



Voortgangsrapport Covid Informatie en Monitoring Systeem (CIMS) CP en ZVP (DVP_145)

Periode	21-10-2020 t/m 16-11-2020
Projectnummer	V/220038/01/AR
Project	Covid Informatie en Monitoring Systeem (CIMS) (CIMS Zorgverlenersportaal, CIMS Cliëntenportaal)
Projectleider	[REDACTED]
ProjectStatus	CIMS ZVP: start bouw skeleton; CIMS CP: start bouw skeleton.

Oplegnotities bij de agenda van de Stuurgroep d.d. 17 november 2020

- Communicatie naar burgers - wie neemt dat op zich en hoe gaat dit in zijn werking?
- Communicatie naar zorgverleners- wie neemt dat op zich en hoe gaat dit in zijn werking?
- Ondersteuner [REDACTED] – status?
- RIVM toegang is nog geen team maar zij moeten eerder live dan wij- uitzetten in de markt duurt nu nog paar weken en dan moeten ze nog starten...
- Afstemming API's moet starten –
- In nieuws item NOS vrijdag 13-11 gesproken over tekort professionals voor vaccinatie en dat er studenten etc ingezet moeten gaan worden. Wat betekent dat voor scope/ toegang tot portaal?

Voortgang

CIMS ZVP

Gedaan:

- Concept PID opgeleverd status 0.1
- Status 0.3 opgeleverd PSA
- Uitvragen inhoudelijk verantwoordelijke (producteigenaar)
- Start ontwikkelaar
- Selectie architect
- Koppelingen naar CIMS Functioneel verder besproken
- Start sprint 1 16-11
- Team bij elkaar muv architect

Te doen:

- Scoping [] tov PSA helder krijgen
- Budget PID afronden
- Starten architect
- Finaliseren PSA
- Zekerheid in Inzien en Opvragen (en de gevolgen daarvan voor het project) van gegevens of toch alleen Inzien

CIMS CP

Gedaan:

- Concept PID opgeleverd status 0.1
- Status 0.99 opgeleverd PSA
- Selectie architect
- Koppelingen naar CIMS Functioneel verder besproken
- Team bij elkaar muv architect
- Start sprint 1 16-11
- Start ontwikkelaar

Te doen:

- Budget PID afronden.
- (Ondersteunend) Producteigenaar toegewezen krijgen.
- Starten architect

Aandachtspunten:

- Verschil ik scope VZP [] en []. Meeting voor belegd, wel zorgelijk.

Aandachtspunten/Afwijkingen	Voorstel Acties
CIMS ZVP	
<ul style="list-style-type: none"> • Verschil ik scope VZP [] en [] 	Meeting voor belegd, wel zorgelijk.

CIMS CP	
te weinig tijd	Ondersteuner uitgevraagd intern. Status?



Voortgangsrapport Covid Informatie en Monitoring Systeem (CIMS) CP en ZVP (DVP_145)

Periode	16-11-2020 t/m 1-12-2020
Projectnummer	V/220038/01/AR
Project	Covid Informatie en Monitoring Systeem (CIMS) (CIMS Zorgverlenersportaal, CIMS Cliëntenportaal)
Projectleider	[REDACTED]
ProjectStatus	CIMS ZVP: realisatie bouw skeleton en API's; CIMS CP: realisatie bouw skeleton en API's

Oplegnotities bij de agenda van de Stuurgroep d.d. 1 december 2020

- N.a.v. meeting communicatie zorg rond communicatie naar zorgverleners neergelegd bij [REDACTED]?
- Opdracht(gever) nodig voor start realisatie toegang tot portalen in rivm.nl. mijn.rivm.nl (voorlopig) van de baan
- Ondersteuning vanuit Open Shift nodig die niet wordt verkregen – we lopen vertraging op
- Voor 'extreem goed documenteren' hebben wij graag een voorbeeld van hoe dit er dan uitziet
- Voor rol documenteren waarschijnlijk architect opschalen om documentatie te gaan verzorgen -> hoger budget
- Inschatting budget voor beheer nog niet klaar
- N.a.v. overleg met [REDACTED] hoofd communicatie, komt er een UX-er bij om de reis richting en binnen de portalen zo goed mogelijk te maken -> hoger budget

Voortgang

CIMS ZVP

Gedaan:

- Concept PID opgeleverd status 0.2
- Status 0.3 opgeleverd PSA
- Koppelingen naar CIMS Functioneel verder besproken
- 1^{ste} sprint afgerond
- Architect ingewerkt
- Ping naar CIMS is succesvol uitgevoerd
- Budget opgeleverd
- Afstemming API's gestart
- Afstemming RIVMToegang gestart

Te doen:

- Goed documenteren starten
- Finaliseren PSA

CIMS CP

Gedaan:

- Concept PID opgeleverd status 0.2
- Status 0.99 opgeleverd PSA
- Architect is gestart
- Ping naar CIMS is succesvol uitgevoerd
- Team bij elkaar muv architect
- 1^{ste} sprint afgerond
- Architect ingewerkt
- Budget opgeleverd
- Afstemming API's gestart
- Afstemming RIVMToegang gestart

Te doen:

- Budget PID afronden
- Goed documenteren starten

Beheer

- Afstemming beschikbaarheid etc. heeft plaatsgevonden
- PBS is opgesteld

Te doen:

- Vragen beheer verder uitwerken en aan [REDACTED] sturen
- PBS voorleggen aan andere PM's CISM
- Budget beheer scherp krijgen

Aandachtspunten/Afwijkingen

Voorstel Acties

CIMS ZVP	
<ul style="list-style-type: none">Vershil in scope VZP [redacted] en [redacted]	[redacted] gevraagd n.a.v. meeting met [redacted] af te stemmen
CIMS CP	



Voortgangsrapport Covid Informatie en Monitoring Systeem (CIMS) CP en ZVP (DVP_XX)

Periode	1-12-2020 t/m 15-12-2020
Projectnummer	V/220038/01/AR
Project	Covid Informatie en Monitoring Systeem (CIMS) (CIMS Zorgverlenersportaal, CIMS Cliëntenportaal)
Projectleider	
ProjectStatus	CIMS ZVP: realisatie bouw skeleton en afronding; CIMS CP: realisatie bouw skeleton en API's

Oplegnotities bij de agenda van de Stuurgroep d.d. 17 december 2020

- Officiële Communicatie richting IV over deprioriteren ZVP
- Opdrachtgever voor mijn.rivm.nl
- Opdracht(gever) nodig voor start realisatie toegang tot portalen in rivm.nl. mijn.rivm.nl (voorlopig) van de baan
- Akkoord op PID Adrie nodig, versie 0.9 gister aangeleverd
- Plek voor een architect in een van de CIMS projecten voor 24 uur?
- Graag helderheid wat DVP (centraal) regelt qua beheer en wat er bij de projecten hoort
- Ter informatie: er moet nog een aparte assesment worden gepland voor de check op DigiD. Er werd gedacht dat dit bij de pentesten erbij in zat maar dat blijkt niet het geval. Ook een gebruikers test wordt afgenomen door een extern bureau in februari, pentesten, een code review en accesibility testen. Dit is meer dan voorzien dus planning komt onder druk te staan voor CP aangezien uit deze vijf testen werk komt wat pas helder wordt na uitvoering hiervan.
- PBS is opgeleverd en andere pm's hebben hun PBS toegevoegd. Wat gebeurt hier nu mee?
- Vooruitkijkend: moeten we al werk gaan verrichten/uitzetten om na Fase 1 CP Fase 2 direct op te starten?

Voortgang

CIMS ZVP

Gedaan:

- Demo gehouden
- Skeleton verder afgebouwd
- Acties bepaald om werk af te ronden
- Allocatie ontwikkelaar naar CP na afronden skeleton
- PID afgerond en voor de 2e keer rondgestuurd- geen feedback op ontvangen 2e ronde

Te doen:

- Her-allocatie architect wellicht voor andere CIMS projecten
- Akkoord opdrachtgever [REDACTED] op PID ontvangen
- Werkzaamheden afronden
- Documentatie van kwaliteit opleveren zodat dit na de zomer weer kan worden opgepakt
- Finale versie ZVP ontvangen

CIMS CP

Gedaan:

- Demo gehouden
- Skeleton verder afgebouwd
- Sessie pentesten, code reviews gehouden.

Te doen:

- Assesment onderzoeken voor koppelen met DigiD – dit is nieuwe informatie want dit zou eigenlijk in de pentesten zitten maar dat bleek niet het geval
- Akkoord opdrachtgever [REDACTED] op PID ontvangen
- Finaliseren wireframes
- Start bouwen schermen
- Aanleveren definitieve content door PO

Beheer

Gedaan:

- Functionele vragen vanuit beheer beantwoord en gedeeld met [REDACTED] voor toevoeging aan geheel. [REDACTED] zet dit door naar [REDACTED]
- PBS gedeeld met CIMS team
- In Topdesk proces in gang gezet om na live gang calls te kunnen typen voor de portalen

Te doen:

- Vragen beheer verder uitwerken en aan [REDACTED] sturen
- PBS voorleggen aan andere PM's CISM
- Budget beheer scherp krijgen
- Meeting met [REDACTED] voor het Infopunt icm [REDACTED] van Communicatie houden voor vervolgstappen

Periode	08-10-2020 t/m 21-10-2020
Projectnummer	V/V22003001/AR
Project	Covid Informatie en Monitoring Systeem (CIMS) (Zorgverlenersportaal -ZVP, Cliëntenportaal-CPI)
Projectleider	
ProjectStatus	CIMS ZVP: idee; CIMS CP: initiatie.

Oplegnotities bij de agenda van de Stuurgroep d.d. 26 oktober 2020

Geen.

Voortgang**CIMS ZVP****Gedaan:**

- Meerdere overleggen over scoping.
- Start gemaakt met PSA.
- Uitvragen inhoudelijk verantwoordelijke (producteigenaar)
- Uitvraag ontwikkelaar.
- Afbakening projectscope t.o.v. CIMS Functioneel/Infra aangaande koppelingen.

Te doen:

- Scoping helder krijgen.
- Verder uitwerken PID (waaronder WBS en planning).
- Verder uitwerken PSA.
- (Ondersteunend) Producteigenaar toegewezen krijgen.
- Afronden selectie sollicitanten ontwikkelaar.
- Uitnodigen sollicitanten ontwikkelaar.
- Zekerheid in Inzien en Opvragen (en de gevolgen daarvan voor het project) van gegevens of toch alleen Inzien

CIMS CP**Gedaan:**

- Rollen helder krijgen van Communicatie, DVP, Campus.
- Resources uitgevraagd bij Richard van Vliet voor UX/Front-end designer, technisch beheerder en tester.
- Resource voor Functioneel beheer of Functioneel Ontwerp uitgevraagd bij Georget.
- Start vastleggen User Stories (scope) in projecttool Jira met Initiatiefase team.
- Uitvraag ontwikkelaar.

Te doen:

- Afronden selectie sollicitanten ontwikkelaar.
- Uitnodigen sollicitanten ontwikkelaar
- Selectie te ontvangen CV's architecten.
- Uitnodigen sollicitanten architect
- Verder uitwerken PID (waaronder WBS en planning)
- Finaliseren PSA
- (ondersteunend) Producteigenaar toegewezen krijgen
- In kaart brengen activiteiten t.o.v. Security i.c.m. [REDACTED]


Aandachtspunten:

- Te weinig capaciteit domeinarchitect [REDACTED] voor ZVP en CP .
- Ontbreken PO voor CP en ZVP en dus ook eigenaarschap en helderheid scope.

Aandachtspunten/Afwijkingen	Voorstel Acties
CIMS ZVP en CP	
Te weinig capaciteit domeinarchitect [REDACTED] voor ZVP en CP.	Snel inzetten Informatie Architect.
Ontbreken PO voor CP en ZVP en dus ook eigenaarschap en helderheid scope.	Aanstellen PO's met mandaat en mensen samenstellen die over scoping ZVP gaan om scope af te bakenen.

Urenbesteding DVP (uren)				
Omschrijving	Begroot	Realisatie	Forecast	Verschil
Algemene projecturen	xxx	xxx	xxx	xxx
Opmerkingen				
Uren volgen				

Urenbesteding Campus (uren)				
Omschrijving	Begroot	Realisatie	Forecast	Verschil
Algemene projecturen	Xxx	xxx	xxx	xxx
Opmerkingen				
Uren volgen .				

Periode	06-1-2021 t/m 21-1-2021
Projectnummer	V/190007/01/CI
Project	Covid Informatie en Monitoring Systeem (CIMS) (CIMS Cliëntenportaal)
Projectleider	
ProjectStatus	CIMS CP: realisatie bouw schermen

Oplegnotities bij de agenda van de Stuurgroep d.d. 25 januari 2021

- Geen oplegnotities

CIMS CP

Gedaan:

- Demo 2 gehouden
- 80% van de schermen gebouwd
- Verder gebouwd aan API's
- ACC omgeving opgeleverd
- Uitvraag Accessibility test gedaan
- Afstemming rondom code review en pentesten gedaan
- Gebruikers testen door extern bureau gestart
- Definitieve teksten aangeleverd gekregen door communicatie

Te doen:

- Performance test voorbereiden
- Performance test-ketentest op de ACC omgevingen houden
- Go Live plan opstellen
- Dry Run plannen op PROD

Beheer

Gedaan:

- 2 wekelijkse afstemmingssessies voor beheer gestart olv [REDACTED]

Te doen:

- Kosten aangeleverd krijgen door [REDACTED]
- Hoe gaat team verder na Fase 1 uit laten zoeken/bepalen door [REDACTED]

Periode	21-1-2021 t/m 3-1-2021
Projectnummer	V/190007/01/CI
Project	Covid Informatie en Monitoring Systeem (CIMS) (CIMS Cliëntenportaal)
Projectleider	[REDACTED]
ProjectStatus	CIMS CP: realisatie

Oplegnotities bij de agenda van de Stuurgroep d.d. 8 februari 2021

- Meer ondersteuning nodig door beheerders en ontwikkelaars vanuit RIVM. Inzet ontwikkelaars ondersteuning wordt volgende week besproken, nu geschat op 10 uur per week tot live gang. Inzet 2 AFM beheerders die elkaar gaan afwisselen, volgende week meer helderheid rond extra inzet, nu geschat op 16 uur per week extra tot live gang.
- Over 7 weken gaan we live, moet ik het team aanhouden voor de volgende fases of contracten niet meer verlengen?
- Koppeling met RVP moet als change worden aangevraagd, voor Fase 2 moet deze aanvraag dan starten omdat dit wel 5 maanden kan duren (begreep ik van [REDACTED])

CIMS CP

Gedaan:

- Demo 3 – CIMS keten- gehouden
- Alle schermen gerealiseerd
- Concept go live plan opgesteld
- Uitvraag Accessibility test is gegund
- Code review en pentesten worden voorbereid
- Gebruikers testen door extern bureau afgerond- uitkomst vooral op tekst, minimale aanpassingen op look&feel
- Performance testen gestart

Te doen:

- Performance test afronden
- OTAP opleveren
- Go Live plan opstellen afstemmen met CIMS keten
- DPIA uitvoeren
- BIO quickscan uitvoeren
- Risico analyse uitvoeren
- Pentesten uitvoeren
- Code review uitvoeren
- Accessibility testen uitvoeren

Beheer

Gedaan:

- 2 wekelijkse afstemmingssessies voor beheer gestart olv [REDACTED]

Te doen:

- Kosten aangeleverd krijgen door [REDACTED] voor beheer
- Hoe gaat team verder na Fase 1 uit laten zoeken/bepalen door [REDACTED]

Periode	3-2-2021t/m 17-2-2021
Projectnummer	V/190007/01/CI
Project	Covid Informatie en Monitoring Systeem (CIMS) (CIMS Cliëntenportaal)
Projectleider	
ProjectStatus	CIMS CP: realisatie

Oplegnotities bij de agenda van de Stuurgroep d.d. 22 februari 2021

- Wat is status Change koppeling met RVP?
- Logius wil inzicht in campagne van VWS aangaande CP, is die er en is dit mogelijk?

CIMS CP

Gedaan:

- DPIA gestart
- Performance testen gestart
- BIO quickscan gestart
- Go live plan opgesteld
- AVG quickscan uitgevoerd
- Verkenning vaccinatie
- Code review en pentesten gestart
- Uitkomsten gebruikerstesten door [REDACTED] opgepakt
- Performance testen gestart

Te doen:

- Performance test afronden
- Productie omgeving opleveren
- Go Live plan afstemmen met CIMS keten
- DPIA afronden
- BIO quickscan afronden
- Risico analyse uitvoeren
- Pentesten bevindingen oppakken
- Code review bevindingen oppakken
- Privacy verklaring opstellen
- Disclaimer oppakken vraag [REDACTED] over juistheid data
- Accessibility testen uitvoeren
- Dry run houden


Beheer

Gedaan:

- wekelijkse afstemmingssessies voor beheer gestart olv [REDACTED]

Te doen:

- Kosten aangeleverd krijgen door [REDACTED] voor beheer
- Rollen matrix finaliseren
- Checklijst afmaken voor beheer

Periode	17-2-2021 t/m 4-3-2021
Projectnummer	V/190007/01/CI
Project	Covid Informatie en Monitoring Systeem (CIMS) (CIMS Cliëntenportaal)
Projectleider	
ProjectStatus	CIMS CP: finalisatie

Oplegnotities bij de agenda van de Stuurgroep d.d. 8 maart 2021

- Na de freeze van 5 maart (plus weekend) zullen er in ieder geval 3 geplande werkzaamheden worden uitgevoerd, graag akkoord dat dit ok is om op te pakken:
- Bevindingen Accessibility test die 8 maart plaatsvindt
- *Uitkomst hertest pentest*
- *Uitkomst 2^e pentest indien voor live*
- *Input vanuit stuurgroep 4-3 op tekst*
- *Daarnaast zal er een veeglijst zijn waarvan gezegd moet worden of dit wel of niet mee gaat*
- Is er groen licht om met de huidige performance live te gaan?

CIMS CP

Gedaan:

- DPIA gestart
- Performance testen doorlopend gehouden
- BIO quickscan afgerond
- Go live plan opgesteld
- AVG quickscan uitgevoerd
- Code review en pentesten Sogeti afgerond
- Issue rondom performance testen escaleren en volgen Taskforce
- Go Live plan afstemmen met CIMS keten vindt meerdere keren per week plaats

Te doen:

- Hertest pentest uitvoeren 8 maart
- Accessibility testen uitvoeren 8 maart
- Intake 2e onafhankelijke pentest
- Performance test afronden
- Manier bepalen performance test op PROD
- Uitvoeren performance test op PROD
- Productie omgeving opleveren
- DPIA afronden
- Risico analyse afronden
- Pentesten bevindingen afronden
- Code review bevindingen afronden
- Dry run houden
- Input voor DigiD assesment leveren scan website
- Sprint afronden voor Freeze

Beheer

Gedaan:

- wekelijkse afstemmingssessies voor beheer gestart olv [REDACTED]
- Rollen matrix gefinaliseerd

Te doen:

- Kosten aangeleverd krijgen door [REDACTED] voor beheer
- Checklijst nalopen na voor beheer
- Scan voor beheer door security

Gegevensbeschermings- effectbeoordeling (DPIA) Inzage vaccinaties DVP Cliëntenportaal

VWS/RIVM/DVP/Inzage vaccinaties Cliëntenportaal

Directie Bedrijfsvoering

Bilthoven, 22-03-2021

Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum

Naam: Typ naam/functie

Advies functionaris voor gegevensbescherming: Selecteer/typ datum

Naam: Typ naam/functie

Advies CIO: Selecteer/typ datum

Naam: Typ naam/functie

Gegevensbeschermings- effectbeoordeling (DPIA)

**VWS/RIVM/DVP/Inzage vaccinaties Cliëntenportaal
Directie Bedrijfsvoering**

Contact:

Ministerie van VWS, directie RIVM
Bedrijfsvoering
DVP

Versie: 0.9

Inhoudsopgave

Inleiding	5
A. Beschrijving kenmerken gegevensverwerkingen	7
1. Voorstel <input type="checkbox"/>	7
2. Persoonsgegevens <input type="checkbox"/>	8
3. Gegevensverwerkingen <input type="checkbox"/>	11
4. Verwerkingsdoeleinden <input type="checkbox"/>	15
5. Betrokken partijen <input type="checkbox"/>	17
6. Belangen bij de gegevensverwerking <input type="checkbox"/>	19
7. Verwerkingslocaties <input type="checkbox"/>	20
8. Techniek en methode van gegevensverwerking <input type="checkbox"/>	21
9. Juridisch en beleidsmatig kader <input type="checkbox"/>	24
10. Bewaartermijnen <input type="checkbox"/>	25
B. Beoordeling rechtmatigheid gegevensverwerkingen.....	26
11. Rechtsgrond <input type="checkbox"/>	26
12. Bijzondere persoonsgegevens <input type="checkbox"/>	28
13. Doelbinding <input type="checkbox"/>	30
14. Noodzaak en evenredigheid <input type="checkbox"/>	32
15. Rechten van de betrokkene <input type="checkbox"/>	34
C. Beschrijving en beoordeling risico's voor de betrokkenen	35
16. Risico's <input type="checkbox"/>	35
D. Beschrijving voorgenomen maatregelen	39
17. Maatregelen <input type="checkbox"/>	39

Inleiding

1. Nederland wordt, net als de rest van de wereld, geconfronteerd met de uitbraak van het COVID-19 virus. COVID-19 kan ernstige klachten veroorzaken met als gevolg een acute ziekenhuisopname, een chronisch ziektebeeld, en in het ergste geval, de dood. Momenteel wordt – onder verantwoordelijkheid van de Minister van Volksgezondheid, Welzijn en Sport (hierna: VWS) – een vaccinatieprogramma tegen COVID-19 vastgesteld¹. Veilige en effectieve vaccins tegen COVID-19 is een essentiële stap in de bestrijding van het coronavirus
2. Het coördineren van de uitvoering, alsmede registratie, bewaking en evaluatie van het vaccin vormt een belangrijk onderdeel van de taak van de Minister van VWS. Deze taak is belegd bij het Rijksinstituut voor Volksgezondheid en Milieu (hierna: RIVM). Ter ondersteuning van deze taak is het COVID-vaccinatie Informatie- en Monitoringsysteem (hierna: CIMS) ontwikkeld en in gebruik genomen². Daarnaast is het Cliëntenportaal ontwikkeld t.b.v. het inzage van medische gegevens te faciliteren aan de burger. Daarbij wordt een eigen aansluiting op DigiD voor authenticatie voorzien.
3. Dit document bevat de gegevensbeschermingseffectbeoordeling (GEB, in het Engels: Data Protection Impact Assessment, hierna: DPIA) van de voorgenomen verwerkingen van persoonsgegevens³ binnen het Cliëntportaal, conform artikel 35 van de Algemene Verordening Gegevensbescherming (hierna: AVG).
4. Bij het opstellen van deze GEB wordt als uitgangspunt genomen dat het vaccinatieprogramma tegen COVID-19 (nog) wordt aangewezen als vaccinatieprogramma als bedoeld in artikel 6b, eerste lid, Wet publieke gezondheid (hierna: Wpg) jo. artikel 11, tweede lid, Besluit publieke gezondheid⁴
5. Een van de strategische uitgangspunten van het RIVM is het centraal stellen van de gebruiker en het streven naar vernieuwing. Gebruikers zijn in dit geval ook burgers die op basis van aangepaste wet- en regelgeving meer regie moeten gaan krijgen over eigen (gezondheids-)gegevens. In het kort vormen de volgende drivers de aanleiding voor de inrichting van een cliëntportaal:
 - a) Aansluiten op de uitgangspunten van de Nederlandse digitaliseringsstrategie;
 - b) Invulling geven aan het Rijksprogramma NL DIGIbeter 2019⁵ als uitwerking van de digitaliseringsstrategie. Een van de pijlers van dit programma vormt regie op eigen gegevens (zie ook de kamerbrief Regie op persoonlijke gegevens bij de overheid, 32761 nr. 147);

¹ Zie de *Kamerstukken II 2020/21*, 25 295, nr. 565 en *Kamerstukken II 2020/21*, 25 295, nr. 745.

² *Kamerstukken II 2020/21*, 25 295, nr. 745, par. 6.

³ Uitgangspunt van deze DPIA zijn de voorgenomen gegevensverwerkingen zoals bekend op 14 december 2020.

⁴ Opneming van het vaccinatieprogramma tegen COVID-19 in art. 11, tweede lid, Besluit publieke gezondheid impliceert met zoveel woorden een centrale aanpak en dus ook een centrale registratie. Dit blijkt uit de nota van toelichting bij de besluiten waarmee andere heel Nederland betreffende infectieziekten werden toegevoegd aan de lijst van infectieziekten in art. 11, tweede lid, Besluit; zie resp. NvT bij Besluit van 20 november 2017, houdende aanpassing van het Besluit publieke gezondheid vanwege het vaccinatieprogramma en het bevolkingsonderzoek, alsmede het aanwijzen van vectoren, *Stb.* 2017, 457 en *Kamerstukken II 2015/16*, 34 472 nr. 3, p. 3, 5, p. 8-9

⁵ Agenda Digitale Overheid (bijlage bij Kamerstuk 34 700, nr.34 en Kamerstuk 26 643, nr. 621)

- c) Binnen de zorg is VWS een samenwerking aangegaan met het zorgveld wat heeft geleid tot het Informatieberaad. Een van de vier hoofdthema's van het Informatieberaad is Patiënt Centraal. Hierbij is afgesproken dat vanaf 2018, alle patiënten de mogelijkheid krijgen om hun belangrijkste medische gegevens digitaal in te zien, veilig, op eigen initiatief, zelfstandig, vanuit een willekeurige locatie⁶.
- d) Met AVG is wettelijk verplicht gesteld dat cliënten inzage krijgen in alle geregistreerde gegevens. De AVG is per 25 mei 2018 van toepassing.
- e) De wet algemene bepalingen verwerken persoonsgegevens in de zorg verplicht tot het geven van inzage c.q. het verkrijgen van een elektronisch afschrift van het eigen medisch dossier⁷.

Gebruikte afkortingen

AVG	Algemene verordening gegevensbescherming
Besluit	Besluit publieke gezondheid
BSN	Burgerservicenummer
BRP	Basisregistratie Personen
CIMS	COVID-vaccinatie Informatie- en Monitoringsysteem
COA	Centraal orgaan asielzoekers
DPIA	Data protection impact assessment
GEB	gegevensbeschermingseffectbeoordeling
GGD	Gemeentelijke gezondheidsdienst
UAVG	Uitvoeringswet AVG
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
VWS	Volksgesondheid, Welzijn en Sport
Wabb	Wet algemene bepalingen burgerservicenummer
Wpg	Wet publieke gezondheid

Leeswijzer

In afwijking van de gangbare gegevenseffectbeoordeling gehanteerde volgorde, worden bij de beschrijving van de kenmerken van de verwerking ook de techniek en methode van gegevensverwerking en (informatiebeveiligings-)maatregelen beschreven en vertaald naar de gevolgen voor betrokkenen.

Het vaccinatiebewijs/vaccinatiepasport ziet niet in de scope van deze DPIA.

De onderstaande (nog levende) documenten zijn gebruikt als onderbouwing van deze gegevenseffectbeoordeling:

1. Systeemdecompositie Cliëntenportaal
2. Quickscan BIO Clientportaal
3. Project Start Architectuur (PSA)
4. High Level Design Cliëntenportaal
5. RIVM Riscoanalyse API Gateway Clientportaal RIVM Toegang

⁶ <https://www.informatieberaadzorg.nl/over-het-informatieberaad/outcomedoelen-en-targets/patient-centraal>

⁷ Artikel 15d Wabvpz

Betrokken bij het DPIA proces:

Aanvrager/opdrachtgever [vaststelling dPIA]: Hoofd. Dienst Vaccinvoorziening en Preventieprogramma's, RIVM DVP

Organisatieonderdelen RIVM betrokken bij de coördinatie en uitvoering van de Registratie Vaccinatie COVID-19

- *Informatiemanager Dienst Vaccinvoorziening en Preventieprogramma's, RIVM DVP*
- *Privacy Coördinator Dienst Vaccinvoorziening en Preventieprogramma's, RIVM DVP*
- *Projectarchitecten CIO-office*
- *Adviseur Informatiebeveiliging CIO-Office*
- *Projectarchitect IV-organisatie Architecten SSC Campus*
- *Projectmanagement CliëntenPortaal*

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel



Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

Klik hier om infotekst te verbergen

Om een PIA te kunnen verrichten moet duidelijk zijn op welk onderwerp/object deze betrekking heeft. Met een korte en bondige beschrijving van het voorstel waar de PIA op ziet, wordt tevens voorkomen dat bij het nalopen van de 17 punten hier verschillend over wordt gedacht. Ten behoeve van de duidelijkheid kan het nuttig zijn om expliciet aan te geven waar de PIA niet over gaat. Bij conceptregelgeving kan voor deze beschrijving van het voorstel aansluiting worden gezocht bij het voorlopige ontwerp van de inleidende paragraaf van de memorie of nota van toelichting bij het voorstel, voor zover deze betrekking heeft op verwerkingen van persoonsgegevens. Bij overheidsverwerkingen kan in hoofdlijnen worden beschreven hoe de gegevensverwerkingen er uit zullen zien. Als dat er is kan worden aangesloten bij het projectvoorstel of een beschrijving van de architectuur.

