	Timeboxing/ Top 5 P risico's / 5 P risico's/ uitgangspunt concept DPIA versie 16.12.2020
1.	Het ontbreken van proces- en procedure beschrijvingen van lijnprocessen waardoor het toetsen van de privacy compliance in onvoldoende mate mogelijk
2.	(Technische) implementatie van de uitoefening van AVG rechten (wissing, rectificatie, inzage), alsmede het recht van bezwaar om in Vaccinatieregister COVID (nog langer) opgenomen te worden.
3.	Onvoldoende passende beveiligingsmaatregelen (zie top 5 IB risico's) vanwege BIO explains ook omdat niet is vastgesteld welke BBN maatregelen passen bij deze omvangrijke, impactvolle verwerking van gevoelige en bijzondere persoonsgegevens en unieke identificatienummers binnen de huidige context (dreigingsbeeld).
4.	Getroffen maatregelen enkel getoetst zijn op opzet en bestaan (dus niet op werking)

5.	Onvoldoende schriftelijk vastgelegde, niet functionele afspraken/eisen met partijen die gegevens aanleveren of afnemen, waardoor AVG compliance niet kan worden vastgesteld

Maatregelen
Een werkinstructie voor het weken met CIMS wordt opgesteld en vormt tevens trainingsmateriaal voor aan te stellen medewerkers. De basisfunctionaliteit volgens scope inrichting CIMS wordt door middel van de werkinstructie Werken met CIMS gecoverd. Na livegang worden waar noodzakelijk nieuwe procedures van kracht, op dit moment is er onvoldoende zicht op welke functionaliteit het eerste halfjaar van 2021 beschikbaar moet komen.
Instructies zijn beschikbaar als kopie van instructies voor het RVP. Deze instructies worden in januari nader toegespitst op de werking van CIMS, de te verwachten AVG-verzoeken. Door management wordt in de loop van januari al aandacht besteed aan het opschalen van capaciteit t.b.v. het kunnen beantwoorden van de verzoeken en het live brengen van de beschikbare procedures. Aparte awarenesssessies op basis van bestaande presentaties voor nieuwe medewerkers worden ingepland begin januari.
Op basis van de gehouden risicoanalyse is BBN gesteld op niveau 2 (departementaal vertrouwelijk). Voor BBN3 zijn op dit geen maatregelen beschikbaar (info van infospecialist). Quickscan CIMS geeft hier uitsluitsel over. Afhankelijkheid in het aansluiten van diplomatengegevens en gegevens van NATO-medewerkers. Mogelijk om de persoonsgegevens van diplomaten en NATO-medewerkers apart te registreren en te voorzien van juiste vaccinatiegegevens. Verscherping van controls op toegang en logging, Logging op administratorniveau vindt plaats bij toeganng tot de database. Elke administrator wordt met username gelogd. Dit geldt ook voor de Linux-beheerders. Beheerders kunnen niet bij de inhoud van een datafile, zien deze wel staan. Functioneel beheer CIMS krijgt rechten om zelf restore te doen, dan heeft databasebeheer daar geen bemoeienis mee. Encryptie is toegepast op de off site back up van de database in het datacenter. Er wordt nu, speciaal voor CIMS, een aparte off site back up ingeregeld met encryptie. De data tussen de applicatie en de SFTP server en database wordt getransporteerd conform encryptie protocollen TLS 1.0, 1.1 en 1.2. Er wordt overgegaan op TLS 1.2 en 1.0 wordt uitgefaseerd. Algemeen, gewerkt wordt conform de BIO-richtlijnen en de algemene architectuureisen Informatiebeveiliging volgens de NORA. VOG-screening technische medewerkers is standaard procedure binnen IV-organisatie.
De basis vormt Praeventis waar de maatregelen wel in place zijn. Een audit tijdens productie moet hier meer uitsluitsel over geven. Dit is in te plannen. Controls door zowel de IB-IV organisatie gebeurt standaard, evenals door functioneel beheer CIMS.

Diverse overeenkomsten met aanleverende partijen voor clientgegevens en vaccinatiegegevens achterhalen en beschikbaar stellen.

