

Aan: [REDACTED]
 Van: [REDACTED]
 Datum: 30 oktober 2020
 Onderwerp: Risicoanalyse op hoofdlijnen
 Kopie aan: [REDACTED]

1. Inleiding

In de afgelopen dagen hebben wij een viertal documenten gelezen die betrekking hebben op de ontwikkeling van de app die bedoeld is om de gegevenslevering aan GGD'en ten behoeve van het bron- en contactonderzoek te ondersteunen. Het gaat om de volgende documenten:

- Ontwerpkeuzes applicatie Thuisrapportage versie 0.41;
- Functionaliteit applicatie Thuisrapportage versie 1.01;
- Specificatie eerste versie oplossing 2 (IZB) app versie 1.0;
- Plan van aanpak oplossing 2 (IZB) app versie versie 0.95.

In deze notitie geven wij onze eerste beelden. Die vallen uiteen in de beschrijving van een aantal zaken die ons in positieve zin opvallen, de belangrijkste risico's die wij op dit moment zien en een aantal aandachtspunten voor het programma.

Wij hebben ons bij het schrijven van deze notitie gebaseerd op papieren documentatie. Dat brengt het risico met zich mee dat wij zaken over het hoofd hebben gezien dan wel dat het programma inmiddels verder is gevorderd dan uit de documentatie blijkt. Daarom hebben wij op 27 oktober 2020 een gesprek gevoerd met [REDACTED]. In dat gesprek hebben wij de belangrijkste risico's besproken zoals wij die waarnemen. Aan de hand van het gesprek met [REDACTED] hebben wij waar nodig de notitie aangescherpt.

2. Positieve waarnemingen

- De keuze voor een "appetizer" (die ondersteunt stapsgewijze ontwikkeling en levert tegelijkertijd snel eerste resultaten).
- Het beleggen van het beheer van de app bij de GGD (VWS is daar als beleidsdepartement minder goed voor geëquipeerd).
- De voorziene dagelijkse sturing op het ontwikkeltraject (dat is noodzakelijk in het licht van de zeer korte ontwikkeltermijn).
- Het gebruik van de basisvoorziening van de GGD'en om gegevens uit te wisselen (dat is een bestaande standaard).
- Aanpasbare vragenlijst, teksten, etc. (om onnodige releases van de app te voorkomen).
- De keuze om de GGD "snap shot" gegevens te laten gebruiken (dat voorkomt een heel complexe oplossing om de gegevens in de app en die bij de GGD te synchroniseren).
- Een aantal ontwerpkeuzes is geëxpliciteerd. Dat zorgt ervoor dat betrokkenen voorafgaand aan de ontwikkeling kunnen instemmen met de gekozen koers.

3. Belangrijkste risico's binnen de gekozen aanpak

Wij hebben de belangrijkste risico's thematisch gerangschikt:

- *Doel oplossing 2*
 - Het doel van Oplossing 2 is om de gegevenslevering aan GGD'en ten behoeve van het BCO te ondersteunen. Achtergrond hierbij is het feit dat naarmate er meer mensen besmet raken met het virus, het steeds meer werk is voor de GGD'en om het BCO uit te voeren. Het nut van Oplossing 2 is daarmee afhankelijk van de mate waarin het BCO door de GGD wordt uitgevoerd (ontlasten GGD). De GGD heeft inmiddels aangegeven dit niet meer grootschalig te doen en het BCO enkel in te zetten voor kwetsbare groepen zoals ouderen. Doorgaans is dit niet de groep die het eerste een app installeert.
 - Het is van belang om gedurende de Coronacrisis naar het nut en het doel van Oplossing 2 te blijven kijken om te voorkomen dat je het paard achter de wagen spant (hoe meer de app gebruikt wordt hoe eenvoudiger en frequenter GGD'en het BCO kunnen inzetten, maar de app heeft pas toegevoegde waarde wanneer het BCO in aanzienlijke mate wordt ingezet) .
 - In het verlengde hiervan, bij het lezen van het doel 'Het sneller benaderen van vermoede gevallen, bijvoorbeeld in afwachting van een testuitslag, zodat deze tijdig in thuisisolatie gaan, advies op maat krijgen en transmissie wordt voorkomen', rees bij ons de vraag: die informatie heb je toch al als er een test is gedaan?.
 - Blijf daarbij ook kijken naar nut en noodzaak van doelen voor latere updates (dynamisch managen van beoogde baten), zoals: 'Patiënten zijn zelf in staat om hun contacten te informeren over hun besmetting, waardoor de BCO-medewerker wordt ontlast'. Mensen hebben al hun eigen contacten in hun telefoon (geen app voor nodig) óf ze kennen ze niet. In dit laatste voorziet Oplossing 1.
- *Integraliteit van de oplossing*
 - Partijen moeten zich realiseren dat de app maar een (klein) puzzelstukje is in het geheel van het BCO.
 - Om het BCO op orde te krijgen zijn meer en ook andere maatregelen nodig dan alleen de ontwikkeling van een app.
 - Het is dan ook van belang het BCO als geheel van (organisatie)processen, ICT-voorzieningen en besturing te beschouwen en van daaruit te werken aan verdere optimalisatie.
- *Besturing*
 - De ontwikkeling van de app vindt onder grote tijdsdruk plaats, het doel is de app per eind oktober 2020 in gebruik te nemen.
 - Het aantal betrokkenen bij ontwikkeling en implementatie is buitengewoon groot.
 - Er is daarnaast sprake van een groot aantal parallel uit te voeren activiteiten, bij veel verschillende partijen.
 - De GGD'en zijn zelfstandige organisaties, die regionaal georganiseerd en bestuurd zijn. Dit maakt het feitelijk onmogelijk om de GGD'en landelijk aan te sturen.
 - De combinatie van deze factoren zorgt voor grote complexiteit in de besturing en in de uitvoering van activiteiten.