Deze DPIA betreft de verwerking van persoonsgegevens in een online cliëntenportaal. Door middel van het cliëntenportaal wordt de inzage in de vaccinatiegegevens gefaciliteerd. Dit geldt voor zowel voor het Covid-19 vaccinatieprogramma (fase 1) als het Rijksvaccinatieprogramma (fase 2). Prioriteit ligt nu bij het ontsluiten van Covid-19 vaccinatiegegevens voor de betrokkenen uit CIMS, maar op termijn komt ook een koppeling met het Rijksvaccinatieprogramma. Dan kan de burger al zijn vaccinatiegegevens via het cliëntportaal inzien. Het cliëntenportaal faciliteert t.b.v. de individuele burger de toegang tot

zijn/haar eigen medische gegevens waarvoor hij/zij gemachtigd is om deze in te zien. Tevens kan men hier verzoeken voor hun AVG rechten kwijt en wordt relevante privacy gerelateerde informatie getoond om te voldoen aan het recht op informatie.

Het cliëntenportaal zal verschillende functies aanbieden, namelijk: het inloggen, ophalen van vaccingegevens of het ophalen van uitwisselingen hierbij valt te denken aan het kunnen inzien van de logging wie wanneer vaccinatiegegevens van de burger heeft ingezien. Daarnaast bestaat er de mogelijkheid voor het afmelden van registratie en een aanvraag doen om gegevens te verwijderen uit de CIMS database. Ophalen in de scope van deze DPIA betekent niet fysiek downloaden maar inkijken via een viewing functie binnen het cliëntenportaal. Via de viewing functie krijgt men zicht op een beperkt deel van de database en deze staat in een aparte omgeving. De toegang tot deze view is gerealiseerd door middel van een interne Application Program Interface (API). **Zie voor nadere toelichting de bijgevoegde Powerpoint (UitlegCliëntenportaal versie 23-03-2021)**

Er is een fasering nodig per functie. Bij realisatie van de initiële invulling op 8 april 2021 wordt de inzage van de vaccinatiegegevens aangeboden. Verder worden de volgende functionaliteiten geleverd:

1. De mogelijkheid om berichten achter te laten;
2. Inzage te verkrijgen wie het vaccinatieregister van betrokkene heeft (bijv. het aantal logfiles of intekenlijst);
3. Het kunnen indienen van een aanvraag om de geregistreerde gegevens uit de CIMS- database te laten verwijderen;

De uitkomst van aanvragen voor inzage van vaccinatiegegevens of het aanvragen om vaccinatiegegevens te verwijderen en te corrigeren worden via het cliëntenportaal volgens de alreeds bestaande procedures door een DVP-regiomedewerker opgepakt. Het is hierdoor dus niet mogelijk voor de burger om zelfstandig zijn / haar data te wijzigen of te verwijderen. Het resultaat wordt aan de burger teruggekoppeld binnen de vastgestelde termijnen zoals vermeld in de AVG artikel 12 lid 3.

De mogelijkheid voor genoemde verzoeken blijft via andere kanalen bestaan. Een verzoek via mail / telefoon of per post wordt daarom ook in behandeling genomen.

2. Persoonsgegevens



Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

[Klik hier om infotekst te verbergen](#)

Beschrijf allereerst alle te verwerken categorieën van persoonsgegevens. Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Natuurlijke personen wil zeggen mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in beginsel geen persoonsgegeven. Deze informatie kwalificeert weer wel als persoonsgegeven indien die ook betrekking heeft op een levende persoon.

Om te bepalen of iemand identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de persoon te identificeren.

Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd. Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis verbonden dat deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.

Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie het gegeven betrekking heeft, niet (meer) identificeerbaar is. Het anonimiseren van persoonsgegevens als zodanig is overigens weer *wel* een verwerking van persoonsgegevens.

Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK- nummer, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag. Ook metadata – informatie over informatie – zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt en de geschreven taal. Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

Typen

Stel vervolgens de aard van de te verwerken categorieën van persoonsgegeven vast. De AVG onderscheidt drie typen van persoonsgegevens – gewone, bijzondere en strafrechtelijke persoonsgegevens – en stelt verschillende eisen aan een rechtmatige verwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

Bijzondere persoonsgegevens

Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens over seksueel gedrag of seksuele gerichtheid.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relatiestatus op sociale media. Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid.

Genetische gegevens

Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon. Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

Biometrische gegevens

Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd. Denk hierbij aan: vingerafdrukken, irisspatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme. Foto's vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken.

Gegevens over gezondheid

Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven. Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

Wettelijke identificatienummers

Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een burgerservicenummer (BSN), BIGnummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtkenummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

Overige persoonsgegevens

Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

- * gegevens over de financiële of economische situatie van de betrokkene;
- * gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties;
- * (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- * gegevens die betrekking hebben op kwetsbare groepen;
- * gebruikersnamen, wachtwoorden en andere inloggegevens;
- * gegevens die kunnen worden misbruikt voor (identiteits)fraude;
- * communicatie- en locatiegegevens.

Betrokkenen

Benoem tot slot de categorieën van betrokkenen van wie de persoonsgegevens worden verwerkt. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetenen van een gemeente. De omvang en categorie van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere (zie ook de anderszins gevoelige persoonsgegevens). Denk bijvoorbeeld aan: minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie. Betrokkenen hebben op grond van de privacyregelgeving bepaalde rechten, zoals het inzage- en correctierecht.

De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingsdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Zo is wanneer het kind jonger is dan 16 jaar zo'n verwerking slechts rechtmatig, indien de toestemming of machtiging tot toestemming wordt verleend door de ouder of voogd. Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop hij geïnformeerd moet worden.

In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

- a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
- b. personen die voor een strafbaar feit zijn veroordeeld;
- c. slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit; en
- d. andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld onder a en b.

Bij conceptregelgeving kan het wenselijk zijn om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen. Wanneer de verwerking onder de werkingssfeer van de Richtlijn valt, is het verplicht om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen.

In het cliëntportaal worden gegevens aangetoond vanuit CIMS. Hiervoor worden de volgende gegevens vanuit CIMS verwerkt:

- Achternaam, initialen
- Geslacht
- Geboortedatum
- Vaccinsoort
- Streefdatum vaccinatie
- Fabrikant vaccin
- Batchnummer

Om toegang tot het Cliëntenportaal te krijgen wordt er gebruikt gemaakt van een externe leverancier, *identity* broker (Signicat) die de volgende persoonsgegevens verwerkt:

- BSN en IP adres

Zij zijn verplicht deze te bewaren voor audit-doeleinden. Dit punt wordt nader toegelicht onder Proportionaliteit & subsidiariteit

3. Gegevensverwerkingen



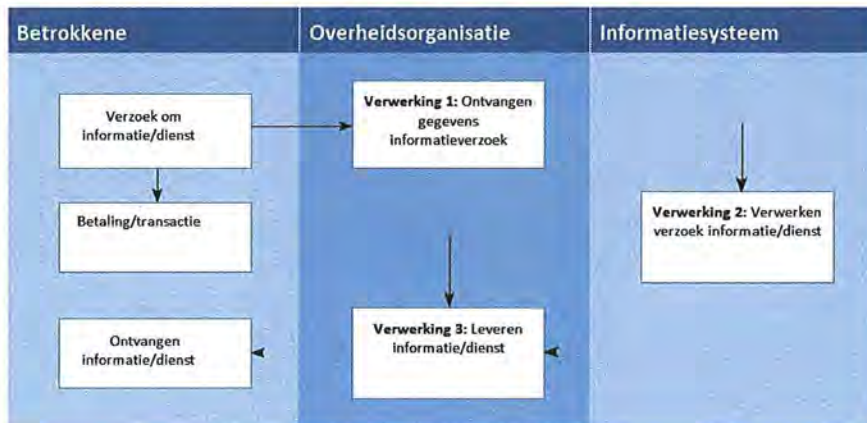
Geef alle voorgenenomen gegevensverwerkingen weer.

Klik hier om infotekst te verbergen

Om de rechtmatigheid van de voorgenenomen gegevensverwerkingen te kunnen beoordelen, is het noodzakelijk om alle gegevensverwerkingen in beeld te hebben. Onder verwerking wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Denk hierbij aan:

het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. Met andere woorden, het begrip omvat het gehele proces dat een persoonsgegeven doormaakt, vanaf het moment van verzamelen tot en met het moment van vernietigen.

Indien mogelijk verdient het aanbeveling om de gegevensverwerkingen te visualiseren, bijvoorbeeld aan de hand van een *input-proces-output* model, *flowchart* of *workflow*.



Het Cliëntenportaal is opgebouwd uit een serie componenten die in nauwe samenwerking de functionaliteit realiseren. De componenten zijn achtereenvolgens: web-client, Signicat identity-broker, DigiD (Logius identity provider), API-Gateway (extern en intern), cliëntenportaal-API en CIMS-API. Signicat verwerkt die persoonsgegevens voor logging doeleinden.

In de messagelog van de Signicat IdP-broker wordt

van de burger opgeslagen. Deze messagelog wordt encrypted opgeslagen op het Signicat systeem en deze is in te zien door de systeembeheerders van SSC-Campus, welke daarvoor expliciet geautoriseerd zijn. Deze messagelog is te benaderen via een internet ingang, welke is afgeschermd wordt met gebruikersnaam, wachtwoord en OTP-multifactor. De message log kan worden gedownload naar bv. het SIEM ten behoeve van monitoring en debugging. **(zie verdere beschrijving in document UitlegCliëntenportaal (slide 5 - 14))**

Om inzicht te bieden is een overzichtelijke plaat opgenomen op pagina 9, hieronder volgt de toelichting per component. Ter verduidelijking tijdens dit proces worden alleen persoonsgegevens verwerkt die voor het aanloggen met DigiD noodzakelijk zijn.

1. De burger bezoekt een informatiepagina op rivm.nl

(het RIVM gebruikt Piwik pro (privacy vriendelijker alternatief van Google Analytics, zie RIVM.nl Cookies statement. Dit zal onder andere het IP adres van de bezoeker gaan loggen).

De invulling van deze pagina is de verantwoordelijkheid voor de afdeling Communicatie en is buiten scope voor het project Cliëntenportaal. De verwerking van de BSN van de burger is via Signicat. Een verwerkersovereenkomst met Signicat is aanwezig. Tevens voldoet Signicat aan de in de BIO gestelde eisen voor dienstenleveranciers

2. De burger klikt op een knop of link die leidt naar het

Cliëntenportaal;

Signicat levert een access token t.b.v. aanmelding API-gateway. De API-gateway bepaalt toegang. Er worden geen persoonsgegevens verwerkt op de API gateway. (zie ook UitlegCliëntenportaal slide 17-21)

De burger ziet in zijn browser mijn.rivm.nl/vaccinaties als domeinnaam.

3. De burger leest de informatie op de homepage van het Cliëntenportaal en klikt op 'Inloggen met DigiD'



(zie ook

UitlegCliëntenportaal slide 22-26)

De applicatie stuurt de burger door naar login.rivm.nl

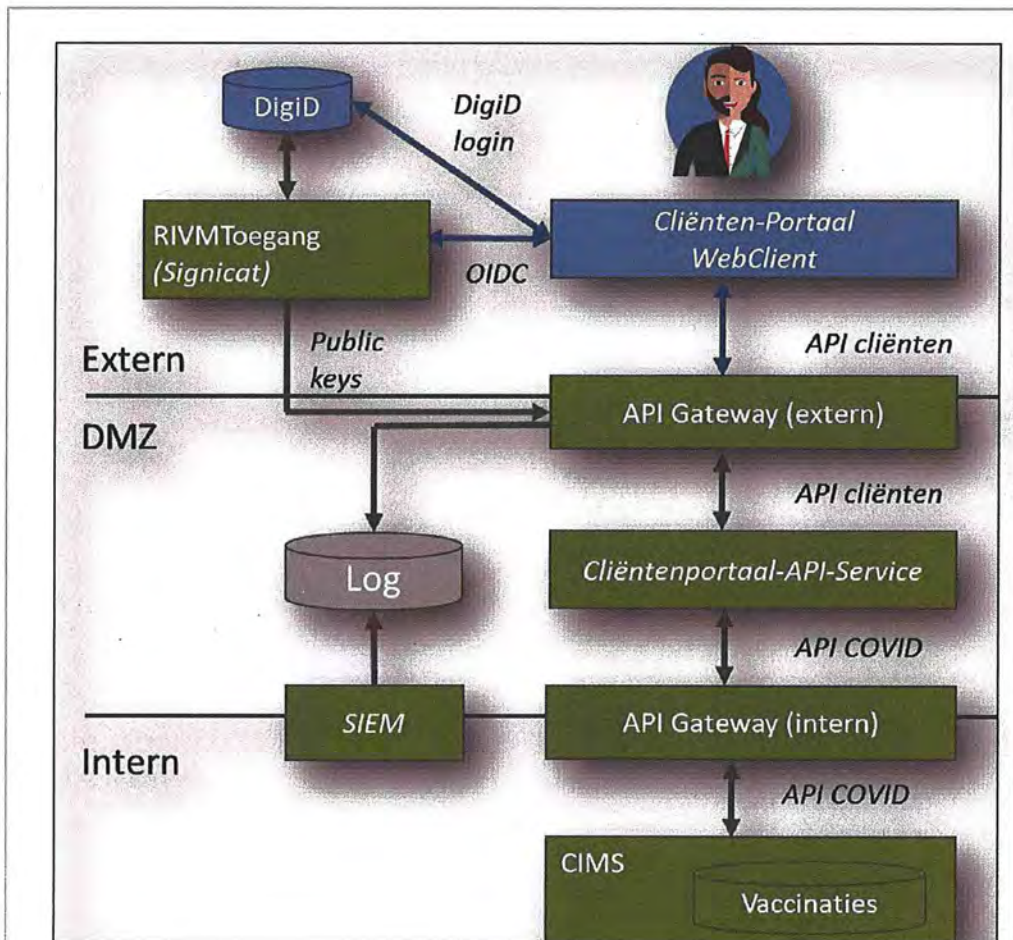
Op dit domein wordt de *identity broker* van RIVMtoegang gehost. De applicatie geeft aan de identity broker mee dat de scope het Cliëntenportaal betreft en dat de burger wenst in te loggen met DigiD.

4. De identity broker stuurt de burger door naar DigiD;
5. De burger logt in met DigiD;
6. DigiD stuurt de informatie over een succesvolle login terug naar de identity broker;
7. De identity broker stuurt de informatie over een succesvolle login terug naar het Cliëntenportaal;
8. Het Cliëntenportaal verwerkt de informatie van de succesvolle login;

De burger is nu ingelogd.

9. De burger kan gebruik maken van het Cliëntenportaal

Een nieuwe knop 'Mijn vaccinaties' verschijnt in het menu. De vaccinatiegegevens worden aangetoond.

**Begrippen:**

Webclient: De webclient is een softwarecomponent welke in de browser wordt geladen van de bezoeker, [REDACTED]. Middels de webclient heeft de bezoeker toegang tot de functies inloggen, ophalen van vaccinatiegegevens, ophalen van planningsgegevens, ophalen van uitwisselingen, versturen van e-mail tbv afmelden, uitloggen.

RIVMToegang: Dit betreft de *Signicat* identity Broker. Het verzoek tot authenticatie wordt door Signicat doorgezet naar DigiD. De bezoeker wordt doorverwezen naar de inlogpagina van DigiD.

DigiD:

[REDACTED]

[REDACTED]

API-Gateway-extern: Dit betreft een [REDACTED]

[REDACTED]

Cliëntenportaal-API-Service: Dit betreft een [REDACTED]
De Cliëntenportaal-API-Service vervult de volgende functies:

1. valideren van het identity-token waarin de BSN zit;
2. controle of BSN voorkomt in CIMS;
3. ophalen van client-, vaccinatie- en planningsgegevens en uitwisselingen, via de interne API-Gateway;
4. doorgeven van deze gegevens naar de Webclient, via de externe API-Gateway.

Het ophalen van de vaccinatie- en planningsgegevens vanuit de Cliëntenportaal-API gebeurt via een [REDACTED]

[REDACTED]

API-Gateway-intern: Deze gateway stelt zeker dat de CIMS-API vanuit de DMZ alleen aangeroepen kan worden door de Cliëntenportaal-API.

[REDACTED]

CIMS-API: Dit is een webservice op basis van [REDACTED]. Middels deze API kunnen gegevens over een client, vaccinaties, planning en uitwisselingen opgevraagd worden, aan de hand van het BSN. In de CIMS-database wordt een audit-log bijgehouden waarin alle raadplegingen worden geregistreerd.

[REDACTED]

SIEM: Security Information and Event Monitoring. Deze component bewaakt de toegang op de externe API-gateway. Het SIEM is een generieke voorziening die ook gebruikt wordt voor het analyseren van divers logfiles.

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen moeten worden getroffen om de risico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf daarom per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.

Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegespitst op de concrete gegevensverwerking, waarbij het algemene overkoepelende doel kan worden gebruikt als kapstok waaraan verschillende subdoelen kunnen worden gehangen, bijvoorbeeld:

- + e-mailadres: noodzakelijk voor communicatie met betrokkene;
- + ip-adres: noodzakelijk ter verificatie dat alleen vanuit een bepaalde locatie contact wordt gemaakt met het systeem;
- + adresgegevens: noodzakelijk om een beschikking naar de betrokkene te kunnen toezenden;
- + financiële gegevens: noodzakelijk om vast te stellen of de betrokken partij in aanmerking komt voor een toeslag;
- + strafrechtelijke gegevens: noodzakelijk om een screening te kunnen uitvoeren.

Wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen (met andere woorden: de persoonsgegevens zijn afkomstig van een andere persoon of organisatie dan wel uit een bestaand databestand) is het noodzakelijk om de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld te herleiden. De privacyregelgeving geeft namelijk als beginsel dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Met andere woorden: de verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld (zie voor de beoordeling van de verenigbaarheid punt 13 hieronder). Met verdere verwerking wordt bedoeld op gebruik van persoonsgegevens die al eerder voor een bepaald doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk, ten tijde van het verzamelen van de gegevens, was beoogd.

Bij **conceptregelgeving** wordt het doel van de gegevensverwerking in de regeling zelf vastgelegd of op zijn minst benoemd in de memorie of nota van toelichting. Een wettelijke doelomschrijving bevordert de rechtszekerheid omdat hierdoor een nadere invulling is gegeven aan het beoordelingskader.

Bij **overheidsverwerkingen** stelt de verwerkingsverantwoordelijke het doel van de gegevensverwerkingen zelf vast. Bij overheidsverwerkingen ter uitvoering van regelgeving moet binnen het doel worden gebleven dat daarin is vastgesteld. Het verdient de voorkeur de verwerkingsdoeleinden zoveel mogelijk op het niveau van werk- en organisatieprocessen te enten.

De doelstelling van het huidige Cliëntenportaal is niet iets nieuws, al in 2019 is er een pilot geweest m.b.t. het Cliëntportaal mede ingegeven door de motie Diertens uit december 2019 inzake de ontsluiting van gegevens naar PGO.
(zie ook Uitleg Cliëntenportaal slide 30 – 34)

Het cliëntportaal zal daadwerkelijk invulling geven aan de bovengenoemde doelstelling en aan de rechten van betrokkenen zoals benoemd in de AVG. Deze rechten zijn:

- Het recht van inzage, (artikel 15 AVG)
- Het recht op rectificatie (artikel 16 AVG)
- Het recht op gegevenswissing (recht op vergetelheid, artikel 17 AVG)

Inzage kan via het Cliëntenportaal verkregen worden door de viewing functie, men kijkt alleen op de relevante persoonsgegevens die in een "cache" worden getoond zoals eerder beschreven op blz 8 en op slide 3 en 4 van de begeleidende powerpoint UitlegCliëntenportaal.

Voor de andere rechten (rectificatie en gegevenswissing) kan een verzoek worden ingediend via het Cliëntenportaal. Middels het Cliëntenportaal wordt voldaan aan de wettelijke verplichting vanuit de AVG om transparantie te bieden richting de burger. Het verschaffen van inzicht in welk vaccin is toegediend en de mogelijkheid om dit zelf in te zien is dan ook van toegevoegde waarde in het leveren van deze transparantie voor de burger en samenleving. Om deze doelen te bereiken moeten persoonsgegevens verwerkt worden, welke alleen maar gegevens die noodzakelijk zijn om de verwerking mogelijk te maken.

Het legitieme doel dat wordt nagestreefd staat in verhouding tot het feit dat daarvoor persoonsgegevens moeten worden verwerkt. Op het moment van schrijven lijkt dit doel niet op een andere, minder ingrijpende wijze (bijvoorbeeld door géén of minder persoonsgegevens te verwerken) te kunnen worden bereikt.

5. Betrokken partijen



Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

[Klik hier om infotekst te verbergen](#)

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, moet inzichtelijk zijn welke organisaties (functioneel) betrokken zijn bij welke gegevensverwerking en in welke hoedanigheid: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger.

Verwerkingsverantwoordelijk is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die/dat het doel van en de middelen voor de gegevensverwerkingen vaststelt. Met andere woorden: degene die formeel bevoegd is te beslissen of persoonsgegevens worden verwerkt, voor welke doeleinden deze worden verwerkt en op welke wijze deze worden verwerkt. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijke en moeten zij onderling vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.

Verwerker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De verwerker verwerkt persoonsgegevens voor de verwerkingsverantwoordelijke, dat wil zeggen volgens diens instructies en onder diens verantwoordelijkheid. De verwerker is een buiten de organisatie van de verwerkingsverantwoordelijke staande persoon of organisatie. De verwerkingsverantwoordelijke en verwerker moeten onderling schriftelijk vastleggen wie waarvoor verantwoordelijk en aansprakelijk is. Om in een concreet geval te bepalen wie de verwerkingsverantwoordelijke is

en wie de verwerker is, moet naast de formele taakverdeling zoals partijen die onderling hebben afgesproken ook worden gekeken naar de feitelijke omstandigheden (waarom vindt de verwerking plaats? Wie heeft deze geïnitieerd?). Dat betekent dat enkel het schriftelijk vastleggen van de taakverdeling niet voldoende is: ook in de praktijk moet de verwerkingsverantwoordelijke zeggenschap hebben over het doel en de middelen van gegevensverwerkingen.

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt. Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens ter beschikking stelt.

Bij **conceptregelgeving** kan het wenselijk zijn om daarin de hoedanigheid van de betrokken organisaties vast te leggen of volgens welke criteria deze wordt aangewezen. Indien een specifieke regeling over gegevensverwerkingen wordt opgesteld ten behoeve van een publiekrechtelijke taak, dient in de regeling de verwerkingsverantwoordelijke te worden aangewezen. Zo is in de Basisregistratie personen vastgelegd wanneer het college van burgemeester en wethouders en wanneer de minister verantwoordelijk is voor het bijhouden van persoonsgegevens in de basisregistratie. In bepaalde gevallen kan het ook wenselijk zijn om wettelijk voor te schrijven dat de toegang tot bepaalde persoonsgegevens beperkt blijft tot een specifieke functionaris, zoals een officier van justitie, vertrouwenspersoon of bedrijfsarts.

Bij **overheidsverwerkingen** zullen, voor zover niet reeds wettelijk voorgeschreven, de organisaties die (functioneel) betrokken zijn bij de gegevensverwerkingen zelf en in onderling overleg moeten bepalen wie in welke hoedanigheid de persoonsgegevens verwerkt. Tevens zal moeten worden bepaald, voor zover eveneens niet wettelijk voorgeschreven, welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens, bijvoorbeeld aan de hand van een autorisatiematrix, in relatie tot de doeleinden van de gegevensverwerking. Hierin kan tevens worden bepaald in welke gevallen en onder welke voorwaarden deze functionarissen toegang krijgen tot de persoonsgegevens.

Betrokk en partij	Rol	Toegankelijk voor
RIVM	Verwerkersverantwoordelijk	Technisch applicatiebeheer: toegang tot de gegevens die door Signicat verwerkt worden. (eerder genoemde messagelog) Dit is mogelijk via het portal van Signicat. Deze log is alleen in te zien door 2 daartoe geautoriseerde systeembeheerders van SSC Campus (RIVM).
Signicat	Verwerker	Deze personen hebben toegang tot data die door Signicat verwerkt wordt: <ul style="list-style-type: none"> - De Signicat systeembeheerders - De technische support van Signicat - De klant (hier: RIVM) welke zelf de gegevens kan inzien die door Signicat bewaard worden
Amazon Web Services	Sub verwerker	Deze partij is een hosting partij en is een subverwerker van Signicat. Ze maken gebruik van datacentra in Ierland en Duitsland. Er bestaat een overeenkomst tussen Signicat en Amazon waarin staat dat de data niet verwerkt zal worden buiten de Europese Unie.
Logius	Leverancier DigiD	Geen toegang tot gegevens dus geen verwerker

6. Belangen bij de gegevensverwerking



Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

[Klik hier om infotekst te verbergen](#)

Bij de beoordeling van de rechtmatigheid van de gegevensverwerkingen kunnen tevens de belangen (lees: de waarde of de voordelen) die met de gegevensverwerkingen gemoeid zijn een rol spelen. Het kan hierbij zowel gaan om de private belangen van de verwerkingsverantwoordelijke, betrokkene en derden als het algemeen belang. Het gaat hier dus niet om de (mogelijk) negatieve gevolgen voor de betrokkenen. Denk hierbij bijvoorbeeld aan: bedrijfsbelangen, financiële belangen en commerciële belangen, het handhaven van juridische vorderingen, toezicht op medewerkers ten behoeve van de veiligheid of managementdoeleinden. (nationale of openbare) veiligheid, zoals de preventie van fraude, misbruik en netwerkbeveiliging, en gezondheid.

Het belang dat gemoeid is met de gegevensverwerkingen werkt door in de toets van de noodzaak (zie punten 11 en 14 hierna).

Het belang van VWS en het RIVM betreft het in de wet als zodanig verwoord algemene belang bij het kunnen voeren van de regie op en coördinatie van het vaccinatieprogramma tegen COVID-19 en de rechten van de betrokkenen.

Het belang van de betrokkenen bij de inzet van het Cliëntenportaal is dat zij op een eenvoudige, veilige, betrouwbare en adequate wijze kunnen worden geïnformeerd en inzage in hun gegevens wordt verschaft.

Het belang van de (sub)verwerker is om via één verbinding authenticatie van eindgebruikers met DigiD mogelijk te maken voor het RIVM en in het kader van fraude detectie (zoals oneigenlijk gebruik van DIGID met als gevolg identiteitsfraude) een zogenaamd messagelog aan te houden. Deze log bevat het originele bericht zoals dat ontvangen is van Logius of het RIVM. Hiermee wordt een audittrail opgebouwd om ook achteraf na te kunnen gaan of de authenticatiepoging veilig en zonder compromittatie verlopen is. Deze maatregel draagt bij aan het garanderen van de integriteit van de verwerking en het verwerkingssysteem. Een ongewijzigde audittrail heeft als doel:

- Onderzoek mogelijk maken naar technische incidenten;
- Onderzoek mogelijk maken naar oneigenlijk gebruik van DigiD (waaronder fraude) bij specifieke authenticatiepogingen;
- Onderzoek mogelijk maken naar specifieke authenticatiepoging bij klachten.

7. Verwerkingslocaties



Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Klik [hier](#) om infotekst te verbergen

De locaties waar de voorgenomen gegevensverwerkingen plaatsvinden, kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Tevens heeft de verwerkingslocatie invloed op de competentie van de (leidende) privacytoezichthouder.

Om te borgen dat de regels betreffende de bescherming van persoonsgegevens niet omzeild worden door persoonsgegevens in een ander land te verwerken, bepalen de AVG en de Richtlijn dat gegevensverwerkingen buiten de Europese Unie enkel onder bepaalde omstandigheden zijn toegestaan. Dit is bijvoorbeeld het geval indien het derde land naar het oordeel van de Europese Commissie een passend beschermingsniveau heeft (een adequaatheidsbesluit) of indien gebruik wordt gemaakt van passende waarborgen om de betrokkenen te beschermen. Daarnaast zijn een aantal specifieke situaties waarin gegevensverwerkingen in een derde land toch zijn toegestaan ondanks het ontbreken van een passend beschermingsniveau en passende waarborgen, zoals uitdrukkelijke toestemming van de betrokkenen.

Naast de AVG en de Richtlijn kunnen andere wettelijke regels of beleid invloed hebben op de locaties waar persoonsgegevens kunnen worden verwerkt. Denk hierbij aan het VIRBI 2013 inzake gerubriceerde overheidsinformatie en situaties waarin opslag in een overheidsdatacenter geëigend is.

De gegevensverwerkingen vinden op één uitzondering na in Nederland plaats. De logs die Signicat bijhoudt worden namelijk door de subverwerker Amazon Web Services (AWS) verwerkt. AWS maakt gebruik van datacentra in Ierland en Duitsland. Er bestaat een overeenkomst tussen Signicat en AWS waarin staat dat de data niet verwerkt zal worden buiten de Europese Unie



8. Techniek en methode van gegevensverwerking

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

[Klik hier om infotekst te verbergen](#)

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, profilering en big data-verwerkingen.

Geautomatiseerde besluitvorming

Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.

Voor verwerkingen die onder de werkingssfeer van de AVG vallen, geldt dat dit verbod niet van toepassing indien het besluit:

- noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
- berust op de uitdrukkelijke toestemming van de betrokkene.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn geldt dit verbod niet indien het besluit:

- wettelijk is toegestaan; en
- voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.

Profilering

Onder profilering wordt verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:

- op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.

