Privacy risico's stand van zaken 21.9.2020 – in samenhang te lezen met PIA versie 16.9.2020 -

#	Risico	IB .	**GEADVISEERDE** Maatregelen	Impact	Kans	Omvang
1.	IB BEVINDINGEN 8.9.2020					
2.	Sessie kan worden overgenomen in een zgn. man in the middle attack		IB			
3.	In het aanmeldformulier voor het onderzoek is geen controle voor mens of een script de aanmelding invult. (IB bevinding 8.9)		Voorstel IB: gebruik Google Recaptcha P nog uit te zoeken risico's voor betrokkene NB: J&V heeft een PIA op Google geinitieerd; let op Freedom Act & Shrems II. P RISICO'S NOG T EBEPALEN			
4.	Er is geen onderhoudscontract met de leverancier (Ib Bevinding 8.9)		IB P Aandachtspunt. Er is geen Overeenkomst met de leverancier Coneno (overtreding artikel 28 lid 3 AVG). Dit kan leiden tot een boete van de toezichthouder en/of reputatieschade voor RIVM.			
5.	Wachtwoorden van deelnemers zijn onvoldoende beschermd (IB bevinding 8.9)		IB			
6.	Accounts van onderzoekers zijn niet gekoppeld aan IAM van RIVM zoals beschreven in de PSA (IB bevinding 8.9)		IB			
7.	Applicatie logs voldoen niet aan de BIO richtlijnen. (IB bevinding 8.9)		BIO art. 9.4.1. Maatregel Conformiteit AVG minimum eisen ? : CHECKEN door IB			
8.	Maatregelen."Het *wachtwoord moet 8 digits bevatten met tenminste 1 hoofdletter en 1 speciaal teken*"		Advies FCC/P BIO eis (9.4.3.1): 8 digits en complex van samenstelling. Dat is dit niet . Advies FCC/P: Aantal inlogpogingen maximeren op 10 en tijdstuur dat een account wordt geblokkeerd vastleggen.			
9.	PRIVACY BEVINDINGEN					
10.	Intrekken toestemming en afmelden voor onderzoek. Afzonderlijk inregelen op de Infectieradar.nl site		Inregelen op site			
11.	Opt in en opt out voor ontvangen Nieuwsbrief en wekelijkse email/ uitnodiging vragenlijst		Inregelen op de site			
12.	Privacy- en toestemmingsverklaring		Inregelen op de site Bij aanpassing verwerking (bijv. G Recaptcha; PIENTER enz.) daar op aanpassen.			
13.	PIA /Maatregelen. Service contract met leverancier. Coneno.		Afspraken maken met leverancier			

	Hoe luiden deze afspraken ? Is de software cf. PbD & SbD ontwikkeld ? Is duidelijk wat in opdracht/in Influenzanet is ontwikkeld en wat niet ? Waar begint "doorontwikkeling" Hoe zit het met de continuiteit van de leverancier ?					
13.	Hoe zit het met de emailbeveiliging.		Actie SSC Advies FCC/P Email-beveiliging (SPF,DMARK, DKIM conform NCSC Whitepaper ?			
14. A	Maatregelen. Authenticatie van deelnemers door username en wachtwoord (wordt multifactor genoemd) is het niet. NB: het gaat om bijzondere persoonsgegevens & gegevens over gezondheid van minderjarigen. Vanuit privacy perspectief risico Hoog. Vanuit IB is BNN 2 aangehouden. Daar is Vertrouwelijkheid om Midden gesteld.		Deelnemers hebben geen toegang tot eerder ingevulde vragenlijsten. Akkoord.			
15.	Maatregelen. *Uitvoeren pentest door onafhankelijke partij.*		Actie SSC FCC/P Advies: Worden er ook vulnerability scans gedraaid. HOLM/MOTIV ?			
16.	Maatregelen. Vercijferde verbinding vanuit de web-client met API's (TLS 2 of hoger)		Advies FFC/P Let ook op Cipher SUITES. Voldoe aan NCSC Whitepaper eisen.			
17.	(Art. 5 lid 1 sub b AVG) Onvoldoende welbepaalde, uitdrukkelijk omschreven doeleinden. Scope van het onderzoek is erg ruim. Ook huid, maag/darm infecties (zie PIA onder voorstel) Onder verwerkingen. *"Het doel van Infectieradar is om aan de hand van de ontvangen gegevens verspreiding van infectieziekten zo goed mogelijk te begrijpen (….) "*		Actie EPI /Scope van het onderzoek aanpassen. NB: bij wijziging/aanpassing vragenlijsten, (= aanpassing verwerking) opnieuw nagaan wat de impact er van is voor rechten en vrijheden van betrokkene (privacy risico's)			
18.	Art. 5 lid 1 sub b AVG) Verdere verwerking van de persoonsgegevens zonder dat daar toestemming voor is gegeven Onduidelijk is, of de door Infectieradar.nl verzamelde gegevens ook door onderzoekers PIENTER gebruikt gaan worden] *RIVM Infectieradar heeft een samenwerking met het PIENTER onderzoek wat ook wordt uitgevoerd door het*		Actie EPI /Verduidelijken. Bij aanpassing, privacy- en toestemmingsverklaring ook aanpassen.			