- Er is feitelijk sprake van een "militaire operatie". Zo'n operatie vergt heldere en strakke sturing vanuit één punt, door één persoon die het totaaloverzicht heeft en regie voert op het gehele veld. Denk aan een programmamanager met doorzettingsmacht, die verantwoording aflegt aan de stuurgroep. Hierin is in de governance niet voorzien.
- De sturing is door het grote aantal gremia (stuurgroep Oplossing 2, expertgroep digitale verbetermogelijkheden, programma RDO, etc.) diffuus. Daarmee ontstaat het risico van onvoldoende gerichte sturing.
- Het is noodzakelijk om de besturing in ieder geval op de volgende punten (opnieuw) te doordenken:
 - Landelijke sturing op de ontwikkeling van Oplossing 2 door één verantwoordelijke (de "generaal").
 - Beleggen van de verantwoordelijkheid voor de implementatie van de app (bij de "generaal" of bij de GGD'en zelf).
 - Aansturing van de GGD'en, zodat er één Product Owner namens de GGD'en is, die als nodig ook de implementatie bij de GGD'en verzorgt (zie vorige punt).
 - De voorzitter van de stuurgroep, die boven de verschillende partijen moet staan.

In het verlengde van het voorgaande: zorg ervoor, ook met het oog op de toekomst, dat de rollen en verantwoordelijkheden van opdrachtgever, opdrachtnemer, business owner en product owner helder worden vastgesteld en worden toegewezen aan individuen zodat helder is en wie waarvoor aanspreekbaar is in welke fase.

- *Agile ontwikkeling*

- Het programma moet onder grote tijdsdruk een resultaat opleveren in de vorm van een app.
- Daarom is terecht gekozen voor agile ontwikkeling, dit is de enige manier om op korte termijn werkende resultaten op te kunnen leveren.
- Deze benadering brengt echter als risico met zich mee dat besluitvorming in het licht van de ervaren druk niet gestructureerd en/of ad hoc plaatsvindt.
- Daarnaast is het van belang in korte ontwikkelstappen steeds een vooraf gedefinieerd resultaat op te leveren, want:
 - Bij een agile aanpak is het zeer verleidelijk om tijdens het ontwikkelproces functionaliteiten te herprioriteren of zelfs toe te voegen.
 - Gezien de korte ontwikkeltijd voor het MVP is dat zeer riskant, want hierdoor komt de oplevering van een release, bestaande uit een geheel aan werkende functionaliteiten, verder weg in de tijd te liggen.

- *Monitoring voortgang en uitvoering activiteiten*

- Het plan van aanpak beschrijft in beperkte mate hoe de voortgangsbewaking is ingericht.
- Aandacht hiervoor is essentieel want:
 - Het programma moet onder hoge tijdsdruk resultaat opleveren.
 - Er is een groot aantal actoren betrokken, die ieder een deel van het resultaat verzorgen (er is feitelijk sprake van een keten, de app kan pas in gebruik worden gegeven als alle schakels werken).