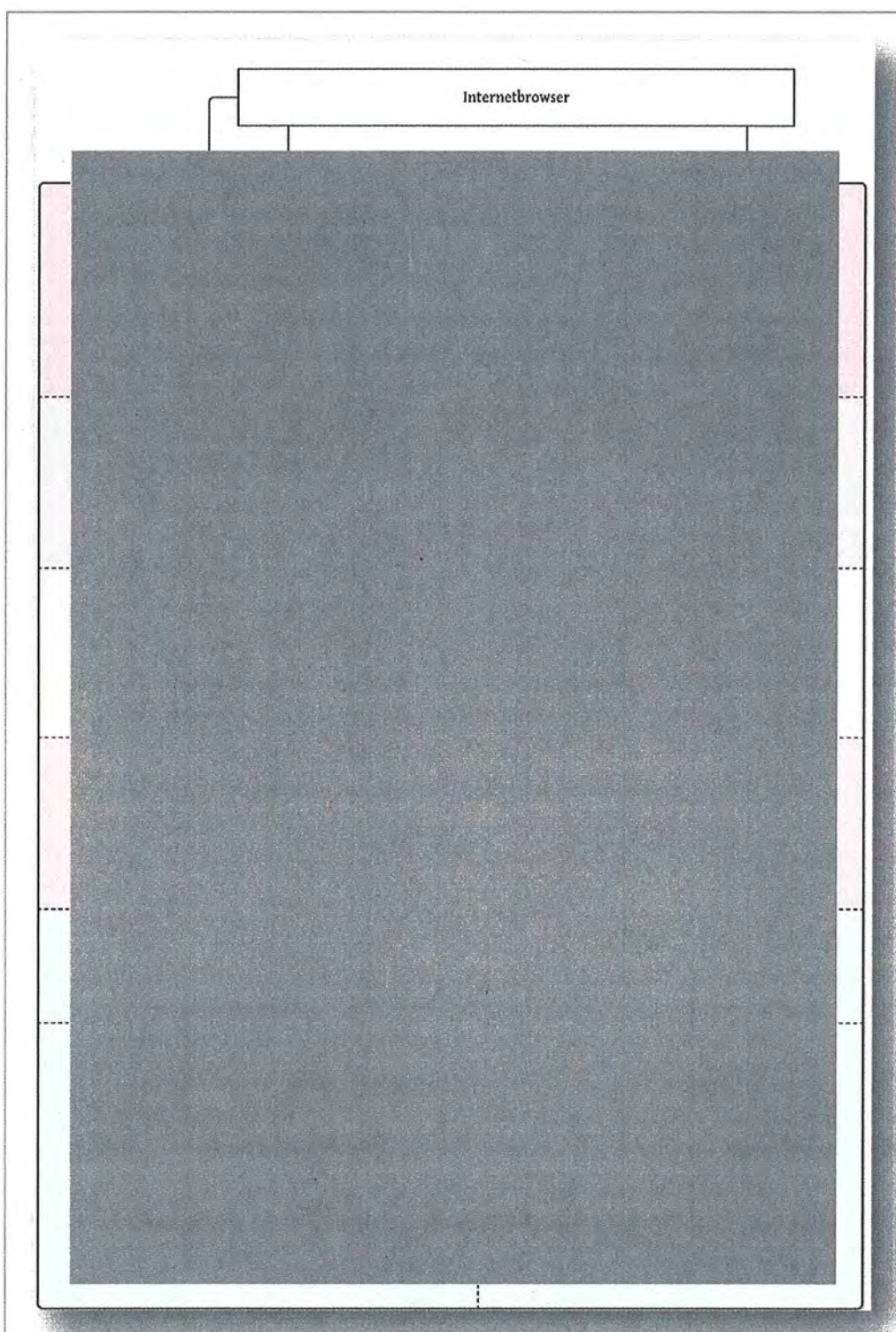
Big data

Big data is als zodanig niet gedefinieerd in de privacyregelgeving, maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering. *Big data* staat voor het verschijnsel dat grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij

geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau. In de kern komt het bij *big data*-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van *big data* brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Nieuwe technologieën

Ook grote verschuivingen in de werkwijze, de manier waarop persoonsgegevens worden verwerkt en de technologie die daarbij gebruikt wordt, kunnen gevolgen hebben voor betrokkenen. Denk aan: intelligente volgsystemen op basis van GPS, biometrie en nieuwe vormen van identificatie.



Koppelvlakken van het Cliëntenportaal

In de Bronsystemen laag vinden we onderaan de CIMS en Praeventis databases. In deze databases worden naast burgergegevens uit de BRP de vaccinatie- en vaccinggegevens opslagen. Ook worden de vaccinatieplanningen in deze databases opgeslagen. Het Cliëntenportaal haalt data uit deze databases door middel van een API die de

database bevraagt. Deze API is alleen intern bereikbaar en wordt ontsloten middels een interne API Gateway. Als identity broker verwerkt Signicat het BSN. Deze wordt vervolgens op de identity broker versleuteld verwerkt, en Signicat heeft de sleutel.

Signicat en haar processen van softwareontwikkeling en dienstverlening zijn ISO27001 gecertificeerd. Dat betekent dat onder andere dat toegang tot productiesystemen (waarin de audittrail te benaderen is) enkel voorbehouden is aan de personen die dat nodig hebben om de uitvoering van de dienstverlening mogelijk te maken.

Daarnaast worden de DigiD-verbindingen onderworpen aan een DigiD-assessment door een onafhankelijke auditor. Deze assessments zijn verplicht door Logius en worden gedaan op basis van het DigiD-normenkader. Het DigiD assessment voor deze toepassing is recentelijk afgerond met een positief resultaat.

Het cliëntenportaal voldoet aan de richtlijnen van de Baseline Informatiebeveiliging Overheid (BIO) en is goedgekeurd door de stuurgroep CIMS op 18 maart 2021.

Functionele mogelijkheden in fase 1 (8 april 2021):

1. in/uit te loggen met DigiD om toegang te verkrijgen tot het Cliëntenportaal
2. aan te geven dat een vaccinatie wel is toegediend;
3. een verzoek in te dienen tot correctie of om zijn of haar gegevens te verwijderen uit zijn of haar CIMS en/of RVP dossier
4. in het Nederlands en in het Engels weer te geven;
5. middels een Privacy Verklaring in te zien hoe het Cliëntenportaal omgaat met zijn of haar privacy;
6. in te zien wie zijn of haar dossier(s) heeft geraadpleegd en / of gemuteerd;

9. Juridisch en beleidsmatig kader



Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

[Klik hier om infotekst te verbergen](#)

Naast of in de plaats van de AVG en de Richtlijn kan (sectorale) regelgeving de mogelijkheden voor gegevensverwerkingen creëren, conditioneren of beperken. Voorbeelden van dergelijke wetten zijn: Wet algemene bepalingen burgerservicenummer, Wet gebruik burgerservicenummer in de zorg, Wet basisregistratie personen, Algemene wet inzake rijksbelastingen, Archiefwet, Telecommunicatiewet.

Kadasterwet, Handelsregisterwet 2007, Kieswet, Wet bijzondere maatregelen grootstedelijke problematiek, Wet op de geneeskundige behandelingsovereenkomst, Omgevingswet, Jeugdwet, Wet maatschappelijke ondersteuning 2015 en Participatiewet. Deze lijst is niet uitputtend.

Er kan ook departementaal of rijksbreed beleid zijn dat de mogelijkheden voor de voorgenomen gegevensverwerkingen conditioneert of beperkt. Bijvoorbeeld ten aanzien van de opslag en beveiliging van persoonsgegevens.

Aan de hand van deze inventarisatie kan bij onderdeel B beoordeeld worden of de voorgenomen gegevensverwerkingen rechtmatig zijn en bij onderdeel D of specifieke maatregelen voorgeschreven zijn.

Het relevante juridische kader staat vooral in de Wet publieke gezondheid (hierna: Wpg) en het bijbehorende Besluit publieke gezondheid (hierna: Besluit), de wet op het RIVM, het Besluit ex artikel 3, eerste lid, onderdeel a, van de Wet op het RIVM

Voor het vaccinatieprogramma is ervoor gekozen om voor de verstrekking van gegevens aan RIVM gebruik te maken van de uitdrukkelijke toestemming van de betrokkene (patiënt). De zorgverlener vraagt dus toestemming van de gevaccineerde persoon voor de verstrekking van de vaccinatiegegevens aan RIVM en alleen als deze de gevraagde toestemming geeft verstrekt de zorgverlener deze vaccinatiegegevens aan RIVM.

10. Bewaartermijnen



Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is. Met andere woorden: indien het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd. Op dit beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering indien de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen.

Bij **conceptregelgeving** zal moeten worden bepaald en gemotiveerd of het al dan niet wenselijk is om een specifieke minimale of maximale bewaartermijn voor te schrijven. Aan de hand van het uitgangspunt dat de bewaartermijn in verhouding moet staan met de verwerkingsdoeleinden, moet de gekozen termijn worden gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn.

Bij **overheidsverwerkingen** moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Indien dat het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden. Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de gegevens periodieke toetsen aan het beginsel van opslagbeperking.

Hierbij moet rekening worden gehouden met andere regelgeving over bewaartermijnen, zoals de Archiefwet 1995.

Voorbeeld opsomming bewaartermijn voor persoonsgegevens bij overheidsverwerkingen (IT/uitvoering):

Categorie	Ingang	Termijn	Motivatie	Verantwoordelijke
Persoonsgegevens	bewaartermijn	van bewaring	bewaring	voor verwijdering

Naam	Vanaf moment dat de betrokkene voor het eerst inlogt in het systeem.	365 dagen, als de gebruiker 'onthouden inloggegevens' aanklikt 30 dagen.	Deze persoonsgegevens zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases.	Functioneel beheerder
------	--	--	---	-----------------------

Zoals bij punt 8 aangegeven worden de berichten, van en naar de Signicat Identity Broker gelogd in een zogenaamde messagelog. Hierin zit het IP, BSN van de burger.

Om het onderzoek naar een specifieke authenticatiepoging betrouwbaar te maken, is het van belang dat er kan worden beschikt over een originele audittrail waarin aantoonbaar geen wijzigingen zijn aangebracht. Een originele audittrail zorgt ervoor dat een authenticatiepoging van begin tot eind met voldoende zekerheid gereproduceerd kan worden. De authenticatiepoging kan zo gekoppeld worden aan een individu/specifiek geval dat onderwerp is van een klacht of onderzoek naar oneigenlijk gebruik van DigiD.

De opslagtermijn is 1 week dit is in overleg met de beheer afdeling van het RIVM afgesproken om het termijn van bewaren van BSN nummer zo kort mogelijk te houden zonder dat dit invloed heeft op de werkzaamheden.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

11. Rechtsgrond



Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

[Klik hier om infotekst te verbergen](#)

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Als uitwerking van dit beginsel is geregeld dat een

gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden:

- a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Op de gegevensverwerkingen noodzakelijk zijn, wordt beoordeeld onder punt 14.

Ten aanzien van de rechtsgronden c (wettelijke plicht) en e (taak van algemeen belang) geldt dat deze moet worden vastgesteld bij of krachtens de wet. De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Met betrekking tot rechtsgrond e (de taak van algemeen belang) geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak tevens worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

De Richtlijn gegevensbescherming opsporing en vervolging voor dat een gegevensverwerking door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid alleen rechtmatig is indien die verwerking gebaseerd is op de wet.

Bij **conceptregelgeving** zal de regeling veelal tot gevolg hebben dat de verwerkingsverantwoordelijke de gegevensverwerking kan baseren op de rechtsgrond genoemd onder c (wettelijke verplichting). Dit is het geval indien de gegevensverwerking noodzakelijk is ter uitvoering van de wettelijke verplichting en indien de verwerkingsverantwoordelijke belast is met de uitvoering van de wettelijke plicht. Daarnaast kan regelgeving tot gevolg hebben dat een overheidsorgaan de gegevensverwerking kan baseren op de rechtsgrond genoemd onder e (taak van algemeen belang). De publieke taak wordt (of is reeds) wettelijk vastgelegd waarbij, naast andere onderwerpen, volgens de Aanwijzingen voor de regelgeving ook aandacht moet worden geschonken aan de daarbij noodzakelijke gegevensverwerkingen. In regelgeving kan ook worden voorgeschreven dat toestemming van de betrokkene vereist is om persoonsgegevens te verwerken, en daarmee de andere rechtsgronden uitsluiten.

Bij **overheidsverwerkingen** zal het overheidsorgaan de voorgenomen gegevensverwerkingen moeten baseren op één van de zes rechtsgronden. De rechtsgrond genoemd onder f geldt niet voor gegevensverwerkingen in het

kader van de uitoefening van publieke taken. Wel kan deze rechtsgrond gebruikt worden voor gegevensverwerkingen in de bedrijfsvoering, zoals cameratoezicht, bezoekersregistratie en toegangscontrole. In veel situaties zal de rechtsgrond genoemd onder a (toestemming) evenmin kunnen dienen als rechtsgrond voor gegevensverwerkingen door overheidsorganen, omdat de betrokkene in de gegeven situatie niet vrijelijk toestemming kan geven.

Indien de gegevensverwerkingen gebaseerd worden op de rechtsgrond genoemd onder f (het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde), dan stelt de AVG als eis dat de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde.

De verwerking binnen CIMS is beschreven in de DPIA CIMS van december 2020. Het Cliëntenportaal voorziet in het recht op inzage zoals is geregeld in de AVG, artikel 12 lid 2 "de verwerkingsverantwoordelijke faciliteert de uitoefening van de rechten van de betrokkene..." In het bijzonder faciliteert het Cliëntenportaal de artikelen 15, 16 en 17 van de AVG. Zoals in overweging 63, behorend bij artikel 15 van de AVG, verwoord staat moet een betrokkene het recht hebben om de persoonsgegevens die over hem zijn verzameld, in te zien, en om dat recht eenvoudig en met redelijke tussenpozen kunnen uitoefenen. Dit houdt ook in dat betrokkenen het recht dienen te hebben op inzage in hun persoonsgegevens betreffende hun gezondheid, zoals de gegevens in hun medisch dossier.

Daarnaast is de aanleiding voor de inrichting van het Cliëntenportaal gebaseerd op de Nederlandse digitaliseringsstrategie om meer regie te geven over eigen gezondheidsgegevens (kamerbrief Regie op persoonlijke gegevens bij de overheid, 32761 nr. 147). Hierbij is binnen de VWS ook afgesproken dat vanaf 2018, alle patiënten de mogelijkheid krijgen om hun belangrijkste medische gegevens digitaal in te zien, veilig, op eigen initiatief, zelfstandig, vanuit een willekeurige locatie (zie het Informatieberaad).

12. Bijzondere persoonsgegevens



Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

[Klik hier om infotekst te verbergen](#)

De AVG verbiedt de verwerking van bijzondere persoonsgegevens. Op dit verwerkingsverbod gelden de volgende uitzonderingen:

- de betrokkene heeft uitdrukkelijke toestemming gegeven;
- de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht;
- de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
- de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
- de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
- de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
- de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnoses, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsel en diensten;
- de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;

- j de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Verdere uitzonderingen zijn te vinden in nationale regelgeving.

De AVG bepaalt daarnaast dat verwerking van strafrechtelijke gegevens alleen is toegestaan door of onder toezicht van de overheid of als dit bij wet geregeld is (zie voor de definitie van strafrechtelijke gegevens de toelichting bij punt 2).

De verwerking van nationale identificatienummers is alleen toegestaan ter uitvoering van de wet of voor doeleinden die bij wet zijn bepaald. Overheidsorganen kunnen bij de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer, zonder dat daarvoor nadere regelgeving vereist is.

De Richtlijn schrijft voor dat verwerking van bijzondere persoonsgegevens slechts is toegestaan wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van betrokkene, en:

- a. wettelijk is toegestaan;
- b. noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of
- c. die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.

Bij conceptregelgeving kan van het verbod op de verwerking van bijzondere of strafrechtelijke persoonsgegevens worden afgeweken, mits passende waarborgen worden geboden ter bescherming van persoonsgegevens en andere grondrechten van de betrokkene.

Veel van de bovenstaande gegevensverwerkingen van gezondheidsgegevens binnen CIMS zijn noodzakelijk met het oog op de uitvoering, coördinatie en monitoring van het vaccinatieprogramma tegen COVID-19 en zijn, in het verlengde daarvan, daarmee van belang voor de volksgezondheid en de bewaking van de individuele gezondheid van de te vaccineren personen. Dit belang heeft de wetgever in de wetsgeschiedenis met zoveel woorden uitdrukkelijk onderkend. Kennis hebben van het vaccinsoort, vaccinatiedatum en productnaam beschermt de vitale belangen van de betrokkene of een ander natuurlijke persoon.

In deze fase van het Cliëntenportaal worden alleen vaccinatiegegevens opgevraagd en getoond via het web portal. Dit zijn de onderstaande gegevens:

- Vaccinsoort
- Vaccinatiedatum
- batchnummer
- productnaam (e.g. AstraZenica)

Zoals eerder genoemd worden in het kader van identificatie en fraude detectie BSN nummers verwerkt. Een BSN nummer is wellicht geen bijzonder persoonsgegeven in de zin van de AVG maar omdat er een kans bestaat het hier herleid kan worden naar vaccinatie gegevens dient het wel degelijk hier vermeld te worden. Gebruik van het BSN is noodzakelijk om te kunnen borgen dat de juiste personen worden opgeroepen, gevaccineerd en geregistreerd. Hiervoor geldt hetzelfde zoals door de wetgever in de wetsgeschiedenis in het kader van het destijds geldende

Rijksvaccinatieprogramma, heeft opgemerkt:⁸

"[...] Om zeker te kunnen stellen dat het RIVM in alle gevallen de doorgegeven vaccinatie plaatst in het RVP-dossier van de juiste persoon moet het RIVM van de toediener [...] de naam en adres gegevens, de geboortedatum, het BSN en de geslachtsaanduiding ontvangen. Naast BSN zijn deze persoonsgegevens noodzakelijk om fouten [...] te achterhalen."

13. Doelbinding



Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze.

De AVG regelt dat de verdere verwerking voor een ander doel toegestaan is indien de verdere verwerking berust op toestemming van de betrokkene of op een specifiek wettelijk voorschrift, dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, monetaire, budgettaire of fiscale aangelegenheden. Daarnaast wordt de verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar geacht met de oorspronkelijke doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkene te beschermen.

Bij **conceptregelgeving** moet worden beoordeeld of het noodzakelijk is om wettelijk te regelen dat verdere verwerking toegestaan is (zie ook punt 14 hierna), bijvoorbeeld in verband met de doorbreking van een geheimhoudingsplicht.

Binnen het hierboven geschetste kader voor verwerking voor een ander doel bestaat ruimte voor een wettelijke regeling op grond waarvan sets van persoonsgegevens van meerdere partijen uit meerdere domeinen worden gecombineerd ten behoeve van een big data analyse, waarbij gegevens worden verwerkt ten behoeve van een in die wettelijke regeling vastgesteld doeleinde, dat niet met het oorspronkelijke doel waarvoor de gegevens zijn verzameld, verenigbaar is. Dit laat onverlet dat de verwerkingsverantwoordelijke die beslissingen neemt ten aanzien van individuele personen of een groep van personen op basis van de uitkomsten van die analyse zelfstandig moet voldoen aan alle eisen voor rechtmatige gegevensverwerking. Een dergelijke verwerking dient op een eigen rechtsgrond te berusten (zie punt 11).

Bij **overheidsverwerkingen** moet de verwerkingsverantwoordelijke zelf beoordelen of de verdere gegevensverwerking voor een ander doel toegestaan en verenigbaar is aan de hand van:

- het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
- de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;

⁸ Kamerstukken II 2015/16, 34 472, nr. 3, p. 3 en 6.

- c. de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
- d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
- e. het bestaan van passende waarborgen.

De Richtlijn staat de verdere verwerking van persoonsgegevens toe voor een doelstelling die binnen het toepassingsgebied van de Richtlijn valt, niet zijnde die waarvoor zij zijn verzameld, voor zover:

- a. de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken, en
- b. de verwerking noodzakelijk is en in verhouding staat tot dat andere doel.

De verdere verwerking voor andere doeleinden is enkel op basis van de wet toegestaan. Wanneer de persoonsgegevens voor zulke andere doeleinden worden verwerkt, is de AVG van toepassing.

De doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking hebben een verband. De verwerker heeft de persoonsgegevens die zijn verzameld van de burger, zoals IP adres en BSN, nodig om diezelfde burger toegang te verschaffen tot het Cliëntenportaal. Men kan immers niet de benodigde informatie inzien als men niet de gegevens benodigd voor identificatie afgeeft. De verwerker verwerkt bijzondere categorieën van persoonsgegevens omdat dmv het nummer benodigd om een persoon te identificeren een kleine kans bestaat (zie hiervoor de verdere uitleg in het risico log) dat d.m.v. het inzage verzoek het vaccinatiegegeven af te leiden is. Daarnaast brengt onzorgvuldig gebruik van het BSN privacy risico's met zich mee. Bijvoorbeeld misbruik van persoonsgegevens en identiteitsfraude. Passende waarborgen zijn noodzakelijk voor de verwerking van deze BSN nummers en worden dan ook uitvoerig in de DPIA beschreven en als privacy risico inclusief mitigatie vermeld.

De doeleinden van de voorgenomen verdere verwerking versterken juist de verhouding tussen de betrokkenen (burgers) en de verwerkingsverantwoordelijke (RIVM) aangezien deze verwerking de transparantie zoals vereist door de AVG (artikel 15,16,17) mogelijk maakt. Het is juist de aard van de persoonsgegevens, wat maakt dat er gebruik wordt gemaakt van een zorgvuldig geselecteerde verwerker met de juiste certificaten (ISO27001) en interne processen (toegang is enkel mogelijk op basis van 2-factor authenticatie en wordt gemonitord en gelogd). Data wordt alleen verstuurd via beveiligde verbindingen (TLS) en logs die t.b.v. de audittrail versleuteld worden opgeslagen.

Dit alles wordt gedaan om de mogelijke negatieve gevolgen van de voorgenomen verdere verwerking voor de betrokkenen tot een minimum te beperken.



14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

- a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?**
- b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?.**

Klik hier om infotekst te verbergen

De privacyregelgeving geeft als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord 'noodzakelijk' in artikel 6 AVG en artikel 8 Richtlijn. De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de voorgenomen gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken.

Daarbij kunnen empirische onderzoeksresultaten helpen.

Bij subsidiariteit wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt. Bijvoorbeeld:

- kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?
- kan het verwerken van de persoonsgegevens in een beperktere vorm of met minder verwerkingen?

Zo kan in bepaalde gevallen met foto's hetzelfde doel worden bereikt (bijvoorbeeld: identificatie) als met het verwerken van filmbeelden. Het subsidiariteitsbeginsel houdt bijvoorbeeld ook in dat als persoonsgegevens openbaar gemaakt gaan worden, niet automatisch alle persoonsgegevens openbaar worden gemaakt, maar een selectie wordt gemaakt op grond van gerechtvaardigde criteria. Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Bij conceptregelgeving kunnen de uitkomsten van deze afweging worden meegenomen in de grondrechtentoets van het IAK.

Voor de proportionaliteitstoets van de hiervoor beschreven verwerkingen in het kader van het DVP Cliëntenportaal is het allereerst belangrijk dat, anders dan bij de reguliere vaccinatieprogramma's, sprake is van veel grotere aantallen van gevaccineerden en ook van een veel hogere mate van urgentie. In het licht daarvan is het, meer dan bij andere vaccinatieprogramma's, nodig dat er op een autonome manier en dus op grotere schaal inzicht kan worden gegeven in de eigen vaccinatiegegevens. Dit kan alleen door middel van een portaal waarbij de burger zijn/haar gegevens individueel in kan zien en waarin de burger zijn/haar rechten kan oefenen. Voor elke verwerking geldt als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is

voor de verwerkingsdoeleinden. Er wordt bij elke verwerking gekeken naar de minimale gegevensverwerking in het kader van dataminimalisatie (conform artikel 6 AVG en artikel 8 Richtlijn).

Het is zonder BSN niet mogelijk je te identificeren en te authenticeren. Daarnaast is DigiD hét middel om op een betrouwbare manier in te loggen en wordt hiervoor al voor veel andere toepassingen gebruikt.

Het achteraf verwerken van DigiD berichten in een zogenaamd messagelog betekent onder meer dat, vastgesteld moet kunnen worden dat de authenticatie of inlog met DigiD betrouwbaar is gebeurd en dat evt misbruik of betwistingen kunnen worden onderzocht en weerlegd. De keten RIVM-Signicat-Logius (DigiD server) moet kunnen aantonen dat die berichten gestuurd zijn en verwerkt conform de eisen vanuit DigiD. Hier wordt Signicat op geaudit, en is er onder meer een TPM verklaring tbv DigiD (ook wel DigiD audit of assessment genoemd op basis van het DigiD normenkader) en een ISO 27001 certificering.

Wanneer we in het bericht het BSN zouden verwijderen, betekent dat ingrijpen in het bericht zoals dat van Logius wordt ontvangen (en dat ook door Logius is ondertekend) en het verbreken van de ondertekening van dat bericht. Dit valt niet te herstellen. Daarmee is de integriteit van het bericht achteraf niet meer vast te stellen. Een fraudeur of een betwisting kan daarmee niet meer weerlegd worden op basis van de gebruikshistorie van DigiD bij het RIVM. Met andere woorden, de veiligheid, betrouwbaarheid en integriteit van hele systeem gaat daarmee achteruit.

Herstelvermogen is een ander relevant uitgangspunt voor deze messagelogs. Wanneer er ergens in de keten een verstoring is, is het belangrijk om te kunnen traceren wat er mis gaat of is gegaan. Dat kan voor een individuele gebruiker, of voor de toepassing zeer relevant zijn. In dit herstelvermogen speelt dezelfde messagelog een belangrijke rol, en ook daarvoor geldt dat het belangrijk is dat de berichten inclusief ondertekening (dus intact) opgeslagen worden.

De messagelog is alleen toegankelijk voor personeel betrokken bij die evt doelen: fraude opsporing, navraag of herstellen van de dienst. Deze toegang is enkel mogelijk op basis van 2-factor authenticatie en wordt gemonitord en gelogd.

Daarnaast is het verwerken van het BSN nummer op deze manier ook opgenomen als geaccepteerd risico en zijn er voldoende mitigerende maatregelen genomen zowel technisch als organisatorisch om de bescherming van de persoonsgegevens van de betrokkenen te waarborgen. (zie het risklog onder nummer 16 in deze DPIA)

Om de subsidiariteitstoets te kunnen toelichten zijn er twee mogelijkheden die uiteengezet kunnen worden. Er is overwogen om een directe koppeling met DigiD te maken, zonder tussenkomst van externe partijen zoals Signicat. Een directe koppeling op DigiD heeft echter tot gevolg dat er voor de overige identificatiemiddelen losse koppelingen gemaakt moeten worden. Het Cliëntenportaal is nu al verplicht om eIDAS (zie eIDAS-verordening van 29 september 2018) aan te bieden. Hiervoor zou dan weer gekoppeld moeten worden met Signicat (of een andere herkenningmakelaar).

Dit is een belangrijk punt, aangezien in de toekomst te verwachten is dat burgers op het Cliëntenportaal naast DigiD ook moeten kunnen inloggen met eIDAS (alle erkende identificatiemiddelen van de Europese lidstaten), Idensys, iDIN, IRMA. Tevens is er de verplichting dat een gemachtigde zaken moet kunnen regelen voor een burger. Machtigingen voor de burger zijn: vrijwillig, bewind voering, ouderlijk gezag, nabestaanden of balie. In dat geval moet iemand met één van de eerder genoemde middelen, of een bedrijf met eHerkenning namens de burger in kunnen loggen op het Cliëntenportaal. Ook de machtigingsvoorzieningen moeten gekoppeld worden.

Ook de doorlooptijd voor het realiseren van een directe koppeling met Logius is niet wenselijk. Dit kost minimaal een maand doorlooptijd voor de techniek en daarnaast nog veel tijd voor assessments, certificeringen, pentesten etc.

Het is belangrijk hierbij te vermelden dat RIVM toegang niet alleen maar de koppeling met DigiD dient. RIVM toegang is toekomst vast, en dat moet ook in consideratie genomen worden bij het kiezen welke diensten erop aangesloten worden. De keuze voor een identity broker als Signicat is dus ook in dit geval noodzakelijk en daarmee ook de eerder genoemde werkwijze kan op dit moment niet met redelijkheid op een andere, voor de betrokkene minder nadelige wijze worden uitgevoerd.

15. Rechten van de betrokkene



Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

[Klik hier om infotekst te verbergen](#)

Betrokkenen hebben op grond van de privacyregelgeving diverse rechten, waarin ook staat op welke wijze en onder welke omstandigheden zij die rechten kunnen uitoefenen. Het betreft het recht op informatie, het recht van inzage, het recht op rectificatie, het recht op gegevenswissing, het recht op beperking van de verwerking, een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens, het recht op overdraagbaarheid van gegevens, het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen moeten altijd op een nationale wet berusten, direct zijn toegestaan op grond van de bepalingen in de Europese privacyregelgeving.

Indien in **conceptregelgeving** een uitzondering wordt gemaakt op de rechten van betrokkenen moet worden beoordeeld of dit is toegestaan op in de privacyregelgeving genoemde gronden en moeten specifieke bepalingen worden opgenomen met betrekking tot ten minste:

- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens;
- het toepassingsgebied van de ingevoerde beperkingen;
- de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte

- e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
- f. de opslagperiodes en de toepasselijke waarborgen;
- g. de risico's voor de rechten en vrijheden van betrokkenen;
- h. het recht van betrokkenen om over de beperking te worden geïnformeerd, tenzij dit afbreuk kan doen aan het doel van de beperking.

Geef bij **overheidsverwerkingen** aan hoe invulling wordt gegeven aan de rechten van betrokkenen, bijvoorbeeld op welke wijze de betrokkenen worden geïnformeerd en hoe wordt omgegaan met een aanvraag voor correctie en wissing van gegevens. Indien de verwerkingsverantwoordelijke uitzonderingen wil maken op de uitoefening van bepaalde rechten van betrokkenen, geef aan waarom dat noodzakelijk is en op welke grond dat is toegestaan.