Documenten
Een werkinstructie werken met CIMS is in concept beschikbaar. Deze is gebaseerd op de werkinstructie werken met Praeventis.
In het worddocument DPV_CIMS_Overzicht procesdocumentatie CIMS privacy zijn gevraagde documenten opgenomen inclusief status
Document quickscan CIMS/risicoanalyse CIMS CIMS Backup en database encryptie_voorstel

Diverse overeenkomsten met aanleverende partijen zijn beschikbaar. GLO's ontbreken nog. Verwerkersovereenkomsten en samenwerkingsovereenkomsten met leverancier beschikbaar.

Actieplan
De werkinstructie wordt ingezet voor trainingdoeleinden en naslagwerk voor de regiomedewerkers betrokken bij de administratie in CIMS. Nadere analyse van benodigde CIMS-functionaliteit moet inzichtelijk maken welke procedures geschikt zijn om toe te passen of nieuw op te stellen. Procesowner CIMS in de lead, ondersteuning regelen door QA-medewerkers
Regiomanagers hierop bevragen en zorgen dat medewerkers getraind worden. Ook infopunt betrekken. Gezamenlijke activiteit met management, infopunt, FCC om dit na livegang in place te krijgen. Clientgegevens moeten verwijderd kunnen worden uit CIMS. Navraag bij Sandra hoe vast te stellen tot op welke hoogte gegevens verwijderd kunnen worden.
De risico analyses op CIMS zijn uitgevoerd tegen een BIO BBN 2 niveau van dataclassificatie. Voor data met een hogere classificatie is CIMS niet geschikt en zal dit ook moeilijk te maken zijn. Het advies is dan ook om uitsluitend met BBN2 data in CIMS te werken. En maatregelen conform BBN2(+) toe te passen. Er komt een aparte Check op de BIO-aspecten t.a.v. informatiebeveiligingsrisico's door 5.1.2e Vastgesteld moet worden of maatregelen toereikend zijn. Backup en restore maatregelen worden tussen IV-organisatie en Ordina verder besproken en vastgelegd. Daarbij speciale aandacht voor toegang en encryptie. Eisen gesteld aan monitoring en logging vanuit IB-plan verder oppakken en in beheer nemen. Beheeraudit na livegang laten plaatsvinden om inhoudelijke werking beheermaatregelen te toetsten.
Audit wordt ingepland in samenwerking met 5.1.2e. Dit zal na livegang plaats kunnen vinden.

GLO's moeten opgesteld worden met de desbetreffende aanleverende partijen uit het zorgveld. Verwerkersovereenkomsten waar nodig up to date maken, met name met leverancier van CIMS, COA.

Overzicht uit te voeren activiteiten t.b.v. livegang CIMS d.d. 30 december 2020		
Datum: 23 december 2020		
Nr.	**1. DPIA: kenmerken verwerking**	**Wie**
1.1	Vaststellen of de beschrijving van de "DPIA voorlopige definitieve" tekst akkoord is (scope)	5.1.2e , 5.1.2e
1.2	Beschrijving van ontbrekende processen	5.1.2e c.s
1.3	Verzamelen van (laatste versies van) procedures, SOP's e.d. maken van een overzicht daarvan	5.1.2e
1.4	Verzamelen en overzicht maken van meest recente afspraken met aanleverende partijen clientgegevens	5.1.2e
1.5	Verzamelen en overzicht maken van meest recente afspraken met aanleverende partijen van vaccinatiegegevens (aansluitvoorwaarden enz.)	5.1.2e
1.6	Schriftelijke afspraken Ordina maken (incl. adresseren van privacy compliance explains Ordina)	5.1.2e
1.7	Check of in DPIA genoemde gegevens ook klopt met gemaakte afspraken. Check of het gaat om minimale gegevensverwerking	VKA
1.8	Overzicht maken van de bestaande procesplaten/procesflows/dataflows	VKA, 5.1.2e , 5.1.2e