- De diverse teams rapporteren over de voortgang en afwijkingen aan het programma RDO van VWS. Dit is verstandig, want zo ontstaat een overkoepelend zicht op de voortgang. Het is hierbij wel van belang dat de voortgang in samenhang wordt gezien, waarbij gewogen wordt wat het effect is van vertraging in één traject op andere trajecten. Door het ontbreken van een overall programmamanager is het ons niet duidelijk of hierin nu wordt voorzien, en zo ja, door wie.
- Het toezien op de samenhang mag daarbij niet beperkt zijn tot tijdsaspecten, ook de inhoudelijke afstemming tussen de verschillende trajecten moet nadrukkelijk in beeld zijn.
- De rapportage aan de stuurgroep dient (bondig) inzicht te geven in inhoud en voortgang en benoemt welke besluiten nodig zijn om tot tijdige en correcte levering van producten te komen.
- Verder moet concreet zijn uitgewerkt hoe de afhandeling van afwijkingen plaatsvindt en wat het escalatiepad is voor "exception reports"
- *Proces versus inhoud*
 - Het plan beschrijft ten aanzien van een aantal aspecten de te nemen acties, zonder daarbij aan te geven welke eisen daarbij aan de orde zijn. Een voorbeeld daarvan is het uitvoeren van een aantal DPIA's.
 - Dit brengt het risico met zich mee dat de aandacht primair is gericht op het uitvoeren van de actie zelf, maar minder of niet op de manier waarop dat gebeurt en het resultaat dat de actie oplevert. Daardoor kunnen op een later moment problemen boven water komen die de ingebruikname van de app in de weg staan.
 - Om bij het voorbeeld van de DPIA te blijven, aan een niet correct uitgevoerde DPIA heb je niets.
 - Het is daarom van belang uitdrukkelijk te (laten) monitoren op de inhoudelijk juiste uitvoering van de voorziene acties.
- *Go/no go besluiten*
 - Het plan benoemt geen go/no go momenten.
 - Daardoor vindt geen expliciete besluitvorming plaatsvindt over (te zetten stappen naar) de ingebruikname van de app of over de in beheer name van de app.
 - Dat brengt het risico van politiek en/of bestuurlijk gemotiveerde besluitvorming met zich mee.
 - Het is noodzakelijk vooraf de go/no go momenten expliciet in kaart te brengen en ook aan te geven op basis van welke criteria besluitvorming plaatsvindt. Drie aandachtspunten daarbij:
 - De meer generieke randvoorwaarden zijn nu al helder (denk aan AVB, BIO, etc.).
 - De criteria zullen soms "tijdens de rit" helder worden, maar zou je dit als standaard werkwijze gebruiken dan ontstaat het risico van 'altijd met de actualiteit meebewegen'.
 - Het programma moet zich hiervan bewust zijn en zonodig expliciet tegengas geven tegen "politieke druk".

- *Toegang tot gegevens*
 - De app slaat persoonsgegevens op, en wel van de hoogste risicocategorie.
 - Dat brengt het risico van schending van de persoonlijke levenssfeer met zich mee. Bij intreden van dit risico zal de bereidheid om de app te gebruiken sterk onder druk komen te staan.
 - Het is daarom van belang de volgende zaken zeer gedetailleerd te definiëren:
 - Welke gegevens legt de app vast, en waarom (uitgangspunt daarbij is proportionaliteit, dus wat is de minimale gegevensset die nodig is om het doel van de gegevensverwerking te bereiken).
 - Wie (arts, burger, GGD-medewerker, medewerker call-center) krijgt waarom toegang tot welke gegevenselementen uit deze gegevensset (wat heeft hij of zij nodig om zijn taak uit te voeren (need to know vs nice to know)).
 - Aan welke eisen de informatiebeveiliging moet voldoen, ten aanzien van infrastructuur, software, processen, etc.
 - Op welke momenten toetsen plaatsvinden om te bezien of deze eisen correct zijn ingevuld.
 - We constateren dat het gegevensmodel nog niet definitief is vastgesteld. Dat maakt het onmogelijk om de hierboven benoemde zaken te beoordelen.
- *Dagelijks beheer van de app*
 - Het ontwikkelen van de app is een incidentele actie, het beheer heeft een structureel karakter
 - Dat beheer is veelzijdig:
 - Monitoren van de beschikbaarheid van de app en signaleren en oplossen van eventuele problemen.
 - Ondersteunen bij het gebruik van de app (help desk).
 - Onderhoud van de vragenlijsten (op regionaal niveau).
 - In productie brengen van nieuwe versies van de app.
 - Communiceren met betrokken partijen (waaronder GGD'en en leveranciers) over deze zaken.
 - Daarbij is van belang dat de app 24/7 beschikbaar is, dat geldt feitelijk ook voor de operationele aspecten rond het beheer.
 - DICTU heeft de uitwerking van het beheer onderhanden. Na afronding daarvan is nog tijd nodig om de beheerorganisatie te ontwerpen en in te richten.
 - Het risico is dat dit vertraging oploopt, waardoor de ingebruikname van de app vertraagt.
 - Wij begrijpen dat dit risico al is ingetreden.
 - Ons beeld is dat inschakelen van andere leveranciers weinig zinvol is, zij hebben bij de start al een achterstand op DICTU, en zullen tegen dezelfde vraagstukken aanlopen die ICTU heeft ervaren.