Via het Cliëntenportaal is voorzien in een privacyverklaring waarin duidelijk aangegeven op welke manier met gegevens van betrokkenen om wordt gegaan. Daarnaast is de inzet van het Cliëntenportaal ook het daadwerkelijk invulling geven aan de rechten van betrokkenen, namelijk: de inzage, correctie en verwijderen van persoonsgegevens, waarbij correctie en verwijderen alleen een aanvraag is die verder door medewerkers wordt afgehandeld. Indien nodig kan via het clientportaal bezwaar worden gemaakt tegen de aanwezigheid van de vaccinatieregistratie van betrokkenen. Dit wordt verder verwoord in de reeds aangehaalde privacyverklaring.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's



Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;**
- b. de oorsprong van deze gevolgen;**
- c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;**
- d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.**

[Klik hier om infotekst te verbergen](#)

Volgens de privacyregelgeving dient een PIA een beoordeling van risico's voor de rechten en vrijheden van de betrokkenen te bevatten. Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen te worden bepaald. Op basis van een objectieve beoordeling kan vastgesteld worden of de gegevensverwerking gepaard gaat met een (hoog) risico. Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.

Het gaat hier om een risicogerichte benadering die kan bestaan uit de volgende stappen:

1. risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

Deze benadering zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging. Daarom kan ook gebruik gemaakt worden van informatie die daaruit naar voren is gekomen. Anders dan bij deze risicoafweging die gericht is op de betrouwbaarheidseisen voor informatiesystemen, en daarmee de risico's voor de verantwoordelijke (zoals aanpassing, vertrouwen, publiciteit, toezicht en handhaving, dienstverlening, betrouwbare informatie), ziet de risicoafweging van de PIA op de risico's voor de betrokkenen.

De privacyregelgeving schrijft niet voor op welke wijze de risicoanalyse moet worden uitgevoerd. Het verdient aanbeveling om aan te sluiten bij internationale standaarden, bijvoorbeeld van de International Organization of Standardization (ISO), Eenduidige Normatiek Single Information Audit (ENSIA) en Organisation for Economic Co-operation and Development (OECD).

1. Risico's identificeren

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens.

Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie. Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties:

- * waar de gegevensverwerking kan leiden tot:
 - a. discriminatie, stigmatisering en uitsluiting;
 - b. (blootstelling aan) identiteitsdiefstal of -fraude;
 - c. financiële verliezen;
 - d. reputatie- of anderszins relationele schade;
 - e. verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
 - f. ongeoorloofde ongedaanmaking van pseudonimisering;
 - g. of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;
- * wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
- * wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;
- * wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- * wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
- * wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

2. Risico's inschatten

Vervolgens moeten de benoemde risico's worden gekwalificeerd door het inschatten van de kans dat een dreiging zich voordoet en de mogelijke gevolgen daarvan voor de betrokkenen. Met andere woorden: wat zijn de gevreesde gevolgen en hoe groot is de impact daarvan op de betrokkenen? En hoe treden deze in werking en

hoe waarschijnlijk is dat? Deze vragen zijn niet gericht op zwart-wit antwoorden, maar op een afweging. Aan de hand hiervan moet een risiconiveau worden bepaald.

De impact/ernst van de risico's hangt af van de context van de verwerkingen: de aard van de persoonsgegevens, de aard van de verwerkingen en de doeleinden waarvoor de gegevens worden verwerkt.

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking. Alsook van de aard van de persoonsgegevens.

Persoonsgegevens die de sleutel vormen voor toegang tot geldelijke middelen of waarmee een betrokkene te chanteren is, zijn aantrekkelijk voor hackers. Denk hierbij aan de inloggegevens voor DigiD of een datingwebsite.

De kans dat zich gevolgen voordoen voor de rechten en vrijheden van de betrokkenen, kan tevens verband houden met de (mate van) beveiliging van de persoonsgegevens. De al dan niet opzettelijke:

- vernietiging en verlies (beschikbaarheid);
 - wijziging (integriteit);
 - ongeoorloofde toegang en verstrekking (vertrouwelijkheid);
- van persoonsgegevens, kan leiden tot schade voor de betrokkene.

Voor het inschatten van de risico's kan het behulpzaam zijn om de betrokkenen of hun vertegenwoordigers te consulteren.

Big data-verwerkingen kunnen specifieke risico's voor de betrokkene met zich brengen. Zo kan een algoritme een correlatie ontdekken die weliswaar in statistische zin logisch is, maar die kan leiden tot vooroordelen en stereotypering, discriminatie en sociale uitsluiting of anderszins impact heeft op de betrokkenen, bijvoorbeeld bij sollicitaties, het aangaan van leningen en afsluiten van verzekeringen.

Ook bestaat het risico dat de betrokkene onderworpen is aan big data-besluitvorming die hij niet begrijpt en waar hij geen invloed op heeft.

3. Risico's beoordelen

Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn.

Risico's in dit kader worden met name gemitigeerd door de technische informatiebeveiligingsmaatregelen. Hierbij wordt daarom verder verwezen naar de risicoanalyse van CIMS. Tevens geven de pentesten ook de nodige aanbeveling om technisch gezien maatregelen te nemen.

#	Privacy Risico's - en MITIGERENDE MAATREGELEN	Status	MITIGERENDE MAATREGELEN	Restrisico na mitigeren	Risico eigenaar	Geaccepteerd?
1	SIGNICAT slaat logfiles met encrypted BSN-nummer op voor fraude-analyse.	Open	<p>MITIGERING d.m.v. nieuwe maatregelen:</p> <ol style="list-style-type: none"> 1. BSN nummer niet langer opslaan dan 1 week 2. Deze situatie accepteren tot er over wordt gegaan naar het nieuwe koppelvak (versie 4.5) van DigiD hier is TVS alreeds op aangesloten. Op dit koppelvak wordt het BSN encrypted doorgegeven. De tussenliggende partij kan het BSN dan niet ontsleutelen Dit zou naar 6 maanden al mogelijk kunnen zijn. <p>Daarnaast zijn er al diverse maatregelen genomen:</p> <ol style="list-style-type: none"> 1.BSN nummers worden zoals aangegeven niet herkenbaar maar als 9 cijfers verpakt in tokens 2.Om aan het data minimalisatie principe te voldoen slaat Signicat het BSN op zonder context op deze manier is Signicat niet in staat om het BSN te gebruiken voor het herleiden van de vaccinatiegegevens. 3.Het messagelog wordt encrypted opgeslagen op het Signicat systeem 4.Het messagelog is in te zien door systeembeheerders van SSC-Campus en specifieke administrators van Signicat welke daarvoor expliciet geautoriseerd zijn 5.De toegang tot de messagelog is afgeschermd met [REDACTED] 	Midden		
2	Blootstelling aan identiteitsdiefstal of -fraude door oneigenlijk gebruik van de DIGID toegang	Open	MITIGERING: misbruik toegang is gezekerd met certificaten en DIGID. Tevens SIEM/SOC logging en monitoring door Signicat via het messagelog	Laag	Stuurgroep registratie	
3	Verlies persoonsgegevens tijdens het uitvoeren van identificaties	Open	MITIGERING: beveiliging van identity broker is conform geldende eisen van ISO en BIO en gebaseerd op best practises, DIGI D assessments zijn uitgevoerd	Laag	Stuurgroep registratie	
4	Enig ander aanzienlijk economisch of maatschappelijk	Open	MITIGERING: kweek bewustwording inzake dit privacy risico, daarnaast een RIVM breed beleid op misbruik van	Laag	Stuurgroep registratie	

nadeel voor de natuurlijke persoon in kwestie;		persoonsgegevens, integreer dit in het gangbare beleid			

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. Maatregelen

I

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Denk bij maatregelen bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid voor de betrokkenen, periodieke controles, toezicht verstevigen, verhogen bewustwording en dataminimalisatie.

Daarnaast kunnen de maatregelen ook beveiligingsmaatregelen omvatten. De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op een dusdanige manier wordt verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De verwerkingsverantwoordelijk moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. In het begrip passend ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip passend duidt mede op een proportionaliteit tussen de maatregelen en erkende privacyrisico's. Naarmate de risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens. Er is geen verplichting om altijd de zwaarste beveiliging te nemen. Enkel is vereist dat de maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn. Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Beveiligingsrisico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een restrisico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom dit aanvaardbaar wordt geacht.

Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismen.

Ter illustratie noemt de AVG de volgende maatregelen:

- a. pseudonimiseren en versleutelen van persoonsgegevens;
- b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- opslag van gegevens in een kluis;
- project-, risico- en incidentenmanagement;
- data opsplitsen;
- dataminimalisatie;
- back-ups;
- integriteitscontroles;
- meerfactor-authenticatie;
- monitoring en logging;
- controle van toegekende bevoegdheden;
- privacybewustzijn- en beveiligingstrainingen;
- managementrapportages over risicobeheer;
- beperken inzageniveau;

- periodiek een audit of hack- of penetratietest uitvoeren;
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- responsible-disclosurebeleid;
- geheimhoudingsverklaringen;
- service level agreements (met boeteclausules);
- verwerkersovereenkomsten;
- screening personeel en VOG-verklaring.

Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Rijksdienst (BIR).

De Richtlijn noemt tot slot de volgende maatregelen:

- a. controle op de toegang tot de apparatuur;
- b. controle op de gegevensdragers;
- c. opslagcontrole;
- d. gebruikscntrole
- e. controle op de toegang tot gegevens;
- f. transmissiecontrole;
- g. invoercontrole;
- h. transportcontrole; en
- i. herstelbaarheid.

De Richtlijn verplicht tot het bijhouden van logbestanden van bepaalde vormen van verwerkingen, opdat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens.

Bij **conceptregelgeving**: ook op het niveau van regelgeving kunnen maatregelen worden getroffen. Denk hierbij aan het voorschrijven van maximum bewaartermijnen, het beperken van inzage in en besluiten over persoonsgegevens tot bepaalde functionarissen of geheimhoudingsverplichtingen.

Big Data

Bij Big data-analyses (zie punt 8) waarbij persoonsgegevens worden verwerkt, dient, gelet op de daarmee gepaard gaande risico's, in het bijzonder aandacht te worden besteed aan het treffen van de volgende maatregelen.







- Zorg ervoor dat naarmate de mogelijkheden van patroonherkenning bij de toepassing van big data minder zijn, een goede validatie door experts op het desbetreffende vakgebied plaatsvindt om het risico van foutieve uitkomsten zoveel mogelijk te reduceren.
- Zorg ervoor dat de data zoveel als met een redelijke inspanning mogelijk is, up to date zijn, de te gebruiken datasets een zo gering mogelijke bias (afwijking) bevatten en dat de te gebruiken algoritmen en analysemethoden deugdelijk zijn.
- Bepaal, rekening houdend met de potentiële impact van de toepassing, de foutmarge die bij de toepassing mag optreden.
- Zorg ervoor dat nuttige informatie aan betrokkenen wordt verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegeven in gebruikte algoritmen en analysemethoden.

Bij de toepassing van de uitkomsten van big data-analyses dient aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg voor menselijke tussenkomst in het proces van geautomatiseerde besluitvorming.

- Naarmate de potentiële negatieve impact voor de betrokkene groter wordt, neemt de noodzaak voor een goede validatie en een weging van de uitkomsten navenant toe.

CLIENTEN PORTAAL				
	Status	Restrisico voor mitigering	MITIGERENDE MAATREGELEN	Restrisico na mitigering
RISICO's - en MITIGERENDE MAATREGELEN				
MISBRUIK IDENTITY MIDDEL		HOOG		Laag
FOUTEN IN TOEGANG TOT ACHTERLIGGENDE DIENST		HOOG	MITIGERING:	Laag
RISICO'S OMDAT KRITIEKE PATCHES NIET UITGEROLD KUNNEN WORDEN		HOOG	MITIGERING:	Laag
SIGNICAT IDENTITY PROVIDER NIET BESCHIKBAAR		MIDDEN	MITIGERING:	Laag
RIVM Toegang NIET BESCHIKBAAR Het risico dat RIVM Toegang haar beschikbaarheidspercentage niet haalt en tijdelijk uit de lucht is.		LAAG	RIVM Toegang heeft Beschikbaarheidseisen en de organisatie wordt zij ingericht dat deze gehaald wordt. Client krijgt bij verstoring een (niet technische) foutmelding te zien.	LAAG

RISICO's - en MITIGERENDE MAATREGELEN	Status	Restrisico voor mitigering	MITIGERENDE MAATREGELEN	Restrisico na mitigering
CLIENTENPORTAAL niet beschikbaar		MIDDEN	MITIGERENDE MAATREGELEN:	Laag
CLIENTENPORTAAL niet beschikbaar door overbevolgung		HOOG	MITIGERENDE MAATREGELEN:	MIDDEN
RISICO bevindingen DIGID assessment niet op tijd opgelost.		HOOG	MITIGERENDE MAATREGELEN:	LAAG
PRODUCTIEGEGEVENS ZICHTBAAR VOOR ONTWIKKELAARS Het risico op inzage Productiegegevens door ontwikkelaars.		MIDDEN	MITIGERING: Wanneer productie-data gebruikt worden in de acceptatieomgeving zijn deze geanonimiseerd.	LAAG
CLIENTENPORTAAL INTERN Benaderbaar.		MIDDEN	MITIGERING:	Laag
Data uit achterliggende dienst niet beschikbaar. => Logging, monitoring. Gebruiker krijgt een melding, Technische melding in logging prio 1.		LAAG	MITIGERENDE MAATREGELEN: Gebruiker krijgt een melding dat het systeem wegens onderhoud niet beschikbaar is	Laag

AVG ASSESSMENT, DIGID ASSESSMENT BEVINDINGEN		HOOG	Geheimen dienen gedeeld te worden op basis van need-to-know , met zo min mogelijk entiteiten en zo kort mogelijk. Zodoende dienen ze beschermd te worden tot op het moment van gebruik door gebruik te maken van sterke encryptie en correct toegangsbeheer.	Laag
PHISHING / FRAUDE / SOCIAL ENGINEERING		MIDDEN	MITIGERING:	Laag
LEGACY CONNECTIES TOT ACHTERLIGGENDE DIENSTEN		HOOG	MITIGERING:	Laag
PENTESTRESULTATEN EN BEVINDINGEN Testfunctionaliteit buiten ontwikkelomgeving		HOOG	MITIGERING:	Laag
PENTESTRESULTATEN EN BEVINDINGEN Plaintext geheim		MIDDEN	Geheimen dienen gedeeld te worden op basis van need-to-know , met zo min mogelijk entiteiten en zo kort mogelijk. Zodoende dienen ze beschermd te worden tot op het moment van gebruik door gebruik te maken van sterke encryptie en correct toegangsbeheer. Plaintext geheim	Laag
PENTESTRESULTATEN EN BEVINDINGEN Onjuist afbreken van sessie		MIDDEN	Oude cookie blijft geldig.	Laag
PENTESTRESULTATEN EN BEVINDINGEN Cross-Origin Resource Sharing policy niet streng genoeg		LAAG	Het is raadzaam om de CORS-policy strenger in te stellen en alleen de domeinen toe te staan die toegang tot de API nodig hebben.	Laag
PENTESTRESULTATEN EN BEVINDINGEN - OPM Digid assessment eis Content-Security-Policy header implementatiefout Als pentestbevinding Laag conform penteststandaardrating op techniek, maar Hoog als bedrijfsrisico omdat het verplicht is voor het Digid assessment.		HOOG / AANBEVELING	Verifieer desondanks of het mogelijk is de CSP strenger in te stellen. De strengere CSP kan eerst getest worden met de Report-Only-functionaliteit, alvorens hem live te zetten.	Laag
PENTESTRESULTATEN EN BEVINDINGEN - OPM Digid assessment eis Referrer-Policy header ontbreekt. Als pentestbevinding Laag conform penteststandaardrating op techniek, maar Hoog als bedrijfsrisico omdat het verplicht is voor het Digid assessment.		HOOG / AANBEVELING	De applicatie maakt geen gebruik van de Referrer-Policy-header. Dit is volgens norm U/PW.03 van de ICT-beveiligingsrichtlijnen voor webapplicaties verplicht voor applicaties die Digid gebruiken.	Laag
PENTESTRESULTATEN EN BEVINDINGEN - OPM Digid assessment eis Information disclosure - Serverinformatie Als pentestbevinding Laag conform penteststandaardrating op techniek, maar Hoog als bedrijfsrisico omdat het verplicht is voor het Digid assessment.		HOOG / AANBEVELING	De API-server toont een kleine hoeveelheid informatie over de gebruikte technologie in een response header. Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen informatie over systemen en software in cookies of HTTP headers mee. Zorg dat foutmeldingen zonder specifieke systeem informatie getoond worden.	Laag
PENTESTRESULTATEN EN BEVINDINGEN Testfunctionaliteit buiten ontwikkelomgeving		LAAG / AANBEVELING	Uit de response valt op te maken dat de democontroller in de acceptatieomgeving aanwezig is.	Laag
VERWERKING BSN EN IP ADRES DOOR SIGNICAT		HOOG	MITIGERING: de verwerking moet z.s.m. stoppen, er is geen duidelijk grondslag om deze persoonsgegevens te verwerken.	Laag

Hier kunt u aanvullende punten toevoegen: selecteer de tab **Invoegen**, kies **Snellerdelen, Aanvullend punt**

Voeg hier wanneer gewenst een afsluitende alinea toe. Denk bijvoorbeeld aan:

- Lessen uit deze PIA
- Volgende stappen etc.

Maatregelen
nemen
Privacybewustwording
Doelbinding
Noodzaak
Effecten in kaart
PIA
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond
Met open vizier

Periode	4-3-2021t/m 17-3-2021
Projectnummer	V/190007/01/CI
Project	Covid Informatie en Monitoring Systeem (CIMS) (CIMS Cliëntenportaal)
Projectleider	
ProjectStatus	CIMS CP: finalisatie

Oplegnotities bij de agenda van de Stuurgroep d.d. 22 maart 2021

- Donderdag 18-3 moet definitieve inhoud/aanpassingen binnen zijn zodat deze voor woensdag de 24^{ste} kunnen zijn opgepakt
- We sturen op live gang van 8 april, op de website hebben we laten zetten dat we half april live gaan. Voorstel is om dit zo te houden en zo een week speelruimte te hebben richting publiek om zo een 'stille' live gang te kunnen hebben
- Consignatiedienst niet (voldoende) bemand. Vanuit BI krijgen we verschillende signalen dat als men na live gang in de avond belt men niet thuis geeft omdat dit niet is geregeld voor een aantal onderwerpen binnen de keten. Denk aan RIVMToegang en API Gateway en ontwikkeling CP

CIMS CP**Gedaan:**

- DPIA gestart afgerond en obv input FG vindt 18-3 sessie plaats
- Risico analyse 0.9 opgesteld en aan stuurgroep voorgelegd vwb de punten die nu nog niet gesloten zijn
- Hertest Code review en pentesten Sogeti afgerond
- Door CIMS en RIVM/Rubix taskforce is hard doorgewerkt
- Go Live plan afstemmen met CIMS keten vindt elke dag plaats
- Start inrichten PROD
- 2nd opinion pentest gepland
- Finale ACC performance en PROD test gepland voor 23 en 25 maart
- Accessibility test is uitgevoerd, score: 42 van de 50 punten voldoen. We kregen een compliment! Nu werken aan de 8 resterende punten

Te doen:

- Uitvoeren performance test op PROD
- Productie omgeving opleveren
- DPIA afronden
- Risico analyse afronden
- Dry run houden

Beheer**Gedaan:**

- wekelijkse afstemmingssessies voor beheer gestart olv [REDACTED]
- Rollen matrix gefinaliseerd
- Beheerplannen gereviewed
- Scan voor beheer door security

Te doen:

- Kosten aangeleverd krijgen door [REDACTED] voor beheer
- Checklist van [REDACTED] doorlopen en acties op ondernemen

Bespreking	Stuurgroep covid-registratie
Vergaderdatum en -tijd	1 april 2021, 11.00 – 12.00 uur
Vergaderplaats	Webex
Deelnemers	[redacted] (vz.), [redacted], [redacted], [redacted], [redacted] (secr.)
Afwezig	
Kopie aan	[redacted], [redacted], [redacted]

1. Mededelingen

- Stuurgroep Covid vaccinaties informatie-uitwisseling adviseert twee wijzigingen in BRBA/BRBB: opslag van data van personen die geen toestemming verlenen om data aan te leveren aan RIVM; data aan te leveren aan de huisartssystemen. [redacted] heeft op 30 maart kennis genomen van het advies. Advies wordt gedeeld met BRBA-team. Bijlage g.
- RIVM voert de VITAL-studie uit en gaat in dat kader ook vaccineren. Aanleveren van vaccinatiedata vanuit VITAL aan het landelijk register is niet geregeld.
- [redacted] heeft verlof van 23 tot en met 30 april 2021. [redacted] neemt rol van [redacted] waar voor interne (RIVM) zaken, [redacted] blijft de externe zaken (bronssystemen) doen.
- [redacted] verlaat het vaccinatieprogramma en daarmee ook haar rol als secretaris voor de stuurgroep Registratie. Opvolger wordt gezocht.
- [redacted] meldt dat [redacted] is aangesteld als product owner CIMS. [redacted] en [redacted] zullen hem in gaan werken.
- Een dataleveranciers heeft een datalek veroorzaakt (data aangeleverd met gegevens over opt in, die RIVM niet mag hebben). Privacy experts nemen de nodige acties. Belangrijk dat communicatie (van RIVM en van de dataleverancier) goed is aangesloten [redacted] checkt bij [redacted] of hier voldoende actie op zit.

Actie 144 Joris: Check bij [redacted] of communicatie van RIVM en dataleverancier voldoende aangesloten is op het datalek.

2. Live gang Cliëntportaal

Volgende week dinsdag is een extra overleg van de stuurgroep gepland, specifiek voor de accordering van de livegang van het cliëntportaal.

Uit de stukken blijkt wat gedaan is met de adviezen van de FG en dat er een risico resteert dat we willen gaan accepteren. Hier is VWS van op de hoogte.

Vastgesteld wordt dat het datalek opgelost moet zijn vóór de livegang. In de oplegnota zal nog iets duidelijk naar voren gebracht worden dat Logius ook naar een oplossing zoekt wat betreft de nu nog nodige inzet van een broker. Voorstel is

daar een termijn van 6 maanden aan te hangen.

Met deze opmerkingen zijn de stukken voor nu verder akkoord.

3. 1 prik scenario

wordt hartelijk welkom geheten. Aan de hand van de korte presentatie geeft ze toelichting over de stand van zaken rondom het 1 prik scenario (na doorgemaakte Covid) en welk stappen er verder nog gezet moeten worden. Er is nog geen analyse gedaan wat het betekent voor CIMS, wat er moet gebeuren, wat haalbaar is en op welke termijn wat in gang gezet moet worden. Over het doel en de bedoeling is geen discussie, maar er zijn wel verschillende beelden over wat kan. CIMS is bedoeld voor Covid registratie en is niet bedoeld voor registratie van infectie. Afsproken wordt dat nu capaciteit vrijgemaakt wordt voor een impactanalyse. Het verder uitwerken is een volgende stap en daar wordt nu nog niet over besloten, omdat daar substantieel capaciteit voor nodig is. Dat kan eventueel leiden tot herprioritering.

Besluit 41: vrijmaken capaciteit voor impactanalyse 1 prik scenario.

Actie 145 en leveren use case aan voor de registratie.

Actie 146, , en : impactanalyse 1 prik scenario (na doorgemaakte Covid) o.b.v. de use case.

4. Prioritering t.b.v. planning en resourcing april 2021

Vorig jaar is een roadmap opgesteld voor 2021 Q1. geeft toelichting op de stukken die nu voorliggen. Allereerst geeft de stuurgroep de complimenten voor de voorliggende stukken.

Voor Q2 is een actuele roadmap nodig en een prioritering voor april. De resourcing (wie hebben we nodig voor welk project) is nog niet heel duidelijk en transparant. Ter verduidelijking: met punt 6 wordt niet alle dashboards bedoeld, maar het dashboard voor de monitoring van de kwaliteit van data.

De organisatie wordt niet alleen belast met vragen rondom CIMS; het registratieprogramma is onderdeel van het Covidvaccinatieprogramma waar resourcing voor gevraagd wordt. Suggestie om na te denken over een splitsing, met als voorbeeld LCC: reguliere werk en Covid-werk. Voor de IV-organisatie speelt dit niet zo, omdat alles met elkaar te maken heeft.

Het 1 prik scenario moet er nog in opgenomen worden.

In het overzicht is beheer meegenomen.

Samenvatting:

- Scope ruimer maken, dus ook de dashboards/managementinformatie en bestelmodule toevoegen.
- Resourcing wat scherper in beeld brengen.
- Impactanalyse 1 prik scenario toevoegen
- Deze lijst regelmatig terug laten komen in de stuurgroep om te checken op actualiteit.

Actie 147 Adrie: past op basis van de bespreking de prioritering incl. Dashboards en Bestelmodule t.b.v. planning en resourcing april 2021 aan.

5. Verbetering datakwaliteit

Eerder is gesproken over de verbetering van de kwaliteit van data. Voorkeur heeft optie 4, waarbij RIVM onjuiste data corrigeert en dit terugkoppelt aan de bron. Daarbij is ook aan de orde geweest dat er onderscheid gemaakt zou kunnen worden in:

- Onjuiste data waar we niets aan willen doen
- Onjuiste data waar die we zelf corrigeren
- Onjuiste data die de bron moet corrigeren.

Het batchnummer is één van de gegevens die juist moeten zijn. Suggestie is dat we daar in ieder geval mee gaan starten.

Actie 148 [REDACTED]: past de beslisnota DPV_265 aan met overige aanpassingen in de data.

6. Hoofdpuntenrapportage Landelijke Registratie

Iedereen neemt kennis van de rapportage en koppelt eventuele vragen en opmerking terug in het volgend stuurgroepoverleg.

7. Verslag voorgaand overleg, acties

Iedereen neemt kennis van het verslag, koppelt eventuele suggesties terug aan [REDACTED], en pakt de acties op.

8. Rondvraag

Geen.

Acties

	Verslag-datum:	Actie:	Wie:	Status:
141	24.03.2021	Clientportaal: risico-acceptatie en bijbehorend formulier verder laten uitwerken en tijdlijn maken voor terugkoppeling aan de FG en vaststelling door de stuurgroep.		Tijdlijn is besproken met privacy coördinatoren. Zij stemmen af met de FG. Nieuwe versie op 1 april in de stuurgroep, vaststelling op 6 april.
142	24.03.2021	Aanlevering procesinformatie: check of er nog iets nodig is op het gebied van DPIA.		Gedaan. FG wil alleen achteraf geïnformeerd worden.
143	24.03.2021	Aanlevering procesinformatie: gezien het dalende percentage, is er actie nodig richting de minister		
144	01.04.2021	Check of communicatie van RIVM en dataleverancier voldoende aangesloten zijn bij datalek		Gedaan, afgehandeld conform RIVM-procedure.
145	01.04.2021	Aanleveren use case 1-priksenario		
146	01.04.2021	Impactanalyse 1 prik scenario opstellen o.b.v. de use case.		
147	01.04.2021	Aanpassing prioritering inclusief Dashboards en Bestelmodule t.b.v. planning en resourcing april 2021.		
148	01.04.2021	Update nota DPV_265 "verbeteren datakwaliteit" met overige dataverbeteringen.		

