet overtuigend, maar ik vind de beweging wel gevaarlijk en onwenselijk. Dat staat nog los van het feit dat minister heeft zeer duidelijk heeft gemaakt dat we niet mensen gaan dwingen. Maar als je toch deze mening poneert dan is het onacceptabel om data op de mobiel niet meer te verwijderen (bij het stuk over retentie). Als er sprake van dwang dan volgt daaruit ook verantwoordelijkheid en moet gegevens na 48 uur worden verwijderd. Los van de dwang is dat bij het aanbieden van de applicatie iets wat mag worden verwacht.
Zie hier een kamerbrief van inzake update bron- en contactonderzoek en quarantaine. Hier wordt ook gesproken dat er momenteel onderzocht wordt of er mogelijkheden zijn om medewerking aan bron-en contactonderzoek minder vrijblijvend te maken of zelf verplicht te stellen.
https://www.rijksoverheid.nl/documenten/kamerstukken/2020/08/11/kamerbrief-inzake-update-bron-en-contactonderzoek-en-quarantaine, p. 5-6

7. De rol van de minister wordt er minimalistisch neergezet. Ik herken me hier totaal niet in, omdat deze weldegelijk een taak heeft. Niet alleen in de Wpg, maar op basis
8. Zoals ik de DPIA lees, wordt er data op het device opgeslagen. Dan lijkt het mij dat de Telecomwet ook een rol gaat spelen en er toestemming moet worden gevraagd.
9. Bij geheimhouding wordt wel heel makkelijk uitgegaan van kloppende maatregelen. Dat is maar zeer de vraag of dat terecht is. Je hoort hierop te toetsen of de controls ook in place zijn. Zeker door alle publiek geworden incidenten mogen we hieraan twijfelen.
10. Bij de noodzaak en evenredig lees ik opeens dat er wisselend handelingsperspectief kan zijn op basis van vragen. Als dat het geval is dan moet je jezelf ook de vraag stellen of de app dan valt onder de Medical Device Regulation (EU 2017/745). Dat lijkt mij het kader waarop dan ook moet worden getoest ook in het kader van de DPIA (het gaat immers om) rechten van betrokkenen.

In het document heb ik zo uitgebreid uitgelegd welke problemen ik verder zie. Maar op dit moment is dit niet een DPIA die je richting afronding afmaken. Er moet nog veel werk worden gedaan, want er is wel veel om bezorgd over te zijn.

Hartelijke groet,

5.1.2e

Op 08-11-2020 om 22:39 schreef 5.1.2e:

Hi allen,

Op de teams-pagina is de laatste versie van de DPIA te vinden.
Graag zou ik willen vragen of jullie vanuit IB naar bijlage 3 zouden kunnen kijken en daarin de eventuele maatregelen die er genomen zijn kunnen invullen/aanvullen.
Daarnaast is er op pagina 18/19 ruimte om een uiteetzetting te geven van de technische maatregelen die er genomen zijn. Zouden jullie deze ook kunnen invullen/aanvullen.
Het lijkt mij het makkelijkste indien jullie vanuit het gedeelde document op teams werken zodat we van elkaar kunnen zien welke aanvullingen er al reeds gedaan zijn.

Tevens heb ik enkele risico's in het rood toegevoegd aan het register op Teams. Ik heb nog geen tijd gehad om de kans en impact te bepalen, maar dan zijn weten jullie alvast dat de rood toegevoegde risico's vanuit de DPIA komen.
Met vriendelijke groet,

5.1.2e

cuccibu

5.1.2e @cuccibu.nl / +31 (0) 6 5.1.2e

Cuccibu B.V.
+31 (0) 85 303 29 84
Boutenslaan 195C, 5654 AN, Eindhoven ,
Olof Palmestraat 16, 2616 LR, Delft
www.cuccibu.nl