- *Moment van inzetten van de app*
 - De GGD attendeert burgers bij testen op beschikbaarheid app en adviseert te installeren.
 - Dat is te laat vanuit het perspectief van alarmeren van contacten, de (potentiële) index kan voor het testen al besmettelijk zijn. Je wilt de contacten vanuit die periode ook kennen en alarmeren.
 - De communicatiecampagne zou er daarom op gericht moeten zijn dat zoveel mogelijk mensen de app preventief installeren en gebruiken (door hun contacten te registreren).

- *(Ontwikkeling in het) Volwassenheidsniveau ICT van GGD/GHOR*
 - GGD/GHOR bevindt zich waar het gaat om ICT niet op hetzelfde volwassenheidsniveau als het programma dat de app ontwikkelt.
 - Het beeld is dat het programma de GGD/GHOR op sleeptouw wil nemen om deze zo naar een hoger volwassenheidsniveau te brengen.
 - Wij schatten in dat deze aanpak niet het gewenste resultaat gaat opleveren. Wij verwijzen daarbij naar het fasenmodel van Nolan:
 - de volwassenwording van organisaties rond informatievoorziening verloopt in dit model fasegewijs, waarbij faseovergangen voorafgegaan worden door een crisis. Door deze crisis beseft de organisatie de noodzaak van verandering.
 - Bij GGD/GHOR is er naar onze waarneming (nog) geen sprake is van een dergelijke crisis.
 - Daarbij, en dit raakt aan ons eerste aandachtspunt, ontstaat het risico dat de meeste energie gaat zitten in het proberen te bereiken van een ander doel dan het eigenlijke doel dat je nastreeft (het ontwikkelen van de app). Met het risico dat geen van beide doelen realiseert.

4. Detailanalyse risico's

- Het is niet helder of in de usabilitytesten/testen op gebruiksgemak ook getoetst is op "verkeerd gebruik" van de app (en de gevolgen daarvan).
- De app maakt gebruik van onderliggende technologie van Google en Apple. In hoeverre is getoetst of dit leidt tot (ongewenste) doorgave van gegevens?
- Het plan van aanpak spreekt (op pagina 6) over "overige nauwe contacten", daarbij komen voorbeelden als hoesten en zoenen aan de orde. Het lijkt me dat de app dit niet kan registreren, daarmee is deze categorie niet objectief vast te stellen.
- Het plan gaat uit van het "goed-pad", waarmee we bedoelen dat het uitgangspunt is dat iedere gebruiker precies doet wat we van hem of haar verwachten. Maar, je hebt het gebruik van de app niet onder controle. Dat roept de vraag op wat er gebeurt als de app oneigenlijk wordt gebruikt (zoals in het geval dat de app valse meldingen van besmetting verzendt (geïnitieerd door de gebruiker of als gevolg van een "hack"))).
- Het is niet helder of over het ontwerp afstemming met de AP heeft plaatsgevonden. Het is van groot belang dat de AP het "privacy by design" onderschrijft.
- Het is niet helder hoe bewaking van voortgang en kosten plaatsvindt.
- Het plan maakt niet helder welke oplossing voor identificatie en authenticatie voor de app is voorzien en evenmin of deze het noodzakelijke betrouwbaarheidsniveau heeft.
- Bij het testen van de app is het van belang voldoende "testdekking" te verzekeren. Het is niet duidelijk of en zo ja hoe dat is voorzien.
- Het is niet helder of toetsen op de kwaliteit van de code plaatsvinden en op basis van welke normen dat gebeurt. Bij toetsen op kwaliteit van de broncode zijn in ieder geval onderhoudbaarheid, aanpasbaarheid en beheerbaarheid van belang.
- Het is niet helder hoe goed de bedrijfssystemen van de GGD's zijn beveiligd (niveau applicaties en niveau infrastructuur).
- In de tweede versie gaat de app mogelijk twee soorten functionaliteiten combineren:
 - Verzamelen van gegevens over contacten (ten behoeve van het BCO).
 - Ondersteunen van de gebruiker van de app bij het bepalen van de ernst van klachten (zelfindicatie).