Afspraken/besluiten

Nummer:	Verslag-datum:	Afspraak
1.	13.08.2020	Samenstelling en rolverdeling projectstuurgroep conform Projectbrief versie 0.3.
2.	13.08.2020	Governance volgens scrummethodiek met productowner en scrumteam. Ook behoudt van de projectstuurgroep (Prince2) om issues op te lossen, kaders te geven en te bewaken, risico's te bewaken. Het scrumteam bestaat uit DVP, BIS, de leverancier(s).
3.	13.08.2020	We gaan starten met twee sporen: 1 kopie Praeventis gereedmaken voor verdere inrichting; 2 ruimere verkenning van informatiesystemen.
4.	13.08.2020	krijgt van mandaat om het project te starten.
5.	31.08.2020	Er wordt niet verder buiten het RIVM naar andere bruikbare systemen gekeken.
6.	31.08.2020	Alle mogelijk bruikbare koppelingen met LSP realiseren.
7.	15.09.2020	De Stuurgroep gaat akkoord met de start van het sprintteam Functionele Inrichting aan de hand van use case versie 0.4.
8.	15.09.2020	Het sprintteam rapportage tooling kan gaan starten zodra de resourcing compleet is.
9.	15.09.2020	wordt afgezend van het RIVM in de stuurgroep LSP+/PGO t.b.v. CIMS.
10.	12.10.2020	wordt de contactpersoon vanuit de IV-organisatie.
11.	26.10.2020	
		s eigenaar van de systeemrisico's van de infrastructuur, de applicatie, portalen en tooling.
13.	26.10.2020	coördineert de antwoorden op de beleidsonzekerheden (samen met).
14.	24.11.2020	Het cliëntbeheer wordt centraal ingericht, d.w.z. dat alle DVP'ers (ongeacht regiokantoor) gegevens kunnen verwerken. De autorisaties en de logging van feitelijke verwerking door individuele medewerkers worden hiervoor ingericht. Indien vanuit privacy-afweging wel beperking opgelegd moet worden, wordt dat geregeld op het niveau van de autorisaties van de DVP'ers.
15.	24.11.2020	Programmabureau covidvaccinatiecampagne is verantwoordelijk voor het aanleveren van de afgestemde Use Case en de bijbehorende afgestemde procesplaten.
16.	07.12.2020	Livegang CIMS is op 30 december 2020.
17.	11.12.2020	Stuurgroep is akkoord met de voorgestelde scope voor DPIA opgesteld voor de livegang CIMS op 30 december 2020.
18.	15.12.2020	Programmanager () en centrumhoofd () tekenen risicoacceptatieformulier, en kijken mee en brengen het in bij . Er is sprake van een getrapte ondertekening: (CISO) en (privacy officer) leggen het risicoacceptatieformulier voor aan de programmanager CIMS (), hoofd DVP () en crisismanager CIMS (). Zij accepteren de genoemde risico's wel of niet, waarna ze het formulier voorleggen aan de CIO () en

		pDG/portefeuillehouder privacy/CFO (). Zij volgen de risicoacceptatie van () (of niet) en bieden het acceptatieformulier aan aan DG-RIVM (). DG-RIVM is eindverantwoordelijk en gaat ultiem akkoord of benoemt extra maatregelen.
19.	15.12.2020	informeert privacy officer over beleidskeuzes die impact kunnen hebben op scope risicoanalyse.
20.	15.12.2020	kanaliseert de aanpassingen aan CIMS. Als deze lijken te bekliven, dan geeft aan door welke wijzigingen in PIA moeten worden meegenomen.
21.	15.12.2020	Stuurgroep stemt in met deprioritering van het Zorgverlenersportaal (zie DPV_182).
22.	15.12.2020	Voorstel aannemen mensen i.h.k.v. inrichting registratiesysteem CMS is bekrachtigd door stuurgroep.
23.	21.12.2020	Stuurgroep is akkoord met een beschikbaarheid van 98,5% voor het platform Praeventis, de SFTP server CIMS en de applicatie/database CIMS. In januari 2021 wordt toegewerkt naar een beschikbaarheid van 99,9%. Stuurgroep is ook akkoord op de voorgestelde voorlopige inrichting van het service window. De stuurgroep gaat ervanuit dat dit een startsituatie voor januari 2021 is, die kan wijzigen. Hiertoe zal eind januari 2021 een evaluatiemoment in de stuurgroep plaatsvinden. Mogelijk worden dan nieuwe of herijkte afspraken gemaakt.
24.	28.12.2020	Stuurgroep: <ul style="list-style-type: none"> – onderschrijft dat GGDHOR alleen volgens de reeds bestaande werkwijze vaccinatiedata kan aanleveren, omdat de tijd ontbreekt om de geplande oplossing te realiseren; Wij kunnen rechtstreeks in hun omgeving met hen koppelen. – neemt kennis van de risico's en de daarmee samenhangende politiek/bestuurlijke kwetsbaarheid voor RIVM; hangt reputatie rondom route. – besluit de koppeling met GGDGHOR te realiseren.
25.	28.12.2020	Stuurgroep is akkoord met de functionaliteiten genoemd in DVP_195 en stuurt aan op livegang op 8 januari 2021 onder de condities gegeven in DVP_195. Het formele besluit wordt op 7 januari 2021 genomen.
26.	05.01.2021	Stuurgroep besluit dat DPIA en IB-analyse beide groen licht geven voor het ontvangen van gegevens van GGD GHOR voor CIMS.
27.	05.01.2021	Stuurgroep stemt in met het verwijderen van Geboorteland uit de registratie.
28.	06.01.2021	Stuurgroep accepteert de informatiebeveiligings(rest)risico's zoals deze benoemd zijn in de Oplegnotitie risicoregister CIMS 1.0 voor livegang van CIMS release 1 en accordeert de beschreven vervolgacties voor ná livegang.
29.	06.01.2021	Stuurgroep heeft in lijn met DPIA, analyse door Privacy Officer en het advies van de FG voldoende vertrouwen dat er in CIMS release 1 op een goede manier met privacy wordt omgegaan.
30.	06.01.2021	Stuurgroep gaat akkoord met de genoemde functionaliteit, compliance, beheer en in te richten CAB zoals genoemd in DPV_194 Besluitnota livegang CIMS release 1. Stuurgroep besluit om CIMS release 1 live te brengen op 6 januari 2021.
31.	14.01.2021	Stuurgroep neemt kennis en onderkent de behoefte van het leveren van gegevens aan stakeholders direct na start van de vaccinatiecampagne. Stuurgroep gaat akkoord met een verkorte DPIA en Quickscan BIO ten behoeve van de levering van voornoemde gegevens voorafgaand aan de officiële livegang van de rapportage omgeving.
32.	04.02.2021	Clíëntbeheer wordt op de regiokantoren uitgevoerd door CIMS medewerkers die hiervoor opgeleid worden.
33.	04.02.2021	De stuurgroep is niet het gremium te besluiten over grondslag en risicoacceptatie voor COA. Het besluit moet genomen worden door het strategisch crisisberaad op 5 feb 2021.
34.	18.02.2021	zal vanuit EPI deelnemen aan stuurgroep Covid-registratie.
35.	18.02.2021	Stuurgroep accepteert de restrisico's uit het addendum DPIA en de IB risicoanalyse voor inlezen COA-en Probas-bestanden en stelt ze hierbij vast. Het Probas-convenant kan ondertekend worden.
36.	22.02.2021	Stuurgroep besluit voor optie 3 uit DPV_245 - het laten maken van een overzicht van hoe het project het beste vorm gegeven kan worden, en er voor te zorgen dat de hiervoor benodigde personen enkele uren tijd krijgen om hieraan te besteden. Zodat daarna commitment gegeven kan worden aan doorgang van het project met een aangepaste en voor het RIVM haalbare planning.
37.	04.03.2021	Stuurgroep gaat akkoord met de mitigatie van de restrisico's voor het oproepproces, maar wil weten hoe gecontroleerd kan worden of Xerox conform afspraken werkt.
38.	04.03.2021	Stuurgroep is akkoord met de vervolgacties (waarbij de nu niet aanwezige stuurgroepleden nog per mail kunnen reageren) en bevestigt de livegang van de rapportage tooling.
39.	11.03.2021	Stuurgroep besluit tot uitstel van de livegang van het cliëntportaal zodat teksten aangepast kunnen worden.
40.	18.03.2021	De Stuurgroep gaat akkoord met de wijzigingen t.b.v. de performanceproblemen CIMS.

41.	01.04.2021	De stuurgroep besluit capaciteit vrij te maken voor impactanalyse 1 prik scenario (na doorgemaakte Covid)
-----	------------	---



Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

nota

Nota nummer DPV_263
Aan Stuurgroep Covid-registratie
Van Projectmanager CIMS Cliëntenportaal ()
() en Product Owner Cliëntenportaal
()
Afgestemd met Programmamanager ()

Gevraagd besluit

De stuurgroep Covid-registratie wordt gevraagd:

- 1) Kennis te nemen van de 2 restrisico's m.b.t. het Cliëntenportaal en deze risico's voorlopig te accepteren;
- 2) De beschreven vervolgacties voor ná live gang te accorderen;
- 3) En de conclusie te ondersteunen dat er geen belemmeringen zijn, vanuit informatiebeveiliging, die een live gang van het Cliëntenportaal op 8 april in de weg staan.

Achtergrond CIMS

CIMS is het landelijk centraal registratiesysteem voor de registratie van de COVID-19 vaccinatie. Het RIVM verzorgt o.a. de centrale registratie van binnenkomende berichten van zorgverleners die de vaccinaties zetten bij personen. Naast centrale registratie wordt CIMS gebruikt voor kwaliteitsmonitoring en rapportage, het kunnen nemen van maatregelen na constateren van bijwerkingen en het doen van recalls. Met registratie wordt de vastlegging van de vaccinatie bij een persoon bedoeld.

Doel

Het CIMS Cliëntportaal geeft de burger inzage en daarmee ook regie over zijn/haar bij de overheid geregistreerde (medische) gegevens. Het RIVM voldoet hiermee aan de wettelijke taak en opdracht (wabvpz – wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, AVG – algemene verordening gegevensbescherming en UAVG – uitvoeringswet algemene verordening gegevensbescherming). De burger kan, mits toestemming verleend, voor uitwisseling tussen uitvoerder en RIVM de COVID vaccinatieregistratie gegevens inzien. Daarnaast wordt inzage verstrekt wie inzage heeft gehad in het dossier van deze burger. Ook is het mogelijk dat de burger een aanvraag indient rondom het recht van betrokkenen en het stellen van vragen.

Uitgangspunten

1. Registratie aan de bron wat doorgegeven wordt aan CIMS en één op één getoond wordt in het Cliëntenportaal.
2. De burger is verantwoordelijk voor het verkrijgen van een DigiD,
3. Inzage in het dossier wordt in CIMS geregistreerd en getoond in het Cliëntenportaal, de registratie medewerker is verantwoordelijk voor het juist vastleggen van deze gegevens.

Locatie

mijn.rivm.nl/vaccinaties

Beschrijving van de restrisico's

Hieronder de restrisico's kort benoemd, voor de volledige omschrijving en maatregelen, zie bijlage C.

- A. LAAG: BSN in Logfile Signicat
- B. LAAG: mTLS implementatie uitstellen

Volgens de mening van de FG zijn de gegevens die de externe broker verwerkt in deze context een gevoelig gegeven, omdat als gevolg van het inzageverzoek het vaccinatiegegeven af te leiden is. De FG heeft op dit punt (toegang door externe partij tot de persoonsgegevens, en met name BSN) bezwaar tegen de voorgenomen verwerking en adviseert de voorgenomen verwerking in de huidige vorm niet voort te zetten, tenzij het bezwaar is weggenomen.

Acceptatie van dit risico met een maximaal termijn van 6 maanden totdat Logius over is gestapt naar het nieuwe koppelvlak (versie 4.5) van DigiD hier is TVS alreeds op aangesloten. Op dit koppelvlak wordt het BSN encrypted doorgegeven. De tussenliggende partij kan het BSN dan niet ontsleutelen.

Advies

De geïdentificeerde restrisico's voorlopig te accepteren en de aanvullende maatregelen en vervolgacties na livegang, die worden genoemd in de risico-tabel, te accorderen.

Vervolgacties

Zie bijlage C

Verwerking privacy maatregelen

Zie bijlage D

Beheer

Het Cliëntenportaal wordt op 8 april 2021 in beheer genomen door AFM.

Bijlages

- Bijlage A: DPIA
- Bijlage A1: DPIA toelichten voor FG
- Bijlage B: IB&P-analyse

- Bijlage C: acceptatieformulier voor de restrisico's - openstaande punten /advies voor vervolg
- Bijlage D: Verwerking Privacy maatregelen

Bijslage: Schermen Cliëntenportaal

Onderstaande schermen zijn ook beschikbaar in het Engels

Home pagina

MijRIVM - vaccinaties

Als u een coronavaccinatie heeft gekregen kunt u hier vinden:

- Werk coronavaccinatie u wanneer heeft gekregen.

Let op: u vindt hier geen actuele locaties of vaccinaties die in het kader van werk of opleiding zijn gegeven. Hiervoor kunt u contact opnemen met de arts of organisatie die u de vaccinatie heeft gegeven.

Ik wil naar mijn vaccinaties

[Loggen met DigiD](#)

Service

Contact

- [Volg het RIVM op Twitter](#)
- [Volg het RIVM op Facebook](#)
- [Volg het RIVM op LinkedIn](#)
- [Volg het RIVM op YouTube](#)
- [Volg het RIVM op Instagram](#)

Over deze website

- [Cookies](#)
- [Toegankelijkheid](#)
- [NVOB-verzoeken bij het RIVM](#)
- [Copyright](#)

Meer informatie over

- [Rijksvaccinatieprogramma](#)
- [COVID vaccinatie](#)
- [Vaccinaties op maat](#)
- [Rijksvaccinatie](#)
- [Griepvaccinatie](#)

Talen

- [Engels](#)
- [Nederlands](#)

Home pagina – DigiD info

Informatie over DigiD

Inloggen met DigiD

Met DigiD laat u zien wie u bent als u op internet iets regelt. Op deze website kunt u uw vaccinatiegegevens inzien. U kunt op verschillende manieren inloggen met DigiD.

Heeft u nog geen DigiD?


Heeft u nog geen DigiD en wilt u een account aanvragen? Gebruik dan het aanvraagformulier op www.digid.nl.

DigiD is niet verplicht

Voor vragen over vaccinaties kunt u ook contact opnemen met de [Dienst Vaccinvoorziening en Preventieprogramma's](https://www.rivm.nl/rivm/organisatie/dienst-vaccinvoorziening-en-preventieprogramma-s/contactgegevens-regiokantoren-dienst-vaccinvoorziening-en-preventieprogramma-s).

<https://www.rivm.nl/rivm/organisatie/dienst-vaccinvoorziening-en-preventieprogramma-s/contactgegevens-regiokantoren-dienst-vaccinvoorziening-en-preventieprogramma-s>

Vaccinatiegegevens


Nederlands English

MijnRIVM - vaccinaties

Mijn vaccinaties
Mijn gegevens
Vragen
Contact
RIVM.nl
KG6r9g

Persoonsgegevens

Voornaam bich4	Geboortedatum 27-04-1993
Achternaam K66r9g	Geslacht Vrouw

Mijn Vaccinaties

Naam	Belicht	Datum	Fabrikant
SARS-CoV-2	CV5640K	16-12-2020	Pfizer/BioNTech

[Print](#)

Het overzicht toont de informatie die het RIVM van uw zorgverlener heeft ontvangen. Staat uw coronavaccinatie niet in het overzicht?

- Het kan enkele dagen duren voordat uw vaccinatie in het overzicht staat.
- Misschien heeft u geen toestemming gegeven om uw vaccinatiegegevens met het RIVM te delen.

Meer informatie over de mogelijkheid van de vaccinatie kunt u vinden op de [pagina over de coronavaccinatie](#) over coronavaccinatie.

De arts of GGD die u heeft gecoördineerd kan u ook meer informatie geven over uw vaccinatie.

Snel naar

- Vaccinatieplanning
- Toevoegen vaccinatie
- Inzage dossier

Gebruikte afkortingen

SARS-CoV-2 Corona virus

Service

Contact

- [Volg het RIVM op Twitter](#)
- [Volg het RIVM op Facebook](#)
- [Volg het RIVM op LinkedIn](#)
- [Volg het RIVM op YouTube](#)
- [Volg het RIVM op Instagram](#)

Over deze website

Cookies

Toegankelijkheid

WOB-verzoeken bij het RIVM

Copyright

Privacy

Uitschrijven bij MijnRIVM

Meer informatie over

Rijksvaccinatieprogramma

COVID vaccinatie

Vaccinaties op maat

Religieuze vaccinatie

Griepvaccinatie

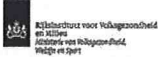
Talen

English

Nederlands

Vaccinatieplanning

NL Scenario A (geen vaccinatie gehad)


Nederlands English

MijnRIVM - vaccinaties

Mijn vaccinaties
Mijn gegevens
Vragen
Contact
RIVM.nl
Testgebruiker

Persoonsgegevens

Voornaam Development	Geboortedatum 05-04-1996
Achternaam Testgebruiker	Geslacht Man

Vaccinatieplanning

Wilt u weten wanneer u aan de beurt bent voor de coronavaccinatie? Kijk op [Rijksoverheid.nl](#).

Snel naar

- Vaccinatieplanning
- Privacy
- Inzage dossier

Service

Contact

- [Volg het RIVM op Twitter](#)
- [Volg het RIVM op Facebook](#)
- [Volg het RIVM op LinkedIn](#)
- [Volg het RIVM op YouTube](#)
- [Volg het RIVM op Instagram](#)

Over deze website

Cookies

Toegankelijkheid

WOB-verzoeken bij het RIVM

Copyright

Privacy

Uitschrijven bij MijnRIVM

Meer informatie over

Rijksvaccinatieprogramma

COVID vaccinatie

Vaccinaties op maat

Religieuze vaccinatie

Griepvaccinatie

Talen

English

Nederlands

NL Scenario B (wel vaccinatie gehad)

**Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport**

Nederlands English

MijnRIVM - vaccinaties

Mijn vaccinaties Mijn gegevens Vragen Contact RIVM.nl Testgebruiker

Persoonsgegevens

Voornaam: Development
Achternaam: Testgebruiker
Geboortedatum: 05-04-1986
Geslacht: Man

Vaccinatieplanning

U heeft al een **COVID-19 vaccinatie** gekregen. U hoort van uw arts of zorgverlener of u een tweede vaccinatie krijgt. Als u al twee vaccinaties hebt gehad, bent u volledig gevaccineerd.

Snel naar

- Vaccinatieplanning
- Privacy
- Inzage dossier

Service

- Contact
- Volg het RIVM op Twitter
- Volg het RIVM op Facebook
- Volg het RIVM op LinkedIn
- Volg het RIVM op YouTube
- Volg het RIVM op Instagram

Over deze website

- Cookies
- Toegankelijkheid
- WOB-verzoeken bij het RIVM
- Copyright
- Privacy
- Uitschrijven bij MijnRIVM

Meer informatie over

- Rijksvaccinatieprogramma
- COVID vaccinatie
- Vaccinaties op maat
- Reizigersvaccinatie
- Griepvaccinatie

Talen

- English
- Nederlands

Privacy pagina
NL

**Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport**

Nederlands English

MijnRIVM - vaccinaties

Mijn vaccinaties Mijn gegevens Vragen Contact RIVM.nl Testgebruiker

Privacy

Wilt u meer weten over hoe het RIVM uw gegevens verwerkt en wat dit voor u betekent? Lees dan onze [Privacy Verklaring](#).

Snel naar

- Vaccinatieplanning
- Privacy
- Inzage dossier

Service

- Contact
- Volg het RIVM op Twitter
- Volg het RIVM op Facebook
- Volg het RIVM op LinkedIn
- Volg het RIVM op YouTube
- Volg het RIVM op Instagram

Over deze website

- Cookies
- Toegankelijkheid
- WOB-verzoeken bij het RIVM
- Copyright
- Privacy
- Uitschrijven bij MijnRIVM


Meer informatie over

- Rijksvaccinatieprogramma
- COVID vaccinatie
- Vaccinaties op maat
- Reizigersvaccinatie
- Griepvaccinatie

Talen

- English
- Nederlands

Inzage dossier


Rijksoverheid voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Wetgeving en Sport

Nederlands English

MijnRIVM - vaccinaties

Mijn vaccinaties Mijn gegevens Vragen Contact RIVM.nl

Testgebruiker

Inzage dossier

Uw vaccinatiegegevens zijn strikt vertrouwelijk. Een zorgverlener mag uw gegevens alleen inzien als daar een medische reden voor is.

Overzicht inzage dossier

Bekijk hier welke externe zorgverlener informatie over uw dossier heeft ontvangen.

Datum informatieverzoek		09-02-2021	
Verwerker	Medewerker	Aanvrager	Client zelf
Soort	Ontvangen	Informatie	Schriftelijk
Informatieverzoek	vaccinatiepapieren	verstuurd per	

Snel naar

- Vaccinatieplanning
- Toevoegen vaccinatie
- Inzage dossier

Service

- Contact
- Volg het RIVM op Twitter
- Volg het RIVM op Facebook
- Volg het RIVM op LinkedIn
- Volg het RIVM op YouTube
- Volg het RIVM op Instagram

Over deze website

- Cookies
- Toegankelijkheid
- WOB-verzoeken bij het RIVM
- Copyright

Meer informatie over

- Rijksvaccinatieprogramma
- COVID vaccinatie
- Vaccinaties op maat
- Reizigersvaccinatie
- Griepvrij

Talen

- English
- Nederlands

Vragen


Rijksoverheid voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Wetgeving en Sport

Nederlands English

MijnRIVM - vaccinaties

Mijn vaccinaties Mijn gegevens Vragen Contact RIVM.nl

Kids-9q

Vragen

Waar gebeurt er met mijn gegevens?

Waarom staat mijn coronavaccinatie niet in mijn overzicht?

Er zijn 3 mogelijke redenen:

- Het kan enkele dagen duren voordat uw vaccinatie in het overzicht staat.
- Misschien heeft u geen toestemming gegeven om uw vaccinatiegegevens met het RIVM te delen.
- Misschien heeft u zich eerder laten uitschrijven uit de registratie.

Wilt u meer informatie over uw vaccinatie? Neem dan contact op met de arts of GGD waar u de vaccinatie heeft gekregen.

Wilt u MijnRIVM - vaccinaties?

Hoe werkt MijnRIVM - vaccinaties?

Hoe kan ik mij uitschrijven uit MijnRIVM - Vaccinaties?

Ik heb een uitzondering van een onderzoek ontvangen. Waarom is dat?

Snel naar

- Vaccinatieplanning
- Toevoegen vaccinatie
- Inzage dossier

Service

- Contact
- Volg het RIVM op Twitter
- Volg het RIVM op Facebook
- Volg het RIVM op LinkedIn
- Volg het RIVM op YouTube
- Volg het RIVM op Instagram

Over deze website

- Cookies
- Toegankelijkheid
- WOB-verzoeken bij het RIVM
- Copyright

Meer informatie over

- Rijksvaccinatieprogramma
- COVID vaccinatie
- Vaccinaties op maat
- Reizigersvaccinatie
- Griepvrij

Talen

- English
- Nederlands

Uitschrijfpagina

Nederlands English

MijnRIVM - vaccinaties
Mijn vaccinaties Mij gegevens Vragen Contact RIVM.nl Klér +00

Uitschrijven registratie MijnRIVM

Als u het niet prettig vindt dat uw coronavaccinatiegegevens bij het RIVM bekend zijn, dan kunt u ervoor kiezen u uit te schrijven uit MijnRIVM.

De gevolgen van uitschrijven bij MijnRIVM:

- Het RIVM kan u dan geen inzage geven in uw vaccinatiegegevens.
- Het RIVM kan u niet berademen als u een probleem met een vaccin blijkt te zijn.

Wilt u zich laten uitschrijven? Stuur een email door op de knop te drukken.

[E-mail sturen](#)

Snel naar
[Vaccinatieplanning](#)
[Toevoegen vaccinatie](#)
[Inzage dossier](#)

Service
Contact
[Volg het RIVM op Twitter](#)
[Volg het RIVM op Facebook](#)
[Volg het RIVM op LinkedIn](#)
[Volg het RIVM op YouTube](#)
[Volg het RIVM op Instagram](#)

Over deze website
Cookies
[Burgersiteheld](#)
[Nieuw vaccineren bij het RIVM](#)
Copyright

Meer informatie over
[Rijksvaccinatieprogramma](#)
[COVID vaccinatie](#)
[Vaccinaties op maat](#)
[Reizigersvaccinatie](#)
[Griepvaccinatie](#)

Talen
English
Nederlands

STUK UIT BIJLAGE C: Verwerking rechten van betrokkenen

mTLS implementatie uitstellen tot later moment.

Deze sprint van 5 maart 2021 staat voor het Clientenportaal op de planning om mTLS te implementeren tussen de API Gateway en de Clientenportaal API. Gezien de tijdsdruk het verzoek mTLS nog niet in te voeren.

Zie NUANCE: NUANCE: Om de API van het Clientenportaal direct vanaf het interne netwerk aan te roepen heeft de aanroeper wel een geldig id_token nodig. Deze hebben we nodig om de burger te identificeren. Dit is impliciet een extra beveiligingsmaatregel voor het Clientenportaal, waardoor het risico een stuk minder makkelijk te exploiteren is. Echter lijkt het mij wel goed om vast te houden aan de oplossing hierboven beschreven, ook met oog op API's in de toekomst die deze extra functionaliteit niet nodig hebben (en dus niet zullen implementeren).

RISICO ACCEPTATIE met nuance. Actie
[REDACTED]/[REDACTED]: [REDACTED] en [REDACTED] leggen Risico
Acceptatie voor

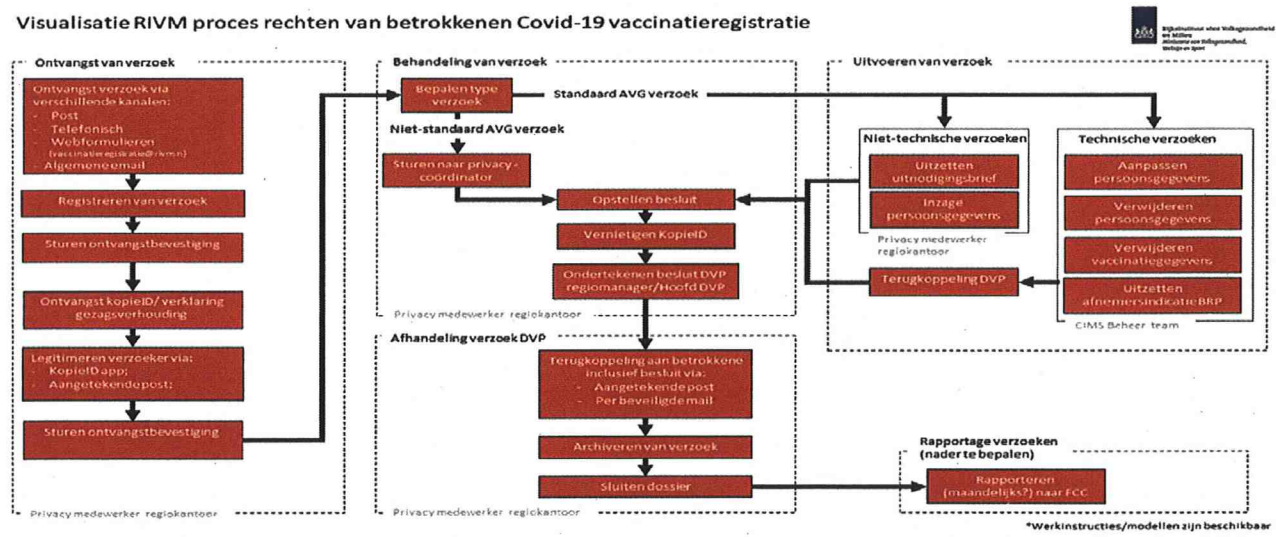
SIGNICAT slaat logfiles met encrypted BSN-nummer op voor fraude-analyse.

MITIGERING: BSN nummer niet langer opslaan in Logfiles dan dat de sessie duurt;
RIVM logfiles laten opslaan;
Signicat geen logfiles laten opslaan langer dan dat de sessie duurt. 20210315AHAN: deze wordt nu opgelost, BSN verwijderen uit logfile, want showstopper voor CP.
20210323: DPIA en RisicoAcceptatie door privacyfunctionaris.
20210329AHAN: update [REDACTED]: Om hier op te antwoorden, ik heb mij - zoals aangegeven door [REDACTED] - vooral gefocust op het privacy risico zoals aangegeven door de FG in haar advies (BSN nummer door Signicat). Het risico acceptatie formulier is klaar maar dient nog met de laatste update vanuit Signicat aangepast te worden.
(@ [REDACTED]: dit is besproken tijdens onze meeting op vrijdag ik hoop dat ze dit voor woensdag gaan terugkoppelen?). Dan is het klaar om ondertekend te worden en de vraag is door wie. Ik hoop dat dit [REDACTED] is en zal hem hier over vandaag updaten. Ik ga ervan uit dat we alles op woensdag dan klaar kunnen hebben, ik hou jullie hiervan op de hoogte!

Conclusie: DPIA en RISICO ACCEPTATIE (LAAG, bijna gereed voor acceptatie)
20210330AHAN: Dit is een RIVMToegang risico.

BIJLAGE D: Verwerking rechten van betrokkenen

Visualisatie RIVM proces rechten van betrokkenen Covid-19 vaccinatieregistratie





Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

nota

Betreft	Ontwikkelingen m.b.t. Mijn.RIVM.nl
Nota nummer	DPV_278
Contactpersonen	[REDACTED], [REDACTED]
Besluit	Ja

Doel

De stuurgroep Covidvaccinatieregistratie wordt gevraagd kennis te nemen van ontwikkelingen m.b.t. Mijn.RIVM.nl en vervolgens in te stemmen met voorgestelde maatregelen.

Aanleiding

Het Mijn.RIVM.nl is op 6 april 2021 live gegaan. Na op 4 april 2021 te hebben besloten om live te gaan hebben een aantal ontwikkelingen plaatsgevonden:

- Na livegang zijn er vragen van burgers ontvangen. In Bijlage 1 is een overzicht van de vragen gegeven. Ook zijn vorige week tijdens het Kamerdebat opmerkingen gemaakt door de partij BBB die in lijn liggen met de vragen in de bijlage en heeft de Minister toegezegd beter en meer te zullen communiceren over Mijn.RIVM.nl en het gebruik van o.a. BRP-gegevens door RIVM. Deze vragen gecombineerd leiden mogelijk tot een heroverweging van hetgeen getoond wordt op Mijn.RIVM.nl.
- In de periode 22 april 2021-heden zijn ruim 60.000 AVG-verzoeken binnen gekomen via e-mails en ingevulde webformulieren. De verzoeken zijn veroorzaakt door acties op sociale media. In Bijlage 2 is een overzicht van het type verzoeken gegeven. Ook worden voorstellen voor vervolgacties gedaan.
- Onderzoek naar feiten (fact check) is gestart. Zie bijlage 3.

De ontstane vragen en de verzoeken geven aanleiding tot extra maatregelen in 5 categorieën.

Gevraagd besluit

De Stuurgroep wordt gevraagd akkoord te geven op onderstaande maatregelen of desgewenst richting te geven aan andere maatregelen:

T.a.v. Mijn.RIVM.nl:

1. Maak onderscheid tussen verwerken van data in CIMS en tonen van data in cliëntenportaal.
2. Toon alléén vaccinatiedata¹ in het cliëntenportaal, dus géén BRP-gegevens. De cliënt ziet alléén de data waarvoor expliciet toestemming is gegeven. Ook de persoonsnaam? En wat te zien als meerdere personen dezelfde naam hebben?
3. Verwerk dataverzoek van de cliënt specifiek gericht op de CIMS-database (dus de BRP-data) via de normale procedure (AVG-team DVP en FCC) en niet via Mijn.RIVM.nl.
4. Implementeer als volgt:
 - a. De burger logt in op Mijn.RIVM.nl gebruikmakend van DigiD;
 - b. Na inloggen ziet de burger dan een korte welkomboodschap zoals "welkom meneer/ mevrouw ..." waarbij dus alleen de naam wordt getoond (dataminimalisatie);
 - c. Vervolgens wordt dan een aantal opties geboden om de AVG-rechten uit te oefenen; inzage, verwijdering, correctie etc. (keuze voor welk recht).
 - d. Indien gevaccineerd en toestemming gegeven is, dan zien mensen hun vaccinatiegegevens.
 - e. Pas de privacyverklaring en gerelateerde webpagina's hier op aan.