1.9	Voor zover correct, onderdeel uit laten maken van DPIA	VKA
1.10	Procesplaat aanleveren voor de publieksversie van de DPIA	5.1.2e
1.11	Check op de afspraken/overeenkomsten om de grootste (juridsiche) onvolkomenheden te inventariseren	VKA
1.12	Procedures rechten van betrokkenen opstellen	VKA
	2. Communicatie	
2.1	Informatieplicht	Communicatieplan publiek & communcatie zorgprofessionals aan te leveren door N. Troisfontaine c.s.
2.2	Oproepbrief checken	5.1.2e
2.3	Doeldocument LHV, Lareb, RIVM checken	
2.4	Document toestemming patiënt (client)	idem
2.5	RIVM site Privacy verklaring review van en in overeenstemming brengen met scope van verwerking CIMS release 1 en opvolgende releases	VKA
2.6	Alignment publicitaire uitingen RIVM site, Rijksoverheid e.d. met de (beoogde) scope & omvang verwerkingen van Vaccinatieregister	VKA
2.7	Concepttekst maken voor inschrijving in verwerkingenregister (conform AVG standaard)	VKA i.s.m. 5.1.2e
	3. Maatregelen in aanvulling op/overlap met IB	
3.1	Opschaling & procedure (organisatorisch) uitoefening rechten van betrokkenen AVG-RIVM mailbox, capaciteit FCC	DVP/FCC
3.2	Opschaling & procedures /SOPS(technische) AVG rechten (wissing, rectificatie, inzage enz.)	DVP-regiokantoren/Infopunt
3.3	Opschaling & procedures (& technisch regelen) wanneer burger bezwaar maakt tegen opname clientgegevens in CIMS	DVP

3.4	Opschaling & procedures voor handmatige invoer (dataverificatie bij input van zorgverleners)	DVP-BIS
3.5	Opschaling & procedure checken/ maken voor datalekken CIMS	DVP
3.6	Opschaling & procedure & procedure gegevensdeling RIVM-Lareb	DVP-BIS
3.7	Opschaling& procedure (afstemming van) informatieverschaffing infopunt DVP/klachten/AVG-RIVM mailbox	DVP/Infopunt
3.8	Vaststellen welke (genomen/te nemen) IB maatregelen in de risico-inventarisatie moet worden meegenomen zodat een IB risicoanalyse kan worden gedaan die aansluit op de beschreven kenmerken van de verwerkingen (zie onder 1.)	5.1.2e
3.9	Beschrijving maken van getroffen privacy controls	VKA
3.10	Procedure beschrijven en inregelen voor het valideren, aanpassen en bijwerken van de gegevens, zodat juistheid en volledigheid van de CIMS gegevens is geborgd	CIMS

3.11	Inzichtelijk maken waar in de processen wel/ geen maatregelen als veilige gegevensoverdracht, versleuteling en eindpuntbeveiliging is geregeld	CIMS
3.12	Identiteit en toegangsbeheer in opzet en bestaan en werking	CIMS- 5.1.2e 5.1.2e
3.13	Inzichtelijk maken waar in de processen wel en geen registratie van toegang (logging & monitoring) is	CIMS
3.14	Beschrijving waarom er geen privacy by design is en welke privacy afwegingen hierin zijn gemaakt om toch te komen tot keuze kopie Praeventis	CIMS
3.15	Wijzigingsbeheer voor livegang inregelen en procedure opstellen IB&P adviseurs onderdeel van CAB	5.1.2e
3.16	Wijzigingsbeheer na livegang inregelen en procedure opstellen IB&P adviseurs onderdeel van CAB	