Deze twee functionaliteiten hebben niets met elkaar te maken. Het combineren ervan leidt tot onnodige omvang en complexiteit van de app en compliceert het gebruik van gevoelige persoonsgegevens. Ook impliceert dit dat de app (naast vaststelling besmetting) medische gegevens vasthoudt.
- De app zal in beperkte kring worden gebruikt om eerste ervaringen op te doen. Het is niet helder op welke manier de ervaringen daaruit tot bijstellingen in ontwerp, testen, implementatie, etc. leiden.
- De ontwikkeling van de app vindt "agile" plaats. In het licht van de beperkte doorlooptijd en de wens de app door te kunnen ontwikkelen is het van belang over een ontwerp op hoofdlijnen (dan wel architectuur) te beschikken, die als kader voor de ontwikkeling fungeert en die verzekert dat de bedoelde doorontwikkeling daadwerkelijk kan plaatsvinden. Het is niet helder of een dergelijk ontwerp is opgesteld.
- Een ontwerp zoals bij het vorige punt bedoeld is ook nodig om tot een robuuste oplossing te komen rond generieke zaken als de te registreren gegevens, de beveiligingsmaatregelen, etc.
- De realisatie van functionaliteiten vindt "agile" plaats. Er is een lijst met te realiseren functionaliteiten voor de eerste versie van de app. Deze lijst moet leidend zijn bij de ontwikkeling (die daardoor minder of niet "agile" plaatsvindt).

- In het plan van aanpak is aangegeven dat dit een "levend document" is. Dat staat haaks op de wens in zeer korte tijd tot een concreet resultaat te komen in de vorm van een eerste versie van de app. Dat vergt een heldere koers, die uitgewerkt is in een plan dat de basis vormt voor de uitvoering en dat gedurende die uitvoering niet (meer) verandert.
- Het plan geeft aan dat penetratietesten voorzien zijn. Het is van belang dat die zowel "white box" als "black box" plaatsvinden.
- Het is niet duidelijk of de GGD's ieder over eigen informatiesystemen beschikken, dan wel dat zij gebruik maken van landelijk ontwikkelde en beheerde systemen. Als iedere regio een eigen informatiesysteem heeft leidt dit tot een aanzienlijke verzwarende van het testproces (zowel technisch als inhoudelijk). Daarnaast zijn de DPIA's dan per regio verschillend (waardoor we mogelijk geen gebruik kunnen maken van een raamwerk voor de DPIA).
- Vanuit de app vindt overdracht van gegevens naar de GGD plaats (eerst door inlink in het portaal, daarna door koppelvak met GGD-systemen). Het is van belang dat deze gegevensset toekomstvast is (dat geldt overigens ook voor het gegevensmodel in de app).
- Na oplevering van de tweede versie van de app draagt VWS deze over aan de GGD'en. VWS en GGD'en moeten vooraf heldere afspraken hebben gemaakt wat VWS overdraagt (dus welke code, welke licenties, welke documentatie, etc.) en wat dit betekent voor de verdeling van verantwoordelijkheden, rollen en taken.
- Op welke manier is verzekerd dat het intellectueel eigendom van de app bij VWS berust?
- Het onderwerp aansprakelijkheid is niet benoemd en daardoor niet uitgewerkt.
- Het is niet uit te sluiten dat zich incidenten voordoen. In dit kader zijn twee zaken van belang:
 - Partijen moeten beschikken over een noodplan/calamiteitenplan.
 - Partijen moeten vooraf helder afspreken hoe de woordvoering plaatsvindt.
- Het risico op hack-pogingen is groot. Daarbij kan het gaan om hackers-collectieven, criminelen en statelijke actoren. Het programma voorziet een aantal toetsen op de informatiebeveiliging. Daarbij behoeven twee zaken expliciet aandacht:
 - De inrichting van de infrastructuur waarop de applicaties draaien (inclusief de koppelingen tussen de verschillende delen van de infrastructuur).
 - De werking van de totale keten, van en met de installatie van de app tot en met het gebruik van de gegevens in de systemen van de GGD'en.
- Het programma maakt de broncode van de app openbaar. Dat gaat reacties op drie aspecten opleveren:
 - Functionaliteit
 - Codekwaliteit (en gebruikte libraries)
 - Beveiliging(srisico's)