T.a.v. gebruik BSN in Signicat-verkeer:

1. Kennis nemen van advies van privacy team om geen gebruik te maken logging o.b.v. BSN.

T.a.v. de AVG-verzoeken:

1. Akkoord geven op de voorgestelde acties en oplossingsrichting.

T.a.v. communicatie:

1. Akkoord te gaan met het communicatiebericht in Bijlage 4.

Nadere toelichting per categorie

1. Privacy en Mijn.RIVM.nl

Er zijn grofweg twee verschillende visies binnen het RIVM:

1. **Visie 1 (grofweg):** "we tonen de persoonsgegevens uit de BRP op Mijn.RIVM.nl om burgers inzage te geven in wat het RIVM van ze weet, en tegelijkertijd geeft het ook vertrouwen zodat je weet dat jouw vaccinatiegegevens aan de juiste persoon gekoppeld zijn."

Deze visie is begrijpelijk, echter de argumentatie is problematisch. Het RIVM deelt op dit moment niet alle BRP-data die wij over een burger hebben op Mijn.RIVM.nl. Zo laten wij bijvoorbeeld geen adresgegevens zien, hoewel wij die wel bezitten. Als we, zoals voorgesteld wordt, besluiten om alleen maar vaccinatiedata te laten zien dan tonen we

¹ Vaccinatiedata: datum van vaccinatie, naam en batchnummer van het vaccin

dus ook niet alle persoonsgegevens maar alleen maar die data waarvoor door de burger expliciete toestemming is gegeven. Dit verhoogt het vertrouwen omdat je alleen die data terug ziet waar je expliciete toestemming hebt gegeven. Bovendien kan het inloggen van een burger *an sich* niet gezien worden als een verzoek tot inzage in gegevens. Het reguliere, ingerichte AVG-proces (met webformulieren) voorziet in deze behoefte.

2. **Visie 2 (grofweg):** *"hoewel er een grondslag is voor het verwerken en tonen van de persoonsgegevens uit de BRP vanuit CIMS (die in CIMS staan t.b.v. uitnodigen) op Mijn.RIVM.nl, is het onwenselijk dat te doen alvorens mensen gevaccineerd zijn en alvorens zij (bijv.) een (AVG-)verzoek tot inzage gedaan hebben – Mijn.RIVM.nl moet derhalve aangepast worden."*

Hier worden twee verwerkingen door elkaar genoemd:

1. Verwerken van data in CIMS; de grondslag hiervoor is al nader toegelicht in de DPIA CIMS release 1.0. van december 2020. Grofweg komt het er op neer dat dit is geregeld in het Autorisatiebesluit van 19 november 2020. RIVM is daarmee in staat gesteld de noodzakelijke voorbereidingen te treffen in het kader van het vaccinatieprogramma voor COVID-19 (voor nadere informatie: zie betreffende DPIA).
2. Het tonen van data in het Cliëntenportaal; de grondslag hiervoor is zoals beschreven in de DPIA Cliëntenportaal versie 1.0: het Cliëntenportaal voorziet in het recht op inzage zoals is geregeld in de AVG, artikel 12 lid 2: "de verwerkingsverantwoordelijke faciliteert de uitoefening van de rechten van de betrokkene..."

Voorgestelde oplossing

Vanwege de privacyvragen wordt om in Mijn.RIVM.nl alleen maar vaccinatiedata te tonen en niet de andere (BRP-data) die ook in CIMS voorkomen. Hiermee worden in één klap een hoop onduidelijkheden weggenomen en vindt men in Mijn.RIVM.nl alleen de data terug waarvoor men ook daadwerkelijk expliciete toestemming heeft gegeven.

Een data-/ AVG-verzoek welke niet specifiek gericht is op de CIMS-database (dus de BRP-data) zou dan via de normale procedure (AVG-team DVP en FCC) kunnen gaan en niet via Mijn.RIVM.nl. Hiervoor zou het proces rechten van betrokkenen gedeeltelijk moeten worden herzien.

De voorgestelde oplossing leidt dan tot een getrapte manier van inloggen:

1. De burger logt in op het Cliëntenportaal gebruikmakend van DigiD;
2. Na inloggen ziet de burger dan een korte welkomboodschap zoals "welkom meneer/ mevrouw ..." waarbij dus alleen de naam wordt getoond (dataminimalisatie);
3. Vervolgens kan er dan een aantal opties geboden om de AVG-rechten uit te oefenen; inzage, verwijdering, correctie etc. (keuze voor welk recht) waarna naar de Formdesk-formulieren verwezen wordt.

Het is in dat geval niet nodig om in een pop-up helder te maken waarom er geen data zichtbaar is als er geen data-aanlevering heeft plaatsgevonden. Dit geldt ook voor cliënten onder de 18 jaar, die op dit moment in Nederland sowieso niet gevaccineerd worden.

Extra maatregelen:

1. Aanpassing van de DPIA MijnRIVM.nl als we kiezen voor de voorgestelde oplossing;
2. Aanpassing van de privacyverklaring als we kiezen voor de voorgestelde oplossing;
3. FG informeren over deze wijziging en de aangepaste DPIA sturen ter informatie (alleen als dit ook álle aanpassingen zijn!).

2. Functioneel

Implementeer de getrapte manier van inloggen, zoals beschreven onder de voorgestelde oplossing.

3. Informatiebeveiliging

Signicat heeft een standaard audittrail aangelegd waarmee het mogelijk is om geautomatiseerd de route van geautoriseerde toegang van DigiD naar MijnRIVM.nl te volgen. In het versleutelde messagelog van de audittrail staan BSN's van de toegestane inlogpogingen. Dit versleutelde log is noodzakelijk voor eventueel forensisch onderzoek bij vermoeden van misbruik van DigiD/identiteitsfraude. Voor een dergelijk onderzoek wil je de hele autorisatie-keten in kaart hebben.

De verantwoordelijken bij het RIVM zijn na uitvoerige afweging a.d.h.v. de risicoacceptatie ermee akkoord gegaan dat het stoppen van de verwerking van het BSN door Signicat 6 maanden in beslag neemt. FG VWS en privacy jurist RIVM hebben ná livegang opgemerkt dat het messagelog in deze vorm een verwerking is van BSN waar geen juridische grondslag voor is. Hierdoor is de audittrail niet in overeenstemming is met de AVG².

Het privacy team van RIVM adviseert om deze verwerking te stoppen. Vanwege het ontbreken van de juiste grondslag (nieuw inzicht op basis van juridische analyse) hierdoor neigt dit naar oneigenlijk gebruik van het BSN. Tenzij er vanuit security een duidelijke grondslag hiervoor te formuleren is, kunnen z/wij het niet verklaren aan de FG van VWS.

Het risico van stopzetten van logging met BSN betekent dat achteraf geen onderzoek kan plaatsvinden naar eventuele BSN-fraude. Signicat past dezelfde manier van logging overigens binnen de Rijksoverheid breed toe. Hieruit zou kunnen worden afgeleid dat het een gangbare implementatie en manier van handelen betreft.

Extra maatregelen:

² Juristen van Signicat hebben gesteld dat het audittrail wél in overeenstemming is met de AVG.

1. Geen. Oplossing risico afhandelen conform DPV_263D
Cliëntenportaal risico-acceptatie.

4. Verwerken individuele verzoeken

Er zijn ruim 60.000 mails binnengekomen met AVG-verzoeken (peildatum 8 mei 2021). Ruim de helft hiervan betreffen AVG webformulieren voor de rechten van betrokkenen. Al deze formulieren worden op het moment van schrijven geladen in Topdesk en zullen conform de vastgestelde procedures verwerkt, gemonitord en afgehandeld gaan worden. De overige 30.000 mails zijn ingedeeld in 10 categorieën (zie Excel bestand 'Status en voorstel afhandelen AVG verzoeken'). Voor elke categorie is een afhandeling voorgesteld, waarbij op korte termijn een eerste reactie naar de afzenders gestuurd zal worden.

Aandachtspunten:

- We kunnen niet lang meer wachten (uiterlijk tot en met zondag 23 mei 2021) met "opschorten" (omdat we de AVG-termijn van één maand niet gaan halen en daarom in totaal drie maanden nodig hebben). Er moet in de mails opgenomen worden dat de behandeling van de verzoeken langer dan 1 maand gaat duren.
- De groep van ca. 22.000 mails type 1, waaronder lege mails en korte verzoeken als "Schrijf mij uit", etc. willen we beantwoorden met een standaard mail (zie Excel bestand 'Status en voorstel afhandelen AVG verzoeken', tabblad 3 en 4) waarin we de afzenders vragen om alsnog het juiste webformulier in te vullen. De vraag hierbij is: als we hen dit retourbericht gaan sturen, kunnen we hun oorspronkelijke verzoek dan als afgehandeld beschouwen, of niet?
- Er moet een team samengesteld worden dat de afhandeling kan verzorgen. De stuurgroep wordt gevraagd akkoord te gaan met het voorstel in Excel bestand 'Status en voorstel afhandelen AVG verzoeken', tabblad 5.

5. Publiekscommunicatie

De minister heeft bij een Kamervraag op 6 mei 2021 aangegeven dat RIVM in publiekscommunicatie (nog) meer gaat aangeven waarom persoonsgegevens worden verwerkt, wat de persoonsgegevens zijn, hoe de verwerking gebeurt en welke rechten betrokkenen hebben.

Het RIVM mag persoonsgegevens gebruiken als onderdeel van hun wettelijke taak om de coronavaccinatie te monitoren en te coördineren, deze gegevens zijn bijvoorbeeld nodig om mensen uit te kunnen nodigen voor de vaccinatie. De persoonsgegevens ontvangt het RIVM uit de Basis Registratie Personen (BRP). De pagina Mijn.RIVM.nl geeft (op dit moment) aan de burger inzage in (een deel van) de BRP gegevens die het RIVM van hen heeft, zoals naam en geboortedatum.

De ontvangst van deze persoonsgegevens door het RIVM vanuit de BRP staat los van de toestemming die mensen moeten geven om

vaccinatiegegevens aan het RIVM (vanuit een andere bron) door te geven. De vaccinatiegegevens, medische gegevens, zullen alleen te zien zijn op deze pagina als de betreffende persoon toestemming heeft gegeven om deze gegevens te delen met het RIVM. Als je nog niet gevaccineerd bent, of je hebt geen toestemming gegeven om je gegevens te delen met het RIVM zal hier staan dat er geen vaccinaties gevonden zijn. Er staat niet dat u niet gevaccineerd bent. Zo heeft de burger op de Mijn.RIVM.nl pagina's inzage in hun eigen gegevens waarover het RIVM beschikt.

De toon op sociale media is ongenueanceerd en geschreven media (o.a. AD) beginnen interesse te tonen in het onderwerp. Ook de FG van VWS waarschuwt voor escalatie, en ontvangt boze e-mails van burgers, bijvoorbeeld over de vraag waarom zij nog geen reactie van RIVM hebben gehad op hun verzoek.

Samen met Communicatie RIVM is gewerkt aan beantwoording van vragen n.a.v. een verzoek van een fact check bureau (zie bijlage 3). Daarnaast is op vrijdag 7 mei 2021 aan communicatie RIVM gevraagd om te werken aan een bericht dat mogelijk gebruikt kan worden voor proactieve communicatie. Hier wordt aan gewerkt (zie bijlage 4 voor concept).

Stel we besluiten tot de voorgestelde functionele wijziging van MijnRIVM.nl, hoe leggen we dat dan uit aan het publiek? En hoe stemmen we dit af met min. VWS?

Extra maatregelen:

1. Persbericht (zie bijlage 4)
2. Ingezonden artikel in dagbladen?
3. Uit te zoeken: Hoe leggen we de eventuele functionele wijzigingen op Mijn. RIVM.nl uit aan het publiek?

Bijlage 1: Veel gestelde vragen na lancering MijnRIVM.nl

1. Waarom heeft RIVM een registratie met alle burgers van Nederland. Wat is hiervoor de wettelijke grondslag?
2. Hoe/waar kan ik mijn in het buitenland ontvangen vaccinatie(s) laten registreren?
3. Ik ben gevaccineerd maar mijn vaccinaties zijn niet te zien in Mijn.RIVM (heb toestemming gegeven).
4. Ik ben gevaccineerd, heb geweigerd mijn gegevens te delen met het RIVM, hoe kan ik dit wijzigen zodat mijn gegevens alsnog gedeeld worden?
5. De vaccinaties in Mijn.RIVM kloppen niet.
6. De vaccinaties in Mijn.RIVM kloppen niet, hierbij kopie/bewijs dat ik een ander vaccin heb gekregen/andere prikdatum geweest, met verzoek deze te verwerken.
7. U geeft aan dat het enkele weken duurt voordat ik mijn vaccinaties te zien krijg in Mijn.RIVM, maar mijn vaccinaties zijn al maanden geleden gegeven.
8. Ik ben gevaccineerd en heb een 2-3-4 dubbele uitnodiging ontvangen, uw administratie klopt niet, hierbij stuur ik de juiste gegevens en met verzoek deze te corrigeren.
9. Over welke persoonsgegevens beschikt RIVM?
10. Waarom worden mijn persoonsgegevens al getoond in het clientportaal terwijl ik nog niet ben gevaccineerd?
11. Waarom wordt door RIVM gewerkt met mijn BSN? Grondslag?
12. Heeft elke Nederlander automatisch een mijn-RIVM pagina? En zo ja, is dat specifiek voor de coronavaccinatie of hadden we deze altijd al?
13. Klopt het dat de informatie alleen op verzoek van bv. Lareb wordt gedeeld (en dus niet zomaar met 'derden')?

Bijlage 2: Status mailbox vaccinatieregistratie@rivm.nl op 08-05-2021

Omschrijving	Aantal	Toelichting	Eerste actie
Afzien van deelname	7613	ingevuld formdeskformulier	Laden in Topdesk
Recht op beperking	171	ingevuld formdeskformulier	Laden in Topdesk
Recht op inzage	179	ingevuld formdeskformulier	Laden in Topdesk
Recht op rectificatie	142	ingevuld formdeskformulier	Laden in Topdesk
Recht op vergetelheid	13274	ingevuld formdeskformulier	Laden in Topdesk
Recht van bezwaar	9484	ingevuld formdeskformulier	Laden in Topdesk
Verzoek tot uitschrijven	21870	Mails waarin gevraagd wordt de gegevens uit ons systeem te halen. Dit zijn voornamelijk de mails die binnengekomen zijn via 'de knop' binnen het clientportaal. Veel korte en deels lege mails. Bevatten géén ID bewijzen.	Z.s.m. een mail sturen waarin we: - Uitleg geven over de reden dat wij de gegevens hebben - Link naar de privacy verklaring en de pagina rechten van betrokkenen - Indien men alsnog besluit gebruik te maken van de rechten van betrokkenen dan verzoeken tot het invullen van het juiste formulier - Verwachtingsmanagement tijdsduur afhandeling meegegeven - Mails hierna verwijderen???
ID bewijzen	6220	Mails met ID bewijzen in de bijlage of als foto in de mail zelf. De meeste hiervan zijn een reactie op de reply mail die men heeft ontvangen op het ingevulde webformulier. Ook zijn er een aantal mails met een ID met de vraag om uitgeschreven te worden.	Onderzoeken of het mogelijk is de mails in Topdesk te laden en automatisch te koppelen aan het juiste dossier. Z.s.m. een mail sturen waarin we aangeven: - Het ID bewijs in goede orde ontvangen te hebben - Indien er reeds een formulier is ingevuld we het verzoek in behandeling gaan nemen - Indien alleen het ID gestuurd is dat er dan ook een officieel verzoek via een webformulier ingevuld moet worden - Verwachtingsmanagement tijdsduur afhandeling meegeven
Vragen	37	Diverse vragen.	Doornemen en waar mogelijk afhandelen.
Meerdere webformulieren ingediend	61	Een aantal mensen hebben domweg alle formulieren ingevuld.	Ik heb deze in een apart mapje gezet in verband met het koppelen van het ID. ID z.s.m. toevoegen aan formulieren in Topdesk.
Recht op vergetelheid	3	Handmatig ingevuld webformulier met ID.	Laden in Topdesk
Recht van bezwaar	1	Handmatig ingevuld webformulier met ID.	Laden in Topdesk
Weigering aanleveren ID	116	Als reactie op de reply van de webformulieren, waar gevraagd wordt om een ID op te sturen, geven deze mensen aan géén ID op te gaan sturen.	Z.s.m. een mail sturen. Hier moet een standaard mail voor ontwikkeld worden. Wat is het beleid hierin? Wel of niet in behandeling nemen?
Zonder bijlage	73	In deze mails geeft men aan het ID op te sturen, maar de bijlage ontbreekt.	Ik denk dat we hier nog even niets mee moeten doen. Deze mails zijn gestuurd al antwoord op de reply van een webformulier. Bij de afhandeling van de formulieren in Topdesk gaan we alsnog een ID opvragen als dit ontbreekt.
Reactie op bevestiging AVG verzoek	32	Diverse reacties op de reply van de webformuliere.	Doornemen en waar mogelijk afhandelen.
Mails binnengekomen via het AVG team	304	Deze mails zijn door het AVG team naar deze mailbox doorgestuurd. Moeten verder uitgezocht worden.	Doornemen en waar mogelijk afhandelen. Lastig om mee te nemen in uit te sturen bulk mails, omdat ze dan bij het AVG team terecht komen.
	701	Out of the office replies, undeliverable en dubbele mails aangeleverd.	Definitief verwijderen
	60281		

Bijlage 3: Factchecker

- Heeft elke Nederlander automatisch een Mijn.RIVM-pagina? En zo ja, is dat specifiek voor de coronavaccinatie of hadden we deze altijd al?

Het RIVM heeft een clientportaal ("Mijn.RIVM.nl") opgezet voor alle Nederlandse burgers. Iedereen met een DigiD kan inloggen bij het clientportaal. Zoals men dat ook kan doen bij andere overheidsinstanties in Nederland zoals de Belastingdienst of de zorgverzekeraar.

De eerste versie van het cliëntportaal staat vanaf begin april 2021 online. De gegevens die worden ontsloten zijn de vaccinatieregistratiegegevens van het vaccinatieprogramma COVID-19. Registratie van individuele vaccinatiegegevens in het landelijke registratiesysteem (CIMS) van het RIVM vindt alleen plaats als daar expliciet toestemming voor gegeven is. Iedereen in Nederland kan dus zijn coronavaccinatiegegevens inzien, mits zij toestemming hebben gegeven aan hun zorgverlener voor de registratie van hun vaccinatiegegevens.

Het is de bedoeling dat er in de toekomst ook andere vaccinatiegegevens van Nederlanders en/of hun kind te zien zijn via het clientportaal. Denk daarbij aan vaccinaties die gezet zijn in het kader van het Rijksvaccinatieprogramma. Over andere toepassingen van het clientportaal wordt nagedacht binnen het RIVM.

- Wordt er van tevoren toestemming gevraagd een Mijn.RIVM-pagina te maken? Of wordt er alleen toestemming gevraagd om daar de gegevens over de coronavaccinatie in te zetten?

Om gegevens van individuen te kunnen koppelen aan de juiste vaccinatieregistratiegegevens gebruikt het RIVM persoonsgegevens uit de basisregistratie personen (BRP). Dit betreft o.a. de namen en geboortedata van alle Nederlanders. Het RIVM heeft voor het gebruik van deze gegevens een wettelijke grondslag³. Voor het gebruiken van deze persoonsgegevens door het RIVM is dan ook geen expliciete persoonlijke toestemming vooraf vereist. Iedereen met een DigiD kan dus kijken of en welke gegevens geregistreerd zijn.

Voor het doorgeven van vaccinatiegegevens m.b.t. COVID-19 van de zorgverlener aan het RIVM is altijd expliciete toestemming vereist van de gevaccineerde in kwestie. Voor mensen die geen toestemming hebben gegeven zal het systeem laten zien dat er geen gegevens over de

³ De 'gewone' persoonsgegevens (NAW, geboortedatum, geslacht, etc., maar ook het BSN) worden door het RIVM, daartoe geautoriseerd door het ministerie BZK, verkregen uit de Basisregistratie Personen (BRP). De grondslag voor de verweking van deze 'gewone' persoonsgegevens is 'uitvoering van een taak van algemeen belang', AVG art. 6, lid 1e. In de BRP-autorisatie wordt verwezen naar art. 3 van de Wet op het RIVM waarin de taken van het RIVM op hoofdlijnen zijn geformuleerd.

vaccinatie zijn geregistreerd. Daarnaast kunnen mensen die in eerste instantie toestemming hebben gegeven, hun gegevens altijd laten verwijderen via mijn.rivm.nl. Deze mogelijkheid is wettelijk vastgelegd in de wet AVG.

- Klopt het dat de informatie alleen op verzoek van bv. Lareb wordt gedeeld (en dus niet zomaar met 'derden')?

De persoonlijke gegevens van individuen in het cliëntenportaal worden niet met derden gedeeld en zijn ook niet door derden te raadplegen.

De gegevens die mensen in kunnen zien op het clientportaal komen uit het landelijk vaccinatieregistratiesysteem (CIMS). Uit deze achterliggende database kan het RIVM gegevens delen met bijwerkingencentrum Lareb. Het Lareb gebruikt deze gegevens voor de monitoring van bijwerkingen na vaccinatie tegen COVID-19. De geanonimiseerde gegevens uit CIMS kunnen ook gebruikt worden voor onderzoek.

Hiermee geeft het RIVM invulling aan haar wettelijke taak om de volksgezondheid van Nederlanders te beschermen.

Bijwerkingen:

Zowel burgers als zorgverleners kunnen bijwerkingen melden bij het Lareb. Bij de melding worden gevraagd om aan te geven met welk vaccin en batchnummer zij zijn gevaccineerd is. Vervolgens doet het Lareb verder onderzoek. Op het moment dat het batchnummer ontbreekt, vraagt Lareb de gegevens op bij het RIVM. Het RIVM zoekt hierna in CIMS het juiste batchnummer en deelt deze informatie met het Lareb. Het opvragen van missende batchnummers vanuit Lareb gebeurt alleen als mensen bij Lareb daar ook expliciet toestemming voor hebben gegeven.

Voor mensen die geen toestemming hebben gegeven zal het systeem laten zien dat er geen gegevens over de vaccinatie zijn geregistreerd. Voor deze mensen kan het RIVM dan ook geen gegevens doorgeven aan het Lareb. Het kan voorkomen dat iemand wel toestemming heeft verleend voor de registratie van vaccinatiegegevens, maar dat de gegevens nog niet bij het RIVM zijn ontvangen. In dat geval kan het RIVM ook nog geen gegevens verstrekken.

Het RIVM registreert alle dataverzoeken van het Lareb op persoonsniveau, of er nu een vaccinatie is gevonden of niet. Ook dit is te zien in het cliëntportaal.

Functionaliteit CIMS

Met CIMS houdt het RIVM gegevens over de COVID-19-vaccinatie bij die belangrijk zijn om de epidemie te bestrijden. Denk naast de vaccinatiegraad ook aan de effectiviteit van het vaccinatieprogramma.

CIMS is bijvoorbeeld ook van belang om het risico op zeldzame bijwerkingen te kunnen berekenen, zoals nu voor het vaccin van AstraZeneca. Op basis van uitgeleverde vaccins kunnen we niet bepalen hoeveel mannen en vrouwen van een bepaalde leeftijd een bepaald vaccin

heeft gekregen. Dat zou je uit willen zetten tegen het aantal mannen en vrouwen van een bepaalde leeftijd die een bepaalde bijwerking heeft gehad om de kans op een bijwerking zo goed mogelijk te bepalen naar leeftijd en geslacht.

Bijlage 4: Communicatiebericht Mijn.RIVM.nl

Vaccinatiegegevens COVID-19 na toestemming op Mijn.RIVM

Iedereen die toestemming heeft gegeven voor het delen van vaccinatiegegevens met het RIVM, kan deze bekijken via mijn.rivm.nl. Via deze website kunnen mensen met hun DigiD de vaccinatiegegevens die het RIVM van hen heeft, zien. Iedereen kan dus zijn of haar gegevens over de ontvangen coronavaccinatie(s) terugvinden, wanneer er toestemming is gegeven voor het registreren van die vaccinatiegegevens. De eerste versie van Mijn.RIVM staat sinds begin april 2021 online.

Mijn.RIVM laat alleen vaccinatiegegevens COVID-19 zien van Nederlanders die uitdrukkelijk toestemming hebben gegeven om deze gegevens te delen met het RIVM. Na toestemming geeft de organisatie (o.a. GGD, instelling, ziekenhuis of de huisarts) die de vaccinatie geeft, gegevens over de vaccinatie door aan het RIVM. Na verwerking staan de vaccinatiegegevens in een persoonlijk vaccinatieoverzicht. Dit overzicht is geen officieel vaccinatiebewijs. Wel kunnen mensen de informatie uit mijn.rivm.nl in de toekomst gebruiken om een bewijs aan te vragen. Voor mensen die geen toestemming hebben gegeven, laat Mijn.RIVM zien dat er geen gegevens over de vaccinatie zijn.

Geen vaccinatie of geen toestemming, toch gegevens

Om gegevens van individuen te koppelen aan de vaccinatieregistratiegegevens gebruikt het RIVM persoonsgegevens uit de Basisregistratie Personen (BRP). Dit gaat om o.a. de namen en geboortedata van Nederlanders. Het RIVM heeft deze gegevens nodig voor de uitvoering van het vaccinatieprogramma, bijvoorbeeld om mensen een uitnodiging te sturen. Er is voor het gebruik van deze gegevens een wettelijke grondslag. Mensen die nog geen vaccinatie hebben ontvangen en aan wie dus ook nog geen toestemming is gevraagd, hebben ook al toegang tot Mijn.RIVM. Deze mensen vinden op mijn.rivm.nl op dit moment alleen hun persoonsgegevens terug.

Wat doet het RIVM met de gegevens?

De landelijke registratie van vaccinatiegegevens is belangrijk. Het RIVM gebruikt de informatie over de coronavaccinatie voor onderzoek om te kijken of de vaccins goed werken, eventuele bijsturing van de vaccinatiecampagne en voor aanlevering van batchnummers als Bijwerkingencentrum Lareb daar om vraagt. Ook kunnen mensen bijvoorbeeld snel worden gewaarschuwd bij bijwerkingen.

Op grond van de wet bewaart het RIVM vaccinatiegegevens in principe 20 jaar. Mensen kunnen de gegevens altijd laten verwijderen via mijn.rivm.nl. Deze mogelijkheid is wettelijk vastgelegd in de wet AVG.

Bespreking Stuurgroep covid-registratie
Vergaderdatum en -tijd 12 mei 2021, 09.45 – 11.00 uur
Vergaderplaats Webex
Deelnemers

[REDACTED] (vz.), [REDACTED],
[REDACTED], [REDACTED], [REDACTED],
[REDACTED] en [REDACTED],
(agendapunt 2), [REDACTED],
(secre.)

Afwezig
Kopie aan

[REDACTED], [REDACTED], [REDACTED]

1. Opening en mededelingen

- [REDACTED] opent het overleg en de agenda wordt vastgesteld.

2. Ontwikkelingen mb.t. Mijn.RIVM.nl en stand van zaken AVG-verzoeken

[REDACTED] en [REDACTED] worden hartelijk welkom geheten.

Ruim een maand geleden is mijn.RIVM.nl live gegaan. In Mijn.RIVM.nl worden gegevens uit het BRP getoond. Na de livegang zijn er vragen van burgers gekomen. Vanaf 22 april tot heden zijn ruim 60.000 AVG verzoeken binnen gekomen via e-mails en ingevulde webformulieren.

Vanuit privacy oogpunt is het niet zo dat er een issue m.b.t. compliance is. Het is juist goed om de gegevens te laten zien. Zoals het nu ingericht is, doet de burger geen formeel verzoek tot inzage. Dat kan ondervangen worden door een welkom-pagina in te richten, met een vervolgvraag tot inzage. Het tonen van de gegevens is gerechtvaardigd en afgedekt door de opdracht die gegevens is (en waar een DPIA voor geweest is). De gegevens waar het in Mijn.RIVM.nl om gaat, zijn de vaccinatiegegevens; dat is ook het doel van Mijn.RIVM.nl. Andere data kunnen via de AVG-desk opgevraagd worden. De gegevens die vanuit BRP geladen worden, hebben we o.a. nodig voor uitnodigingen, herhaal-uitnodigingen en check of iedereen bereikt is.

Het voorstel dat er nu ligt betreft een aanpassing van het portaal, waarbij de BRP gegevens niet meteen getoond worden, eerst een welkom-pagina en daarna een vervolgvraag voor inzage gegevens. Daar kan er ook op gewezen worden dat als de burger verder wil zien welke gegevens er zijn, hier een reguliere, maar separate route voor is (AVG-desk). Zo wordt maximaal transparantie gegeven hoe de informatie bereikt kan worden (conform privacy wetgeving), zonder dat alles zichtbaar is en zonder dat de transparantie de privacy van anderen raakt. De communicatie is hier essentieel in. En vanzelfsprekend ook de afstemming met VWS/Minister.

Overigens is de start van het proces inloggen met DigiD, daar zit al een persoonsidentificatie in.

De stuurgroep gaat akkoord met dit voorstel, en legt het nog voor aan de stuurgroep van het programma a.d.h.v. een beknopt memo.

Besluit 47: Akkoord met het voorstel aanpassing Mijn.RIVM.nl door invoegen van een welkom pagina, waarna verzoek tot inzage vaccinatiegegevens gedaan kan worden. Voor inzage van overige gegevens is de reguliere route beschikbaar en dit voorleggen aan de stuurgroep van het programma.