Status (Wie, wannneer, wat)
Update 23-12: Afhankelijk van laatste beschrijving door 5.1.2e
Update 23-12: Procesgang Lareb under construction, afhankelijk van te maken afspraken door betrokken RIVM-collega's. Processen t.a.v. AVG under construction, moeten worden verfijnd voor CIMS en komen op de roadmap doorontwikkeling CIMS per 01-01-2021
Update 23-12: er is een overzicht aangeleverd met daarin de processen en procedures zoals nu beschikbaar voor Praeventis, vertaald naar CIMS. Dit behoeft nadere verfijning, zie onder 1.2
Update 23-12 COA: verwerkersovereenkomst beschikbaar, GLO moet worden opgesteld Probas: aangeleverd d.d. 24-12. PIVA: navraag bij 5.1.2e BRP (incl. RNI): autorisatiebesluit
Update 23-12: Geen update beschikbaar. VZVZ-LSP: 5.1.2e E-Zorg: 5.1.2e GGD-GHOR: 5.1.2e Actiz: 5.1.2e ARBO: 5.1.2e Overige partijen:
Update 23-12: Nieuwe samenwerkingsovereenkomst inclusief beheerplan en SLA aangeleverd, is wel een conceptversie. Afspraak om een addendum op te stellen met daarin de actuele afspraken (geldend voor 01-01-2021) Mogelijk dat er geen verwerkersovereenkomst nodig is vanwege veranderende structuur in beheer en onderhoud.
Update: 23-12: 5.1.2e gaat hiermee aan de gang overeenkomstig opdrachtbeschrijving. Start 22-12
Update 23-12: Er is een overkoepelende procesplaat en presentatie beschikbaar (opsteller P. Thuis). Daarnaast zijn de nodige procesplaten opgeleverd. Er volgt nog een aparte sessie d.d. 23-12.

zie 1.8
Door extern bureau wordt de publieksversie opgesteld. Communicatie 5.1.2e wordt benaderd).
5.1.2e gaat hiermee aan de gang overeenkomstig opdrachtbeschrijving. Start 22-12
Update 23-12: Zie onder 1.2. Deze procedures behoeven een verfijning gerelateerd aan de werking van CIMS.

Kamerbrief afdoende (5.1.2e 21/12)
Done 5.1.2e 21/12)
Done 5.1.2e
Done 5.1.2e 21/12)
5.1.2e gaat hiermee aan de gang overeenkomstig opdrachtbeschrijving. Start 22-12
Privacycheck n.a.v. nieuwe release. 5.1.2e pakt dit met Communicatie op.
Voor 24-12 staat de verwerking CIMS in RIVMData; Geven aan 5.1.2e

Update 23-11: Aan management DVP is duidelijk gemaakt dat dit begin januari om een concreet plan vraagt. Inclusief te maken afspraken met FCC.
Er zijn al afspraken met 5.1.2e, verantwoordelijk voor Infopunt. SOP's in wording, worden ook meegenomen in training voor registratiemedewerkers. Script komen voor elk contactpunt/kanaal. Opschaling is managementverantwoordelijkheid.
Update 23-12: Desbetreffende procedure betreft Afzien van deelname en is omgevormd naar CIMS.

Update 24-12: Er is een overeenkomst met Lareb binnengekomen die nu gereviewd wordt door VKA. Er is geen sprake van handmatige invoer als het gaat om berichtgeving Lareb. De huidige procedure met Lareb blijft in stand en geldt ook voor CIMS. Dataverificatie vindt plaats op het moment van automatisch inlezen csv-bestanden. Dataverificatie vindt daarnaast handmatig plaats en kan leiden tot foutenlijsten. Afspraak is dat op dit moment er niks gebeurt met foutieve gegevens. Deze kunnen altijd worden uitgedraaid t.b.v. verder verwerking.
In scope voor eerste release CIMS. Er is een aparte procedure voor datalekken voor de 3 programma's RVP, NHS, PSIE. Oppakken van RVP-procedure meest standaard. Daarnaast een werkinstructie beschikbaar voor het registreren van datalekken in Topdesk door regiomedewerkers. Kan ingezet worden voor CIMS. Zie onder 3.2
Contact met Lareb verloopt via EPI, onderdeel LCI. Aanvraag gegevens door Lareb doorloopt dezelfde procedure als nu gangbaar is voor RVP. Beschrijving hiervan aangeleverd.
Gezamenlijk met 3.1 oppakken
Zie overzicht CIMS_Issue_actielijst P_IB v1.2 dat behandeld is in de stuurgroep. In de lijst worden de risico's gekoppeld aan privacycontrol
op te pakken door 5.1.2e, start 22-12
Update 23-11:Er zijn regels ingebouwd in de automatische verwerking uit csv-bestanden die bepalen of een vaccinatie geregistreerd kan worden (bv uitvoerdatum moet na de geboortedatum liggen, het chargenummer moet bekend zijn, enz.). De documentatie van deze regels ligt nog bij de ontwikkelaar. Daarnaast is er het proces van evaluatie door de CIMS-machine en de 'rode blokjes' lijst. De inrichting van de CIMS-machine heb ik deels beschreven