Als VWS niet ingaat op deze reacties kan dat tot publicitair gedoe leiden. Het is daarom van belang vooraf te duiden welke reacties VWS wil ontvangen (en welke dus niet). Verder moet VWS een proces inrichten om reacties af te handelen (en zo nodig in gesprek te gaan met opstellers van een reactie).
- De inrichting van het testen van de applicatie is in het plan niet beschreven. Aandachtspunten zijn:
 - Geautomatiseerd testen (om te verzekeren dat testen altijd op dezelfde manier en met dezelfde set plaatsvinden).
 - Testdekking (minimaal 80%).
 - Vaste testset (om regressie te testen).
- VWS heeft voorzien de app te beproeven met een kleine groep gebruikers. Welke ervaringen heeft dit opgeleverd en hoe zijn deze ervaringen gebruikt bij de verdere ontwikkeling van de app?

- De terugkoppeling door call-centers levert informatie voor de verdere ontwikkeling van de app. Er moet een proces ingericht zijn voor het ophalen van deze terugkoppeling en de afhandeling ervan.
- Het gewenste betrouwbaarheidsniveau voor identificatie en authenticatie voor gebruik van de app moet zijn vastgesteld (zie Handreiking Betrouwbaarheidsniveau's van het Forum Standaardisatie). Het is niet helder of dit is gebeurd. Het betrouwbaarheidsniveau bepaalt de middelen waarmee gebruikers toegang tot de app kunnen krijgen.
- Hetzelfde geldt voor het betrouwbaarheidsniveau voor de toegang tot het webportaal en de toegang die medewerkers van de GGD'en tot dat portaal krijgen.
- In de programmaorganisatie is een expert community voorzien. Het is van belang heldere afspraken te maken over de rol/opdracht van deze community, de manier waarop zij inbreng in het ontwikkelproces leveren en de manier waarop het programma deze inbreng afhandelt.
- Het ontwerp voor de "sluis" is gebaseerd op "privacy by design". Het is niet helder of er een vergelijkbaar ontwerp voor de app (op de telefoon) is gemaakt. Dat zou wel het geval moeten zijn.
- Uit de documentatie blijkt niet duidelijk hoe de monitoring van het gebruik van de app en het portaal plaatsvindt. Dit is van belang om zicht te krijgen op
 - Technische en performanceproblemen.
 - De mate van gebruik van de app.
 - De resultaten van het gebruik van de app.
- Het is niet duidelijk wanneer de analyse van DICTU over het beheer afgerond is. Die moet snel beschikbaar komen, om de GGD'en in staat te stellen het beheer correct en tijdig in te richten.
- Het is niet duidelijk wie verantwoordelijk is voor de beschrijving en inrichting van de werkprocessen binnen de GGD'en.
- De kennisdragers van de app (degenen die echt weten hoe hij in elkaar zit en werkt) moeten bij de overdracht van de app en het portaal naar de GGD mee overgaan om zo te verzekeren dat kennisoverdracht naar de reguliere beheerders kan plaatsvinden.
- De gebruiker van de app kan gegevens wijzigen en verwijderen. Dat roept de vraag op om welke gegevens het gaat en in hoeverre het wijzigen en verwijderen van gegevens de correcte werking van de app in de weg staat.
- De risicoparagraaf in het plan van aanpak is niet goed uitgewerkt en lijkt niet compleet. De mitigerende maatregelen zijn niet concreet beschreven.
- Oplossingen 1 en 2 vormen samen een (eerste versie van een) applicatielandschap, dat de GGD'en in beheer gaan nemen. Daarvoor is inzicht nodig in de samenhang tussen beide oplossingen.