	*RIVM. Deelnemers aan PIENTER worden ook uitgenodigd om deel te nemen aan Infectieradar. Deze deelnemers worden op dezelfde manier uitgenodigd als de huidige gebruikers van Infectieradar. Het PIENTER team stuurt hiervoor een email/ID lijst naar systeem beheer.*Betekent dit dan ook dat onderzoekers van het PIENTER onderzoek toegang hebben tot (1) Infectieradar.nl gegevens van (1) PIENTER deelnemers, en (2) van andere dan PIENTER deelnemers ? Zo ja, PRIVACYVERKLARING HIER OP AANPASSEN én nagaan of de toestemming van PIENTER deelnemers toereikend is voor Infectieradar.nl verwerkingen		Wat betekent op dezelfde manier als de HUIDIGE gebruikers van Infectieradar ? Is dat de manier van vóór september (deze PIA) of conform de in deze PIA beschreven werkwijze ?			
18.	Deelnemers Infectieradar oud; Infectieradar nieuw; deelnemers PIENTER		Procedure EPI			
19.	Accountgegevens, ingevulde vragenlijsten en onderzoekgegevevens uit eerdere Infectieradar versies (met de toen toepasselijke privacyverklaring en toestemmingsverklaring), worden in huidige Infectieradar.nl samengevoegd.		Procedure EPI			
20.	Verwerkingen onder punt 6. Toegang van onderzoekers tot onderzoeksgegevens. Om welke onderzoekers gaat het ? Punt. 7 Infectieradar onderzoeksteam (de onderzoekers die toegang hebben tot de Infectieradar projectmap op de R: schijf)		Procedure EPI			
21.	Verwerkingen onder punt 9. Toegang onderzoekers tot R: schijf. "Toegang gelinkt aan het RIVM account en kent daarvoor een 2F authenticatie"		Procedure EPI			
22.	Verwerkingen 10. "*De huidige deelnemers van Infectieradar worden met een specifiek protocol uitgenodgd. De email en het huidige ID wordt ingelezen, en ze ontvangen een link om hun wachtwoord aan te passen. Wanneer ze gebruik maken van dez link, en meedoen wordt hun ID aan de onderzoeksgegevens toegevoegd".* Deelnemers oude Infectieradar hebben toestemming gegeven op basis van toen geldende privacyverklaring. Infectieradar nieuw, daar geldt een andere privacyverklaring e.d. voor		Procedure EPI			
23.	Verwerkingen 10. Dit protocol wordt ook gebruikt voor PIENTER deelnemers die aangeven ook mee te willen doen		Idem 22			