Bij de livegang is het risico geaccepteerd van BSN-nummer die gebruikt worden in versleutelde berichten naar Signicat. Na de live-gang hebben de FG en privacy-officer van FCC een stevig negatief advies hierover gegeven. Overigens wordt deze route veel vaker binnen de overheid ingezet, dus is het toch wat verwonderlijk dat er zo'n stevig advies gegeven wordt. Bij de risico-acceptatie is ook meegenomen dat dit binnen 6 maanden opgelost zou worden. Er is een overleg met Signicat gepland hierover. In het volgende stuurgroepoverleg zal de stand van zaken hieromtrent aan de orde komen. [REDACTED] en [REDACTED] zullen dit voorbereiden.

Actie 168 [REDACTED] en [REDACTED]: voorbereiding stand van zaken logging door Signicat voor stuurgroepoverleg van 20 mei.

[REDACTED] geeft een toelichting wat betreft Verwerken individuele verzoeken; het betreft ruim 60.000 verzoeken (mails) die binnengekomen zijn (AVG webformulieren en mails).

Op basis van advisering van jurist moeten alle aanvragen individueel afgehandeld worden. Het verzoek voor verwijderen is vorm-vrij, met als gevolg dat aan de indieners niet gevraagd kan worden nog een formulier in te vullen. Niet uit alle aanvragen is af geleiden welke gegevens de burger verwijderd wil hebben, daarvoor zal nadere informatie ingewonnen moet worden bij de burger(s) om de verzoeken in behandeling te kunnen nemen. Dat maakt het allemaal complex en arbeidsintensief om te behandelen.

Er zal sowieso een bericht naar alle indieners gaan dat volledige afhandeling binnen een maand niet lukt, en dat gebruikt wordt gemaakt van de verlenging. Er zal een team aangetrokken worden.

Vanmiddag volgt er overleg met de experts, hoe een en ander mogelijk geautomatiseerd ondersteund kan worden (en wat handmatig moet).

Ook is er nog overleg met de juristen.

Insteek is dat een zo groot mogelijk groep tegelijk een reactie gestuurd kan worden. Met het samenstellen van het team wordt ook doorgedaan.

Communicatief gaat dit nogal wat vragen. Er ligt inmiddels een voorzet voor een persbericht te publiceren op de eigen kanalen en afgestemd met VWS.

Op basis van de suggesties uit het overleg, zal dit bericht nog aangepast worden.

[REDACTED] zorgt voor een nieuwe versie van de stukken, die vervolgens voorgelegd worden aan de stuurgroep van het programma.

Actie 169 [REDACTED] en [REDACTED]: nieuwe versie van de stukken m.b.t. mijn.rivm.nl die ook naar de stuurgroep van het programma gestuurd worden.

3. Vaststellen procedure calamiteiten in dataverkeer prioritering

4. **Oefening ketencalamiteiten COVID-19 vaccinatie gegevensuitwisseling**

Deze punten wordt gelijk behandeld.

90 [] heeft, conform afspraak in het vorige stuurgroepoverleg, de stukken op basis van de bespreking aangepast. [] geeft aan dat de Stuurgroep "Gegevensuitwisseling covidvaccinatie" (voorgezeten door VZVZ) de oefening gaat inplannen met alle betrokken ketenpartners. De stuurgroep is akkoord.

95 **Besluit 48:** de stuurgroep stelt de procedure calamiteiten in dataverkeer prioritering vast.

Besluit 49: de stuurgroep gaat akkoord met de oefening ketencalamiteiten Covid-19 vaccinatie gegevensuitwisseling. De verdere uitwerking hiervan gebeurt in overleg met de stuurgroep VZVZ en ketenpartners.

100 **Actie 170** []: vraagt [] en [] deze oefening verder op te pakken.

5. **Hoofdpuntenrapportage Landelijke Registratie**

Adrie geeft een toelichting:

- 105 • data-aanlevering gepersonaliseerd: er is een task force ingericht om operationeel uit te zoeken wat er nog allemaal gedaan kan worden. In de task force nemen VZVZ, leveranciers van de bronsystemen en enkele leden van koepels deel.
- 110 • voor een volgende stuurgroep bedenken hoe te komen tot de beslissing en wanneer wat het moment is waarop we over gaan naar CIMS.
- 21 mei is de laatste datum waarop plan B (in het kader van ontsluiten data vaccinatiebewijs) in gang gezet kan worden.

6. **Verslag overleg Stuurgroep Registratie 6 mei 2021.**

115 Akkoord.

De acties worden doorgelopen.

7. **Rondvraag**

120 Wordt geen gebruik van gemaakt.

Acties

	Verslag-datum:	Actie:	Wie:	Status:
147	01.04.2021	Aanpassing prioritering inclusief Dashboards en Bestelmodule t.b.v. planning en resourcing april 2021.		Loopt
157	15.04.2021	DPV_265 bespreken met VWS en de koepelorganisatie, m.b.t. door te voeren correcties in de bronregistraties.		Loopt
159	22.04.2021	De scope van het 1-prikscenario m.b.t. het vaccinatiebewijs (1-prikscenario en/of 2-prikscenario) bespreken met VWS.		Loopt
161	06.05.2021	Check formulering beslispunt beheer calamiteitenprocedure dataverkeer.		Zie DPV_274 Beslisnota calamiteitenprocedure dataverkeer covid-19.
162	06.05.2021	Check hoe de afstemming met de IV-organisatie geweest is over de calamiteitenprocedure dataverkeer		Zie DPV_274 Beslisnota calamiteitenprocedure dataverkeer covid-19.
163	06.05.2021	Calamiteitenprocedure dataverkeer inbrengen in wekelijks overleg met VWS over registratie.		
164	06.05.2021	Mededeling in stuurgroep Covid Programma van DAP en het delen met VWS.		
165	06.05.2021	Stuurgroep van het Covid Programma informeren over de stand van zaken ontsluiten data vaccinatiebewijs.		
166	06.05.2021	Afspraak tussen [redacted] en [redacted] om te bepalen wanneer het laatste moment is dat plan B ingezet kan worden voor ontsluiten data vaccinatiebewijs.		21 mei 2021
167	06.05.2021	Check bij VWS waarom er nog geen besluitvorming over doorgeven registratie vanuit BES/CAS is.		Telefonisch + e-mail van [redacted] (VWS) aan [redacted] op 6 mei: - BES/CAS acht het niet nodig om gepersonaliseerde data aan te leveren - En komt hier op terug als zij vastlopen m.b.t. het covidcertificaat.
168	12.05.2021	Stand van zaken en resultaat overleg Signicat.		
169	12.05.2021	Nieuwe versie van stukken m.b.t. Mijn.RIVM.nl mede t.b.v. de stuurgroep van het programma.		
170	12.05.2021	Vraag aan [redacted] en [redacted] om oefening ketencalamiteiten Covid-19 vaccinatie gegevensuitwisseling verder op te pakken.		

Afspraken/besluiten

Nummer:	Verslag-datum:	Afspraak
1.	13.08.2020	Samenstelling en rolverdeling projectstuurgroep conform Projectbrief versie 0.3.
2.	13.08.2020	Governance volgens scrummethodiek met productowner en scrumteam. Ook behoudt van de projectstuurgroep (Prince2) om issues op te lossen, kaders te geven en te bewaken, risico's te bewaken. Het scrumteam bestaat uit DVP, BIS, de leverancier(s).
3.	13.08.2020	We gaan starten met twee sporen: 1 kopie Praeventis gereedmaken voor verdere inrichting; 2 ruimere verkenning van informatiesystemen.
4.	13.08.2020	[redacted] krijgt van [redacted] mandaat om het project te starten.
5.	31.08.2020	Er wordt niet verder buiten het RIVM naar andere bruikbare systemen gekeken.
6.	31.08.2020	Alle mogelijk bruikbare koppelingen met LSP realiseren.

7.	15.09.2020	De Stuurgroep gaat akkoord met de start van het sprintteam Functionele Inrichting aan de hand van use case versie 0.4.
8.	15.09.2020	Het sprintteam rapportage tooling kan gaan starten zodra de resourcing compleet is.
9.	15.09.2020	wordt afgezand van het RIVM in de stuurgroep LSP-/PGO t.b.v. CIMS.
10.	12.10.2020	wordt de contactpersoon vanuit de IV-organisatie.
11.	26.10.2020	is eigenaar van het project, de projectrisico's en de functionele risico's
12.	26.10.2020	is eigenaar van de systeemrisico's van de infrastructuur, de applicatie, portalen en tooling.
13.	26.10.2020	coördineert de antwoorden op de beleidsonzekerheden (samen met).
14.	24.11.2020	Het cliëntbeheer wordt centraal ingericht, d.w.z. dat alle DVP'ers (ongeacht regiokantoor) gegevens kunnen verwerken. De autorisaties en de logging van feitelijke verwerking door individuele medewerkers worden hiervoor ingericht. Indien vanuit privacy-afweging wél beperking opgelegd moet worden, wordt dat geregeld op het niveau van de autorisaties van de DVP'ers.
15.	24.11.2020	Programmabureau covidvaccinatiecampagne is verantwoordelijk voor het aanleveren van de afgestemde Use Case en de bijbehorende afgestemde procesplaten.
16.	07.12.2020	Livegang CIMS is op 30 december 2020.
17.	11.12.2020	Stuurgroep is akkoord met de voorgestelde scope voor DPIA opgesteld voor de livegang CIMS op 30 december 2020.
18.	15.12.2020	Programmamanager () en centrumhoofd () tekenen risicoacceptatieformulier, () en () kijken mee en brengen het in bij (). Er is sprake van een getrapte ondertekening: (CISO) en (privacy officer) leggen het risicoacceptatieformulier voor aan de programamanager CIMS (), hoofd DVP () en crisismanager CIMS (). Zij accepteren de genoemde risico's wel of niet, waarna ze het formulier voorleggen aan de CIO () en pDG/portefeuillehouder privacy/CFO (). Zij volgen de risicoacceptatie van () (of niet) en bieden het acceptatieformulier aan aan DG-RIVM (). DG-RIVM is eindverantwoordelijk en gaat ultiem akkoord of benoemt extra maatregelen.
19.	15.12.2020	informeert privacy officer over beleidskeuzes die impact kunnen hebben op scope risicoanalyse.
20.	15.12.2020	kanaliseert de aanpassingen aan CIMS. Als deze lijken te bekliven, dan geeft () aan Janet door welke wijzigingen in PIA moeten worden meegenomen.
21.	15.12.2020	Stuurgroep stemt in met deprioritering van het Zorgverlenersportaal (zie DPV_182).
22.	15.12.2020	Voorstel aannemen mensen i.h.k.v. inrichting registratiesysteem CMS is bekrachtigd door stuurgroep.
23.	21.12.2020	Stuurgroep is akkoord met een beschikbaarheid van 98,5% voor het platform Praeventis, de SFTP server CIMS en de applicatie/database CIMS. In januari 2021 wordt toegewerkt naar een beschikbaarheid van 99,9%. Stuurgroep is ook akkoord op de voorgestelde voorlopige inrichting van het service window. De stuurgroep gaat ervanuit dat dit een startsituatie voor januari 2021 is, die kan wijzigen. Hiertoe zal eind januari 2021 een evaluatiemoment in de stuurgroep plaatsvinden. Mogelijk worden dan nieuwe of herijekte afspraken gemaakt.
24.	28.12.2020	Stuurgroep: <ul style="list-style-type: none"> – onderschrijft dat GGDHOR alleen volgens de reeds bestaande werkwijze vaccinatiegegevens kan aanleveren, omdat de tijd ontbreekt om de geplande oplossing te realiseren; Wij kunnen rechtstreeks in hun omgeving met hen koppelen. – neemt kennis van de risico's en de daarmee samenhangende politiek/bestuurlijke kwetsbaarheid voor RIVM; hangt reputatie rondom route. – besluit de koppeling met GGDGHOR te realiseren.
25.	28.12.2020	Stuurgroep is akkoord met de functionaliteiten genoemd in DVP_195 en stuurt aan op livegang op 8 januari 2021 onder de condities gegeven in DVP_195. Het formele besluit wordt op 7 januari 2021 genomen.
26.	05.01.2021	Stuurgroep besluit dat DPIA en IB-analyse beide groen licht geven voor het ontvangen van gegevens van GGD GHOR voor CIMS.
27.	05.01.2021	Stuurgroep stemt in met het verwijderen van Geboorteland uit de registratie.
28.	06.01.2021	Stuurgroep accepteert de informatiebeveiligings(rest)risico's zoals deze benoemd zijn in de Oplegnotitie risicoregister CIMS 1.0 voor livegang van CIMS release 1 en accordeert de beschreven vervolgacties voor ná livegang.
29.	06.01.2021	Stuurgroep heeft in lijn met DPIA, analyse door Privacy Officer en het advies van de FG voldoende vertrouwen dat er in CIMS release 1 op een goede manier met privacy wordt omgegaan.
30.	06.01.2021	Stuurgroep gaat akkoord met de genoemde functionaliteit, compliance, beheer en in te richten CAB zoals genoemd in DPV_194 Besluitnota livegang CIMS release 1. Stuurgroep besluit om CIMS release 1 live te brengen op 6 januari 2021.

31.	14.01.2021	Stuurgroep neemt kennis en onderkent de behoefte van het leveren van gegevens aan stakeholders direct na start van de vaccinatiecampagne. Stuurgroep gaat akkoord met een verkorte DPIA en Quickscan BIO ten behoeve van de levering van voornoemde gegevens voorafgaand aan de officiële livegang van de rapportage omgeving.
32.	04.02.2021	Clientbeheer wordt op de regiokantoren uitgevoerd door CIMS medewerkers die hiervoor opgeleid worden.
33.	04.02.2021	De stuurgroep is niet het gremium te besluiten over grondslag en risicoacceptatie voor COA. Het besluit moet genomen worden door het strategisch crisisberaad op 5 feb 2021.
34.	18.02.2021	zal vanuit EPI deelnemen aan stuurgroep Covid-registratie.
35.	18.02.2021	Stuurgroep accepteert de restrisico's uit het addendum DPIA en de IB risicoanalyse voor inlezen COA- en Probas-bestanden en stelt ze hierbij vast. Het Probas-convenant kan ondertekend worden.
36.	22.02.2021	Stuurgroep besluit voor optie 3 uit DPV_245 - het laten maken van een overzicht van hoe het project het beste vorm gegeven kan worden, en er voor te zorgen dat de hiervoor benodigde personen enkele uren tijd krijgen om hieraan te besteden. Zodat daarna commitment gegeven kan worden aan doorgang van het project met een aangepaste en voor het RIVM haalbare planning.
37.	04.03.2021	Stuurgroep gaat akkoord met de mitigatie van de restrisico's voor het oproepproces, maar wil weten hoe gecontroleerd kan worden of Xerox conform afspraken werkt.
38.	04.03.2021	Stuurgroep is akkoord met de vervolgacties (waarbij de nu niet aanwezige stuurgroepleden nog per mail kunnen reageren) en bevestigt de livegang van de rapportage tooling.
39.	11.03.2021	Stuurgroep besluit tot uitstel van de livegang van het cliëntportaal zodat teksten aangepast kunnen worden.
40.	18.03.2021	De Stuurgroep gaat akkoord met de wijzigingen t.b.v. de performanceproblemen CIMS.
41.	01.04.2021	De stuurgroep besluit capaciteit vrij te maken voor impactanalyse 1 prik scenario (na doorgemaakte Covid)
42.	08.04.2021	Een laatste poging wordt gedaan de BES/CAS te bewegen gegevens te verstrekken. Als de BES/CAS dat niet doet, is er daarna geen mogelijkheid meer de gegevens later in te lezen. De stuurgroep van het programma wordt gevraagd deze lijn te bekrachtigen.
43.	15.04.2021	Onder voorbehoud van afstemming met EPI gaat de stuurgroep akkoord met de in de nota Beslisnota Verbetering Datakwaliteit (DPV_265) onder paragraaf 5 voorgestelde optie van corrigeren van data.
44.	22.04.2021	Besloten wordt de afweging van de scope van het vaccinatiebewijs (1-prikscenario en/of 2-prikscenario) bij VWS neer te leggen.
45.	22.04.2021	Met betrekking tot de vervolgstappen 1-prikscenario houden we de Governance aan.
46.	22.04.2021	Vastgesteld wordt dat de huidige gegevenslevering vanuit CorinIT aan EPI vooralsnog in stand blijft.
47.	12.05.2021	Akkoord met het voorstel aanpassing Mijn.RIVM.nl door invoegen van een welkom pagina, waarna verzoek tot inzage vaccinatiegegevens gedaan kan worden. Voor inzage van overige gegevens is de reguliere route beschikbaar. Dit akkoord voorleggen aan de stuurgroep van het programma.
48.	12.05.2021	De stuurgroep stelt de procedure calamiteiten in dataverkeer prioritering vast.
49.	12.05.2021	De stuurgroep gaat akkoord met de oefening ketencalamiteiten Covid-19 vaccinatie.

Bespreking	Stuurgroep covid-registratie
Vergaderdatum en -tijd	20 mei 2021, 11.00 – 12.00 uur
Vergaderplaats	Webex
Deelnemers	[redacted] (vz.), [redacted] [redacted], [redacted], [redacted], [redacted] [redacted], [redacted] (agendapunt 4), [redacted] (secr.)
Afwezig	[redacted]
Kopie aan	[redacted], [redacted]

1. Opening en mededelingen

- [REDACTED] opent het overleg en de agenda wordt vastgesteld.
- MT uitvoering heeft zich deze week gebogen over de opschalingsvraagstuk, waarin wordt gekeken naar een digitale route en vergroten bereikbaarheid RIVM.
- Met VWS is deze week overleg geweest over de vaccinatiebewijzen en de vertraging die daarop zit. Verschillende scenario's zijn besproken. Voorkeurscenario wordt met behulp van VWS opgepakt waarin wordt gewerkt naar oplevering op 6 juni.

2. Hoofdpuntenrapportage Landelijke Registratie (bijlage b, DPV_ 213), inclusief Vijfmaandsrapportage t.b.v. VWS.

█ geeft toelichting op de hoofdpuntenrapportage. █ vraag █ het overzicht dat we dagelijks van █ krijgen te delen met VWS.

3. Bevindingen “belactie” (bijlage c, Rapportage ontbrekende gegevens in CIMS)

Eerder is besloten om instellingen en huisartspraktijken die volgens de gegevens van RIVM vaccins hebben ontvangen maar geen of nauwelijks vaccinatiegegevens hebben aangeleverd aan RIVM, te bellen. Doel van de belactie was inzicht krijgen in de mogelijke oorzaken van de verschillen en op grond hiervan besluiten of voortzetting van de belactie gewenst was. De belactie heeft bevestigd dat er nog achterstanden zijn bij registreren en met name het 'vrij geven' van de vaccinatiegegevens. Dit speelt vooral bij de instellingen. Vooral tot de huisartspraktijken is nog onvoldoende houvast m.b.t. voor het vinden van een verklaring voor de grote verschillen. Via de procesinformatie (zie 3.1) wordt geprobeerd meer zicht te krijgen op het totaal aantal gezette prikken. Daarnaast wordt een vergelijking gemaakt van alle huisartspraktijken in Nederland en het aantal huisartspraktijken dat (voldoende) gegevens heeft aangeleverd aan CIMS. Het verschil betreft dan praktijken die niet of nauwelijks hebben aangeleverd. Als het lukt om hieraan de HIS-leverancier te koppelen dan wordt het gesprek gevoerd met de leverancier om een bevestiging te vragen. Vervolgens kan in overleg met betrokken partijen (koepelorganisaties en HIS-leveranciers) bepaald worden welke passende vervolgacties aan de orde kunnen zijn. Een vergelijkbaar traject wordt onderzocht voor de instellingen.

4. Use case "1-prikscenario" (bijlage d, nota registratie 1-prikbeleid)

38 Er is vorige week een impactanalyse gedaan over de registratie van de 1-prik. Aanvankelijk was
het de bedoeling dat we in CIMS en in CIMS-BI de registratie zouden opnemen. Met wat
uitzoekwerk is het voorstel om alleen in CIMS-BI de registratie op te nemen. Om die registratie
vervolgens te realiseren tijdens de realisatie van de procesdata CoronIT en ZKHVI en de
aanpassing van een extra veld DPV_210 voor de procesdata. [redacted] vindt dit een heldere notitie en
40 vraagt of dit met VWS is afgestemd. Met VWS is hier over gesproken. [redacted] vraagt hoe het zit
met de CIMS-koppeling met de VWS app wanneer er enkel wordt gekeken of je wel niet of bent
gevaccineerd i.p.v. of je de eerste of tweede prik hebt gehad. [redacted] geeft aan de logica of iemand
een groene kaart krijgt wordt geïmplementeerd in de VWS app en niet bij RIVM. Wij leveren
alleen de vaccinatiedata aan en zij kunnen met beslisregels dit verder vormgeven.
45 De leden van de stuurgroep vragen om een aanscherping m.b.t. het te nemen besluit (Aktie
[redacted]) zodat in een volgend overleg de nota kan worden vastgesteld.

5. Verwerking van verwijderingsverzoeken (bijlage e, DPV_278)

Op basis van de bespreking vorige week, is de nota aangescherpt door [redacted] en [redacted].
50 Complimenten voor de nota van de stuurgroepleden. Het punt over gebruik van DigiD wordt nog
een duidelijker opmerkingen over gemaakt. Duidelijk is dat afhandeling van de inmiddels ca.
62.000 verzoeken tot verwijdering niet in 3 maanden gaat lukken. Een optie zou kunnen zijn om
een self service portal te realiseren; dat zou echter nog helemaal ontwikkeld moeten worden.
Uitgezocht wordt wat de consequenties zijn voor het RIVM als de afhandeling binnen 3 maanden
55 niet lukt.
In de nota is ook een duidelijke paragraaf opgenomen over de communicatie, met diverse opties.
De voorkeur is optie B, in combinatie met optie A. Een optie D zou kunnen zijn: geen
communicatie. De communicatie let nauw, zeker omdat de verwachting is dat dit onderwerp in de
voortgangsbrief opgenomen zal worden. Op basis van de bespreking stelt [redacted] de nota nog iets
60 bij en die wordt vervolgens aan de stuurgroep Programma Covid 19 Vaccinatie voorgelegd.

6. Verslag

Geen bijzonderheden. Het verslag wordt ongewijzigd vastgesteld.

7. Rondvraag

65 - Het is de laatste keer dat [redacted] bij dit overleg is; ze wordt hartelijk bedankt voor haar inzet als
secretaris.



Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

nota

Betreft	Ontwikkelingen m.b.t. Mijn.RIVM.nl
Nota nummer	DPV_278
Contactpersonen	[REDACTED], [REDACTED]
Besluit	Ja

Doel

De stuurgroep Vaccinatie wordt gevraagd kennis te nemen van ontwikkelingen m.b.t. Mijn.RIVM.nl en vervolgens in te stemmen met voorgestelde maatregelen. Voorliggende nota is vervolg op versie 0.5 en versie 1.0 welke op 12 en 19 mei 2021 zijn besproken in de stuurgroep Covidvaccinatieregistratie.

Aanleiding

Mijn.RIVM.nl/vaccinaties is op 8 april 2021 live gegaan. Na livegang hebben een aantal ontwikkelingen plaatsgevonden:

1. Burgers en de FG VWS hebben vragen gesteld over het doel van het tonen van de BRP-gegevens en het portaal.
2. Tijdens het Kamerdebat in week 18 zijn opmerkingen gemaakt door de partij BBB die in lijn liggen met de vragen van burgers. De Minister heeft toegezegd beter en meer te zullen communiceren over Mijn.RIVM.nl en het gebruik van o.a. BRP-gegevens door RIVM.
3. In de periode 22 april 2021 tot heden zijn ruim 72.000 AVG-verzoeken binnen gekomen via e-mails en ingevulde webformulieren. De verzoeken zijn veroorzaakt door acties op sociale media.
4. Inmiddels zijn vragen over MijnRIVM.nl van een fact check bureau dat actief is op sociale media in samenwerking met communicatie beantwoord. Ook heeft een journalist een artikel in voorbereiding over het onderwerp, waarover contact is geweest met woordvoering.

Gevraagd besluit

De Stuurgroep wordt gevraagd akkoord te geven op onderstaande voorstellen t.a.v. uitgangspunten, privacy, Mijn.RIVM.nl/vaccinaties en publiekscommunicatie, of desgewenst richting te geven aan andere maatregelen. Na afloop van besluitvorming wordt COVID-programmadirectie gevraagd besluit en insteek t.a.v. communicatie af te stemmen met min. VWS.

Uitgangspunten:

1. RIVM mag BRP-gegevens verwerken (covidvaccinatie valt onder RVP, RVP valt onder WPG, WPG geeft de grondslag, bovendien is er autorisatie gegeven via autorisatiebesluit);
2. RIVM mag vastgestelde set vaccinatiedata verwerken (wat de set is ligt vast in de DPIA (versie 31 dec 2020);
3. "Inzage geven in vaccinatiedata" en "AVG-rechten geven aan betrokkenen" uit elkaar houden.

Het voorstel is om de uitgangspunten *niet* te wijzigen, immers:

1. Cliënten die Mijn.RIVM.nl/vaccinaties gebruiken krijgen alléén de privacyverklaring te zien; vanuit de verklaring wordt er doorgelinkt naar de webformulieren voor het betreffende wijzigingsverzoek.
2. En vice versa: om "AVG-rechten van betrokkenen" uit te oefenen is er geen inlog nodig op Mijn.RIVM.nl/vaccinaties.

T.a.v. Mijn.RIVM.nl/vaccinaties:

In Mijn.RIVM.nl/vaccinaties worden twee groepen gegevens getoond, te weten:

1. BRP-gegevens. Doel: duidelijk maken van wie de vaccinatiedata zijn. Nu: voornaam/namen, achternaam, geslacht en geboortedatum. Ervaring met het RVP leert dat niet volstaan kan worden met minder BRP-gegevens, omdat cliënten zichzelf én ouders/voogden/bewindvoerders de betreffende persoon moeten kunnen verifiëren dat de BRP-gegevens en betreffende vaccinatiedata bij elkaar horen. Indien RIVM van de cliënt geen vaccinatiedata is opgenomen in het landelijk register, worden op dit moment wel de BRP-gegevens getoond.
2. Vaccinatiedata. Doel: inzage geven in de vaccinatiedata. Dit is een dienst van RIVM aan de burger die past bij het beleid van de Rijksoverheid om cliënten regie te geven over eigen data. Alléén vaccinaties, dus (op dit moment) geen overige data (bijv. hielprikuitslag). De datavelden die getoond worden zijn: Vaccinnaam, batchnummer, vaccinatiedatum, fabrikant. De grondslag voor inzage is veronderstelde toestemming door de cliënt, omdat de cliënt om de inzage vraagt. Wie niet om inzage vraagt, krijgt ook geen vaccinatiedata te zien.

Het voorstel is om:

1. Geen BRP-gegevens te tonen indien van de betreffende cliënt geen vaccinatiedata beschikbaar zijn in het landelijk register. Hiermee wordt voorkomen dat persoonsgegevens zichtbaar zijn zonder dat daar een concrete aanleiding voor is (in casu: vóórdat iemand gevaccineerd is en toestemming heeft gegeven om zijn/haar gegevens te delen). Vanuit privacyperspectief verdient dit de voorkeur. Wat de inloggers wél zullen (blijven) zien is (rechts boven in het scherm) hun achternaam, als bevestiging van de inlogpoging via DigiD. Zie bijlage 1 voor een screen shot van de wijziging, die - onder voorbehoud - aan het einde van week 21 van 2021 gereleased zou kunnen worden.
2. Het portaal ongewijzigd te laten indien:

- a. er wél vaccinatiedata beschikbaar zijn. In dit geval worden dus zowel vaccinatiedata als BRP-gegevens getoond.
- b. er inzage is gegeven aan Lareb of anderen. In dat geval wordt de additionele informatie (alleen) getoond in combinatie met de vaccinatiedata.

T.a.v. privacy (AVG-rechten van betrokkenen):

Identificatie van cliënten die AVG-rechten uitoefenen is noodzakelijk om te voorkomen dat onbevoegden wijzigingsverzoeken doen op naam van een cliënt. Bij de livegang van het portaal is gekozen voor identificatie van burgers zoals nu gedaan wordt voor het Rijksvaccinatieprogramma (RVP), zie DPV_263 Bessluitnota livegang cliëntportaal. (Voor het RVP kan het RIVM nog geen burgers identificeren m.b.v. DigiD.)

Het voorstel is om:

1. Een impactanalyse te maken van de mogelijkheden om een *self service portal* (via MijnRIVM.nl) in te richten voor AVG-verzoeken, waarbij identificatie van personen plaatsvindt o.b.v. DigiD. Zie use case in bijlage 2. DigiD is een betrouwbare tool die door de Rijksoverheid wordt aangeboden voor diensten van de Rijksoverheid aan burgers. DigiD mag niet het enige identificatiemiddel/kanaal zijn voor AVG-verzoeken, omdat niet alle burgers over digitale hulpmiddelen beschikken. Hiermee wordt bereikt dat (veel) minder handmatig werk hoeft te worden uitgevoerd op de regiokantoren van DVP. *Let op:* afhankelijk van de technische impact en omvang van deze wijziging wordt duidelijk of zo'n *self service portal* AVG-verzoeken ook een vruchtbare route is voor de afhandeling van de huidige ca. 70.000 verzoeken in de komende twee maanden (zie hieronder).
2. De afhandeling van AVG-verzoeken verder uit te voeren conform de daarvoor ingerichte procedure, zie DPV_263 Bessluitnota livegang cliëntportaal. Hieronder volgt een stand van zaken.

Op het moment van schrijven (19/5) zijn er 42.574 AVG verzoeken via een webformulier binnengekomen. Daarnaast zijn er nog 33.774 mails met gedeeltelijke verzoeken, vervolg/herhaalberichten en kopieën van ID-bewijzen. Voor de afhandeling van AVG-verzoeken is een identificatie verplicht. Verzoeken zullen daarom één voor één afgehandeld (moeten) worden.