Aanleveren van gegevens door zorgprofessionals via beveiligde verbinding (e-Zorg) op de sftp-server binnen RIVM-IV Organisatie. Betreft een gesloten netwerk. Encryptieprotocol in place conform TLS1.1, wordt geupgrade naar TLS1.2. Indien aangeleverd via mail, dan is Zorgmail de standaard.
CIMS werkt niet anders dan Praeventis. Autorisatiematrix is opgesteld, procedure aanvraag en verwijderen rechten in place. Speciale toegangsrechten worden in kaart gebracht, controle vindt handmatig plaats. In januari wordt dit verder ingericht. Georget leading.
Behandeld in overzicht CIMS_Issue_actielijst P_IB v1.2, zie 3.8
Privacy by design principes opgenomen in PSA-CIMS. Bij keuze voor kopie Praeventis zijn de privacyoverwegingen niet meegenomen. Privacy officer is aangehaakt bij het live brengen van CIMSApart document voor dit besluit is aanwezig.
Aparte PL aangetrokken, 5.1.2e. Standaard wordt gewerkt conform huidige changeproces zoals dit is ingericht voor Praeventis.
Aparte PL aangetrokken, 5.1.2e. Standaard wordt gewerkt conform huidige changeproces zoals dit is ingericht voor Praeventis.

Output / Documenten (zie ook R:schijf)
Scope DPIA vastgesteld (zie Stuurgroep Covid Registratie op 11 dec. jl.)
Procesbeschrijvingen ontbrekende processen
Werkinstructies gebruik CIMS Analyse beschikbare procedures en werkinstructies voor Praeventis, toepasbaar maken voor CIMS.
Autorisatiebesluit BRP beschikbaar COA: verwerkersovereenkomst en GLO Probas: verwerkersovereenkomst en GLO PIVA: verwerkersovereenkomst en GLO
Aansluitvoorwaarden; DVP_161;
Contract Ordina per 1/1/2021 beschikbaar inclusief onderliggende documentatie t.b.v. beheer, service levelafspraken, overeenkomst beheer en onderhoud. Deze stukken ondertekend door beide partijen.
Memo
Procesplaten, procesflows, dataflows worden op de roadmap gezet t.b.v. verdere ontwikkeling en verfijning. Afhankelijk m.b.t. te maken afspraken aanleverende partijen.

Memo
Publieksversie vaccinatie wordt op de in te richten website geplaatst.
Memo
Uitgewerkte procedures en documentatie, gereviewd door Quality assurance DVP. Verplichting tot kennisname door medewerkers CIMS tijdens trainingsessies.

Kamerbrief
Memo
Memo
Memo
Memo
Memo
Memo

Roadmap doorontwikkeling en beheer CIMS
Opgeleverd wordt een roadmap met daarin de op te stellen procedures en werkinstructies voor CIMS. Procesbeschrijving datalekken in overleg met FCC, het standaard datalekkenprotocol wordt gevolgd geldend voor RIVM
Aparte procedure Indienen bezwaar opname in CIMS-register.

Beschrijving afhandelen foutenlijst: staat op de agenda voor de volgende sprint, week 52
Procedure aanmelden en verwerken datalekken CIMS
Gegevensuitwisseling Lareb-RIVM Covid19-vaccinatie registratie
Roadmap
CIMS_Issue_actielijst P_IB v1.2
Memo
Documentatie automatische verwerking csv-bestanden Document beschrijving CIMS-machine

Autorisatiematrix, rollen en rechten in CIMS Procedure aanvraag en verwijderen toegangsrechten
CIMS_Issue_actielijst P_IB v1.2
Besluitdocument kopie van Praeventis
CAB inrichting, mogelijk stuurgroep. Procesbeschrijving CAB, verantwoordelijkheden en besluitvorming
CAB inrichting: Procesbeschrijving CAB, verantwoordelijkheden en besluitvorming