	met Infectieradar en toestemming geven om de Infectieradar data te laten analyseren door het PIENTER team, in samenhang met serologische gegevens.					
23.	Verwerkingen punt. 8 Identificatie deelnemer: emailadres (username) gecombineerd met een wachtwoord. NB: geen 2 F, code is geen extra factor omdat het op hetzelfde adres wordt verzonden.		Geen toegang deelnemer tot eerder ingevulde vragenlijsten. Geen dynamische vragenlijsten. Akkoord			
24.	Identificatie minderjaringen. Ouder/ wettelijk vertegenwoordiger kan vragenlijsten namens hen invullen.		Kinderen 0-16. Akkoord.			
25.	Gebruik Google Recaptcha. Onduidelijk welke gegevens waar worden verwerkt. Het gaat om in elk geval om browser- en gebruikersinformatie krijgt voor het reguliere onderzoekswerk toegang tot de onderzoeksgegevens De door Google verzamelde gegevens (zie hierboven en in de notitie Gebruiken van reCaptcha 20200916. Persoonsgegevens van Europese gebruikers mogen niet zomaar in de VS worden verwerkt, nu volgens het Europese Hof van Justitie, de VS de privacyrechten van Europeanen niet voldoende beschermt. Bovendien hebben de veiligheidsdiensten volgens het Europese Hof van Justitie in de VS te ruime toegang tot de gegevens (Freedom Act). Is er onderzoek gedaan naar alternatieven die minder vergaande inbreuk op de rechten en vrijheden van betrokkene doen dan de Google Recaptcha ? Wat zijn daar de uitkomsten van ? Waarom is uiteindelijk gekozen voor Google ? Hoe is die keus gemaakt in het licht van de privacyrisico's voor betrokkene ? NB: stuurt Google Recaptcha ook je google account mee naast browse en gebruiksgegevens		Nog uit te zoeken welk privacy impact Google Recaptcha heeft Eerder aangegeven dat privacy vriendelijker tooling de voorkeur heeft (bijv. F5/ Web Application Firewall).			
26.	Is ook vastgesteld welke browsers en welke devices worden ondersteund ?		Actie SSC			
27.	Bewaartermijn accountgegevens. Waarom worden deze pas		Procedure EPI			

	na 2 jaar van inactiviteit verwijderd					
27.	Het optreden van een inbreuk op de persoonlijke levenssfeer (of vergelijkbare inbreuken) van één of meerdere betrokkenen doordat **de binnen de verwerking geregistreerde persoonsgegevens worden misbruikt door een beheerder.** Dit kan leiden tot schade voor de betrokkene die moet worden vergoed of een boete van de toezichthouder en/of reputatieschade voor.		Geheimhoudingsverklaring en afleggen eed / belofte als medewerker van RIVM door de gebruikers en beheerders. Loggen alleen met RIVM account. (2F) én 4 ogen. AKKOORD	**Midden**; de vastgelegde (persoons)gegevens zijn van dien aard dat dit kan leiden tot een serieuze bedreiging voor de getroffen persoon of personen.		
28.	***De onderzoeker bepaalt wie toegang heeft tot de surveydata en tot de identificerende gegevens.*** Dit kan leiden tot onbegrip of onzekerheid bij de betrokkene over wat er met zijn gegevens gebeurt waardoor deze de gegevens wil laten **wissen of bij de toezichthouder een klacht indient of de publiciteit zoekt. Dit kan leiden tot een boete van de toezichthouder** en/of reputatieschade voor RIVM.		Procedure EPI	.		
29.	Technologische context waar de IB risico-analyse op is uitgevoerd omvat de applicatie en alle overige product- en technologische componenten die de kritieke gegevens ondersteunen zoals: a) terminal, netwerk en andere toegestane randapparatuur; b) besturingssysteem, configuratie en services; c) geautoriseerde communicatieverbindingen en -poorten; d) COTS en andere producten, zoals Database Management Systemen DBMS gebruikt door de applicatie en zijn technologische infrastructuur; e) kwalificaties en andere processen die verband houden met de technologische context; en f) producten die door de toepassing zijn beïnvloed of gebruikt.		Zie dit in samenhang met opmerking 39 Dit betreft in elk geval de aantoonbaarheid (art. 5 lid 2 AVG)	**Midden**; het is onvoldoende inzichtelijk in welke mate wordt voldaan aan de BIR2017-controls		