Alle burgers die op dit moment een verzoek of anders hebben ingediend zijn op de hoogte gebracht van de verlenging van de termijn van afhandeling van 1 naar 3 maanden. Voor het afdoen van de verzoeken geldt dat zodra een (in)compleet verzoek ontvangen is de termijn van een maand, maximaal te verlengen tot 3 maanden, gaat lopen. Op het moment dat wij betrokkene melden dat de aanvraag niet compleet is schort de termijn op tot het moment dat de aanvraag compleet is.

Een uitvraag in de mantel voor het werven van een AVG-team bij DVP-Zoetermeer loopt. Zodra geworven, kan de afhandeling van alle AVG-verzoeken starten. In totaal wordt een team samengesteld van 18 medewerkers + leidinggevende (deels via mantel en deels aangevuld met

zitten personeel). Doelstelling is om uiterlijk 15 juni 2021 het team operationeel te hebben.

In de eerste weken van afhandelen zal bekeken worden hoeveel verzoeken het team dagelijks af kan handelen. Op basis hiervan kan gekeken worden of opschaling van het team snel resultaten gaat geven.

Het is van belang om te beseffen dat de AVG-termijn van 3 maanden met de huidige beoogde werkwijze niet gehaald zal worden. 3 maanden betekent namelijk dat het grootste deel van de ca. 30.000 verzoeken die in het eerste weekend zijn binnengekomen uiterlijk 23 juli 2021 afgehandeld moeten zijn.

Op 20 mei 2021 heeft overleg met de FG en privacyjuriste van WJZ (VWS) plaatsgevonden over de afhandeling van de vele burgerverzoeken.

Als de afhandelingstermijn van drie maanden niet wordt gehaald kan de burger een ingebrekestelling indienen. RIVM heeft dan twee weken om het gebrek (het niet tijdig besluiten) te herstellen. Indien dat niet gebeurt kan een dwangsom worden opgelegd. Van belang is dat wij ons proces er op in richten dat ingebrekestellingen direct worden opgepakt om binnen twee weken het verzoek af te handelen. De aanvraag is immers compleet. Daarmee wordt voorkomen dat we grote dwangsommen opgelegd krijgen.

Ook is gesproken over manieren om de termijn van afhandeling te verkorten. Buiten systeemtechnische oplossingen (a la de *self service omgeving AVG-rechten*, zie bijlage 3) zijn er tot op heden geen mogelijkheden gevonden. Het verwijderen van de gegevens vóórdat het RIVM een kopie ID heeft ontvangen kan mogelijk tot een versnelling in het proces leiden, maar het verzoek kan pas formeel afgehandeld worden als het ID gecontroleerd en gekoppeld is aan de aanvraag. Voordeel kan van deze werkwijze is dat burgers het gevoel hebben dat hun aanvraag is afgehandeld (zij zullen bijvoorbeeld geen uitnodigingen voor vaccinatie meer ontvangen) en niet (dagelijks) (herhaal)verzoeken blijven indienen.

VWS realiseert zich dat we met een bijzondere situatie te maken hebben welke nog niet eerder is voorgekomen. Zij adviseert in de toekomst DigiD in te zetten zodat burgers zich niet met een kopie ID hoeven te identificeren (zie bijlage 3).

Het is belangrijk om vast te stellen wat de wenselijkheid en/of mogelijkheden voor het organiseren van (meer) hulp en/of escalatie zijn. De stuurgroep Vaccinatie wordt gevraagd hierover mee te denken.

T.a.v. Publiekscommunicatie:

Gezien de voorgestelde functionele wijzigingen van MijnRIVM.nl wordt (door communicatie RIVM) een drietal scenario's voor de communicatie geschetst. DVP heeft communicatie verzocht om deze mogelijkheden, nog voor dat bekend werd dat de Minister wil dat er betere uitleg komt over het gebruik van gegevens t.b.v. vaccineren. VWS heeft aangegeven betrokken te willen zijn bij keuzes over de communicatie van wijzigingen

aan MijnRIVM.nl en een voorkeur te hebben voor optie (a), wat in tegenspraak lijkt met hetgeen de Minister in de Kamer beloofd heeft.

Opties (combinaties mogelijk):

- a. Geen publiekscommunicatie over de voorgestelde wijziging en/of algemene communicatie over MijnRIVM.nl
- b. Algemeen bericht over mijn.rivm.nl (zie concept in bijlage 2)

De aanvankelijke insteek van de communicatie, zoals ook door minister toegezegd. Een algemeen bericht dat burgers informeert over het bestaan en de functionaliteit van mijn.rivm.nl. Hiermee is het RIVM transparant over MijnRIVM.nl en de rechten die burgers hebben.

In dit scenario is het bericht voor nu afdoende, maar kunnen na de voorgenomen wijziging vragen volgen. Hieruit volgt eventueel een tweede bericht na het aanpassen van MijnRIVM.nl.

- b. Bericht waarin ook de wijziging wordt aangekondigd

Hierbij wordt een alinea toegevoegd aan het bestaande bericht waarin kort wordt verwezen naar de ontstane onduidelijkheid door het tonen van de BRP-gegevens. Om dit in de toekomst te voorkomen past het RIVM mijn.rivm.nl aan. Vanaf een nader te bepalen datum in 2021 zijn enkel gegevens zichtbaar van mensen die gevaccineerd zijn én toestemming hebben gegeven voor registratie.

Hiermee laten we zien dat er iets gespeeld heeft, maar ook dat het RIVM het signaal serieus neemt en er iets aan doet.

- c. Bericht waar iets gezegd wordt over de (langere) doorlooptijd van een reactie

Het toevoegen van een alinea over de doorloop tijd van de afhandeling van aanvragen tot verwijdering. Het toevoegen van deze procesinformatie in het bericht kan leiden tot veel vragen over het waarom van de lange doorlooptijd. Deze informatie kan ook elders op de website gepubliceerd worden en staat ook in de reeds vanuit het RIVM verstuurd e-mails aan verzoekers over uitstel van behandeling. Via beide opties is RIVM transparant over de langere doorlooptijd zonder er extra aandacht op te vestigen.

Het risico in alle scenario's blijft dat het RIVM en VWS/de minister vragen vanuit de media en/of kamer krijgen over het hoe en het waarom, alsook de proportionaliteit van het tonen van de BRP-gegevens in de eerste plaats. Voorbereiding op deze vragen is dan ook een belangrijk onderdeel van de communicatie.

De stuurgroep vaccinatie wordt gevraagd een afweging te maken. RIVM Communicatie en DVP/programma CIMS hebben een voorkeur voor een combinatie tussen de opties A + B.

Eventuele extra te overwegen acties:

1. Ingezonden artikel in dagbladen – aanleiding?
2. Communicatie vanuit VWS, bijv. in Kamerbrief?
3. Opstellen woordvoeringslijn en/of Q&A t.b.v. mediavragen

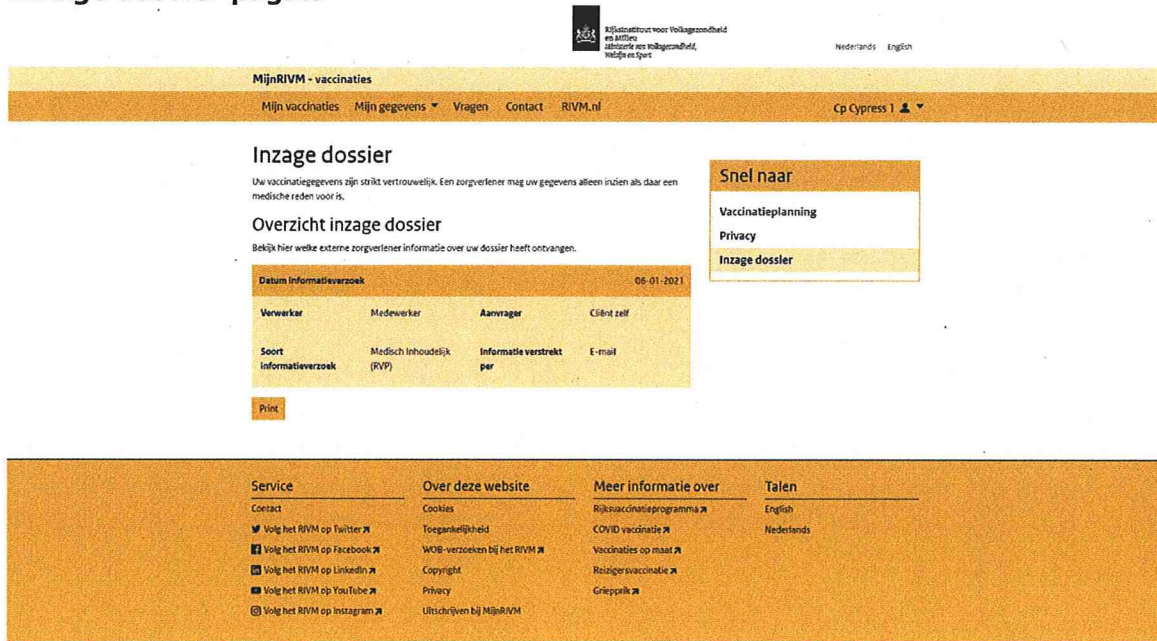
Bijlage 1: Screen shot voorgenomen wijziging MijnRIVM.nl*Burger zonder vaccinatiegegevens:***Vaccinatiegegevens scherm**

The screenshot shows the 'MijnRIVM - vaccinaties' page. At the top, there is a navigation bar with 'Mijn vaccinaties', 'Mijn gegevens', 'Vragen', 'Contact', and 'RIVM.nl'. A 'Testgebruiker' dropdown is on the right. The main content area has a header 'Mijn vaccinaties' and a table with columns 'Naam', 'Batchnr.', 'Datum', and 'Fabrikant'. The table is empty, with the message 'Er zijn geen vaccinaties gevonden.' below it. To the right, a 'Snel naar' box contains links for 'Vaccinatieplanning', 'Privacy', and 'Inzage dossier'. Below the table, there is a 'Print' button and a disclaimer: 'Dit overzicht is geen officieel vaccinatiebewijs. U kunt het dus niet gebruiken als bewijs van vaccinatie.' This is followed by a note about data accuracy and a list of bullet points: 'U heeft nog geen vaccinatie ontvangen.', 'Het kan enkele dagen duren voor dat uw vaccinatie in het overzicht staat.', 'Misschien heeft u geen toestemming gegeven om uw vaccinatiegegevens met het RIVM te delen.', and 'Misschien heeft u althans eenmalig uitschrijven uit de registratie.' Below this is a note about GGD data and a footer with 'Service', 'Over deze website', 'Meer informatie over', and 'Talen' sections.

Vaccinatiegegevens scherm printbaar

The printable version of the 'Mijn vaccinaties' screen. It features the RIVM logo at the top. The main heading is 'Mijn vaccinaties'. Below it is a table with columns 'Naam', 'Batchnr.', 'Datum', and 'Fabrikant'. The table is empty, with the message 'Er zijn geen vaccinaties gevonden.' below it. A disclaimer follows: 'De arts of GGD die u heeft gevaccineerd kan u ook meer informatie geven over uw vaccinatie.' Below this is a 'DISCLAIMER' section stating 'Dit is geen vaccinatiebewijs.' and a 'Gebruikte afkortingen' section with links for 'SARS-CoV-2' and 'Coronavirus'.

Inzage dossier pagina



Inzage dossier

Uw vaccinatiegegevens zijn strikt vertrouwelijk. Een zorgverlener mag uw gegevens alleen inzien als daar een medische reden voor is.

Overzicht inzage dossier

Bekijk hier welke externe zorgverlener informatie over uw dossier heeft ontvangen.

Datum informatieverzoek	06-01-2021		
Verwerker	Medewerker	Aanvrager	Client zelf
Soort informatieverzoek	Medisch inhoudelijk (RVP)	Informatie verstrekt per	E-mail

[Print](#)

Snel naar

- Vaccinatieplanning
- Privacy
- Inzage dossier

Service

- Contact
- Volg het RIVM op Twitter
- Volg het RIVM op Facebook
- Volg het RIVM op LinkedIn
- Volg het RIVM op YouTube
- Volg het RIVM op Instagram

Over deze website

- Cookies
- Toegankelijkheid
- WOB-verzoeken bij het RIVM
- Copyright
- Privacy
- Uitschrijven bij MijnRIVM

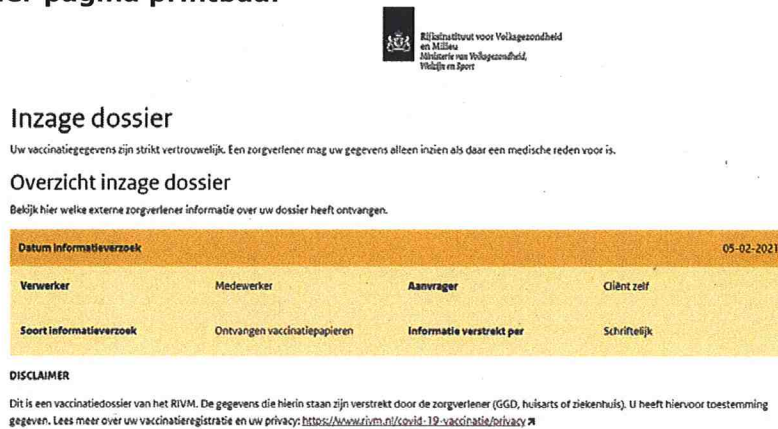
Meer informatie over

- Rijksvaccinatieprogramma
- COVID vaccinatie
- Vaccinatie op maat
- Reiziger vaccinatie
- Grippex

Talen

- English
- Nederlands

Inzage dossier pagina printbaar



Inzage dossier

Uw vaccinatiegegevens zijn strikt vertrouwelijk. Een zorgverlener mag uw gegevens alleen inzien als daar een medische reden voor is.

Overzicht inzage dossier

Bekijk hier welke externe zorgverlener informatie over uw dossier heeft ontvangen.


Datum informatieverzoek	05-02-2021		
Verwerker	Medewerker	Aanvrager	Client zelf
Soort informatieverzoek	Ontvangen vaccinatiepapieren	Informatie verstrekt per	Schriftelijk

DISCLAIMER

Dit is een vaccinatiegegevens van het RIVM. De gegevens die hierin staan zijn verstrekt door de zorgverlener (GGD, huisarts of ziekenhuis). U heeft hiervoor toestemming gegeven. Lees meer over uw vaccinatieregistratie en uw privacy: <https://www.rivm.nl/covid-19-vaccinatie/privacy>

Burger met vaccinatiegegevens:

Vaccinatiegegevens scherm


Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Wetgeving en Sport

Nederlands English

MijnRIVM - vaccinaties
Mijn vaccinaties
Mijn gegevens
Vragen
Contact
RIVM.nl
Cp Cypress 1

Persoonsgegevens

Voornaam Test	Geboortedatum 13-12-1963
Achternaam Cp Cypress 1	Geslacht Man

Snel naar

- Vaccinatieplanning
- Privacy
- Inzage dossier

Mijn vaccinaties

Naam	Batchnr.	Datum	Fabrikant
SARS-CoV-2	HV9934	09-11-2020	Moderna

Gebruikte afkortingen

SARS-CoV-2 Coronavirus

Print

Dit overzicht is geen officieel vaccinatiebewijs. U kunt het dus niet gebruiken als bewijs van vaccinatie.

Het overzicht toont de informatie die het RIVM van uw zorgverlener, na verlenende toestemming van uw kaart, heeft ontvangen. In het bovenstaande overzicht leeg dan kan dit de volgende redenen hebben:

- U heeft nog geen vaccinatie ontvangen.
- Het kan enkele dagen duren voordat uw vaccinatie in het overzicht staat.
- Misschien heeft u geen toestemming gegeven om uw vaccinatiegegevens met het RIVM te delen.
- Misschien heeft u zich eerder laten inschrijven uit de registratie.

Meer informatie over de geldigheid van de vaccinatie kunt u vinden op de [staat en antwoord pagina](#) over coronavaccinaties.

De arts of GGD die u heeft gevaccineerd kan u ook meer informatie geven over uw vaccinatie.

Service

- Contact
- Volg het RIVM op Twitter
- Volg het RIVM op Facebook
- Volg het RIVM op LinkedIn
- Volg het RIVM op YouTube
- Volg het RIVM op Instagram

Over deze website

- Coöls
- Tongeren@theid
- WOS-verzoeken bij het RIVM
- Copyright
- Privacy
- Uitschrijven bij MijnRIVM


Meer informatie over

- Rijksvaccinatieprogramma
- COVID vaccinatie
- Vaccinaties op maat
- Reizigersvaccinatie
- Griepvaccinatie

Talen

- English
- Nederlands

Vaccinatiegegevens scherm printbaar


Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Wetgeving en Sport

Mijn vaccinaties

Persoonsgegevens

Voornaam Test	Geboortedatum 13-12-1963
Achternaam Cp Cypress 1	Geslacht Man

Mijn vaccinaties

Naam	Batchnr.	Datum	Fabrikant
Bezig met laden van vaccinatie gegevens.			

De arts of GGD die u heeft gevaccineerd kan u ook meer informatie geven over uw vaccinatie.

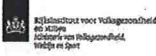
DISCLAIMER

Dit is geen vaccinatiebewijs.

Gebruikte afkortingen

SARS-CoV-2 Coronavirus

Inzage dossier pagina


Nederlands English

MijnRIVM - vaccinaties
[Mijn vaccinaties](#) [Mijn gegevens](#) [Vragen](#) [Contact](#) [RIVM.nl](#) Cp Cypress 1

Inzage dossier

Uw vaccinatiegegevens zijn strikt vertrouwelijk. Een zorgverlener mag uw gegevens alleen indien als daar een medische reden voor is.

Overzicht inzage dossier

Bekijk hier welke externe zorgverlener informatie over uw dossier heeft ontvangen.

Datum informatieverzoek		06-01-2021	
Verwerker	Medewerker	Aanvrager	Client zelf
Soort informatieverzoek	Medisch Inhoudelijk (RVP)	Informatie verstrekt per	E-mail

[Print](#)

Snel naar
[Vaccinatieplanning](#)
[Privacy](#)
[Inzage dossier](#)

Service
[Contact](#)
[Volg het RIVM op Twitter](#)
[Volg het RIVM op Facebook](#)
[Volg het RIVM op LinkedIn](#)
[Volg het RIVM op YouTube](#)
[Volg het RIVM op Instagram](#)

Over deze website
[Cookies](#)
[Toegankelijkheid](#)
[WOB-verzoeken bij het RIVM](#)
[Copyright](#)
[Privacy](#)
[Uitschrijven bij MijnRIVM](#)

Meer informatie over
[Rijksvaccinatieprogramma](#)
[COVID vaccinatie](#)
[Vaccinaties op maat](#)
[Religieuze vaccinatie](#)
[Griepvaccinatie](#)

Talen
[English](#)
[Nederlands](#)

Inzage dossier pagina printbaar


Nederlands English

Inzage dossier

Uw vaccinatiegegevens zijn strikt vertrouwelijk. Een zorgverlener mag uw gegevens alleen indien als daar een medische reden voor is.

Persoonsgegevens

Voornaam	Gebortedatum
Tussenvoegsel	13-12-1963
Achternaam	Geslacht
Cp Cypress 1	Man

Overzicht inzage dossier

Bekijk hier welke externe zorgverlener informatie over uw dossier heeft ontvangen.

Datum informatieverzoek		06-01-2021	
Verwerker	Medewerker	Aanvrager	Client zelf
Soort informatieverzoek	Medisch Inhoudelijk (RVP)	Informatie verstrekt per	E-mail

DISCLAIMER

Dit is een vaccinatie dossier van het RIVM. De gegevens die hierin staan zijn verstrekt door de zorgverlener (GGD, huisarts of ziekenhuis). U heeft hiervoor toestemming gegeven. Lees meer over uw vaccinatie registratie en uw privacy: <https://www.rivm.nl/covid-19-vaccinatie/privacy>

Bijlage 2: Concept-persbericht MijnRIVM.nl**Vaccinatiegegevens COVID-19 na toestemming op Mijn.RIVM**

Iedereen die toestemming heeft gegeven voor het delen van vaccinatiegegevens met het RIVM, kan deze bekijken via mijn.rivm.nl. Via deze website kunnen mensen met hun DigiD de vaccinatiegegevens die het RIVM van hen heeft, zien. Iedereen kan dus zijn of haar gegevens over de ontvangen coronavaccinatie(s) terugvinden, wanneer er toestemming is gegeven voor het registreren van die vaccinatiegegevens. De eerste versie van Mijn.RIVM staat sinds begin april 2021 online.

Mijn.RIVM laat alleen vaccinatiegegevens COVID-19 zien van Nederlanders die uitdrukkelijk toestemming hebben gegeven om deze gegevens te delen met het RIVM. Na toestemming geeft de organisatie (o.a. GGD, instelling, ziekenhuis of de huisarts) die de vaccinatie geeft, gegevens over de vaccinatie door aan het RIVM. Na verwerking staan de vaccinatiegegevens in een persoonlijk vaccinatieoverzicht. Dit overzicht is geen officieel vaccinatiebewijs. Voor mensen die geen toestemming hebben gegeven, laat Mijn.RIVM zien dat er geen gegevens over de vaccinatie zijn.

Geen vaccinatie of geen toestemming, toch gegevens

Om gegevens van individuen te koppelen aan de vaccinatieregistratiegegevens gebruikt het RIVM persoonsgegevens uit de Basisregistratie Personen (BRP). Dit gaat om o.a. de namen en geboortedata van Nederlanders. Het RIVM heeft deze gegevens nodig voor de uitvoering van het vaccinatieprogramma, bijvoorbeeld om mensen een uitnodiging te sturen. Er is voor het gebruik van deze gegevens een wettelijke grondslag. Mensen die nog geen vaccinatie hebben ontvangen en aan wie dus ook nog geen toestemming is gevraagd, hebben via DigiD ook al toegang tot Mijn.RIVM.nl.

Wat doet het RIVM met de gegevens?

De landelijke registratie van vaccinatiegegevens is belangrijk. Het RIVM gebruikt de informatie over de coronavaccinatie voor onderzoek om te kijken of de vaccins goed werken, eventuele bijsturing van de vaccinatiecampagne en voor aanlevering van batchnummers als Bijwerkingencentrum Lareb daar om vraagt. Ook kunnen mensen bijvoorbeeld snel worden gewaarschuwd bij bijwerkingen.

Op grond van de wet bewaart het RIVM vaccinatiegegevens in principe 20 jaar. Mensen kunnen de gegevens altijd laten verwijderen via de webformulieren. Deze mogelijkheid is wettelijk vastgelegd in de wet AVG.

Bijlage 3: Use Case *self service* verwerking AVG-rechten**Doel**

Het doel van de "*self service*" is om de mogelijkheid te geven aan betrokkenen om zelf de AVG-rechten uit te voeren. Dus AVG-rechten uitvoeren zonder tussenkomst van personen bij RIVM. *Self service* is een aanvulling op de RIVM-procedure voor AVG-rechten en *NIET* in plaats van. Het automatiseren van AVG-rechten levert veel tijdswinst op in de uitvoerende processen in de DVP-regio's en maakt het proces ook minder foutgevoelig. De AVG-rechten zijn:

1. Recht op inzage. Buiten scope van de self service. Dit recht is reeds gegeven via mijn.rivm.nl/vaccinaties;
2. Recht op rectificatie/ wijziging van gegevens;
3. Recht op vergetelheid;
4. Recht van bezwaar;
5. Recht op beperking van de verwerking;
6. Afzien van deelname aan coronavaccinatie.

Voorwaarden

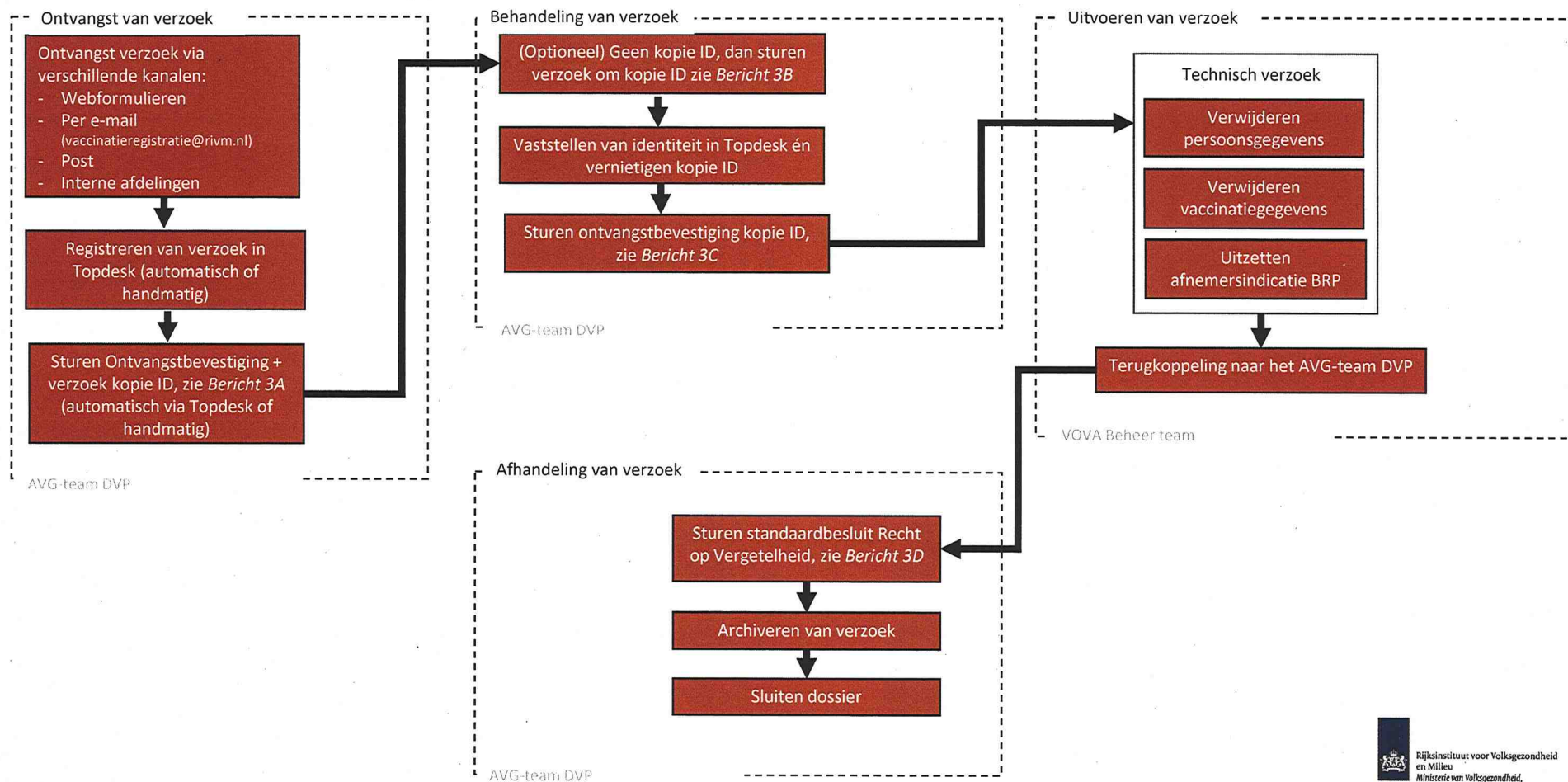
1. Unieke identificatie van de cliënt met DigiD of eHerkenning.
2. Webformulieren die gemakkelijk te vinden zijn door de cliënten.

Vervolgstappen:

1. Compliance-analyse (mag dit?).
2. Verkenning welke partijen binnen de Rijksoverheid hier al ervaring mee hebben en wat de lessen zijn.
3. Recht op bezwaar heroverwegen¹.
4. Herontwerp van de webformulieren, z.d.d.:
 - a. Per dataveld nieuwe inhoud door de cliënt kan worden ingevoerd;
 - b. Het webformulier kan worden "ondertekend/ bevestigd" met DigiD;
 - c. Het webformulier wordt verstuurd naar RIVM;
 - d. Het webformulier wordt (beveiligd) wordt gearchiveerd t.b.v. audits.
5. Indien het formulier met DigiD is "ondertekend/ bevestigd":
 - a. Automatische verwerking van de wijziging. Dit is een change die zorgvuldig moet worden voorbereid!
6. Indien het formulier NIET met DigiD is "ondertekend/ bevestigd":
 - a. Verwerking conform RIVM-procedure.
7. Uitgebreid gebruikersonderzoek om zeker te stellen dat de webformulieren voor de gehele doelgroep leesbaar, begrijpbaar en invulbaar zijn;
8. Belasting op de technische componenten in de gehele keten inschatten en componenten daar op dimensioneren;
9. DPIA aanpassen;
10. Informatiebeveiligingsmaatregelen aanpassen;
11. Ketentest, performancetest, gebruikerstest, acceptatietest, besluit livegang, livegang, beheer.

¹ VKA geeft aan dat "recht van bezwaar" niet van toepassing is.

Visualisatie 3. Recht op Vergetelheid Covid-19 vaccinatieprogramma





Rapportage Recht op vergetelheid

Gemaakt door [REDACTED] op 16 augustus 2021

Specificatie inhoud

Met filters:

- Van 01-04-2021 tot 16-08-2021
- Met selectie 'Meldingen Recht op Vergetelheid'
- Specificatie selectie:
 - Selecteer alle Tweedelijns meldingen
 - die als *Categorie* gelijk aan **AVG CIMS** hebben
 - en
 - die als *Subcategorie* gelijk aan **Recht op Vergetelheid** hebben

Met kengetallen:

- Aangemeld totaal
- Afgerond totaal

Met groepen:

- Veld 'Subcategorie'
- Veld 'Status'
- Periode 'Week'

**Rapportage Recht op vergetelheid**

Gemaakt door [REDACTED] op 16 augustus 2021

Subcategorie	Totaal	
	Aandemeld	Afgerond
<i>Recht op Vergetelheid</i>	34254	3116
<i>Totaal</i>	34254	3116