30.	**De onderzoeker kan zelf de vragenlijsten configureren**. Binnen de Verwerking worden **meer gegevens verzameld dan strikt noodzakelijk** (overtreding artikel 5 lid 1 sub c AVG). Dit kan leiden tot onbegrip of onzekerheid bij de betrokkene over wat er met zijn gegevens gebeurt waardoor deze de gegevens wil laten wissen of bij de toezichthouder een klacht indient of de publiciteit zoekt. Dit kan leiden tot een boete van de toezichthouder en/of reputatieschade voor RIVM.		Geheimhoudingsverklaring en afleggen eed / belofte als medewerker van RIVM door de onderzoeker EPI Procedure voor het wijzigen van vragenlijsten. Met als onderdeel een check op privacy risico's.		.	
31.	***De onderzoeker verandert de vragenlijsten dan wel verrijkt de data set zodanig dat er geen sprake meer is van pseudonimisering dat het initieel vastgestelde beveiligingsniveau niet toereikend is*** **(art. 24 AVG).** Dit kan leiden tot een boete van de toezichthouder en/of reputatieschade voor RIVM. ***(art.*** **XX WPG**) niet voldaan aan de aan deze verwerkingsgrondslag gestelde eis		Procedure wijzigen dataset/verwerking			
32.	***Een betrokkene kan middels een beroep op de rechten van betrokkenen een verzoek indienen om de gegevens in te zien, te rectificeren en/of te wissen (overtreding Hfdst III AVG).*** Als niet adequaat aan dit verzoek gehoor wordt gegeven, kan de betrokkene dit melden aan de toezichthouder en/of de publiciteit opzoeken hetgeen kan leiden tot een boete voor RIVM (opgelegd door de toezichthouder) en/of reputatieschade voor RIVM.		Op de privacy-pagina van RIVM[1] is vermeld hoe een verzoek kan worden ingediend. Akkoord. EPI Procedure hoe dit feitelijk zal worden uitgevoerd			
33.	***Een AVG-verzoek op basis van de rechten van betrokkenen wordt niet of niet tijdig afgehandeld*** (overtreding artikel 12 lid 3 AVG). Dit kan leiden tot een boete van de toezichthouder en/of reputatieschade voor RIVM.		Procedure centraal is ingeregeld. EPI Procedure EPI opstellen/ inregelen. Een register wordt – centraal bij FCC/P bijgehouden voor de registratie en afhandeling van de AVG-verzoeken. Hierop vindt door FCC/P voortgangsbewaking plaats.	**Midden**; gezien de omvang van het aantal verwerkinge n (grootschalig) en de set van gegevens die worden		

[1]

				verwerkt.		
33.	*Een datalek binnen de Verwerking en/of het Informatiesysteem wordt niet gesignaleerd (overtreding artikel 33 AVG).* Als gevolg daarvan kan het datalek voortduren en worden er geen maatregelen genomen om het datalek te dichten en om de gevolgen van het datalek te beperken. Dit kan leiden tot schade voor de betrokkene die moet worden vergoed of een boete van de toezichthouder en/of reputatieschade voor RIVM.		SSC Campus/Logging conform BIO (en IBD logging). AANTONEN ! Binnen de ICT infrastructuur zijn maatregelen genomen om eventuele datalekken te detecteren.. De medewerkers zijn o.a. via Intranet geïnformeerd over het fenomeen datalek en hoe een datalek gemeld moeten worden.	**Midden**; de gehanteerde (persoons)gegevens zijn van dien aard dat dit zal leiden tot (grote) schade van de personen waarvan de gegevens worden gelekt. Qua reputatieschade is dit wel een punt van aandacht: immers elk datalek van een overheidsorganisatie kan in de publiciteit onder het vergrootglas worden gelegd..	**Midden**; gezien de beveiligingsmaatregelen en het bewustzijn van de medewerkers.	
34.	***Een datalek binnen de Verwerking of de gebruikte informatiesystemen wordt niet gemeld of de melding wordt niet correct afgehandeld (overtreding artikel 33 AVG).*** Dit kan leiden tot een boete van de toezichthouder en/of reputatieschade voor RIVM. Dit kan leiden tot schade voor de betrokkene die moet worden vergoed of een boete		De procesbeschrijving Datalekken wordt door CIO office toegepast voor het afhandelen van datalekken. De beoordeling van dit risico valt daarmee buiten de scope van deze DPIA. De medewerkers zijn o.a. via het Intranet geïnformeerd over het fenomeen datalek en hoe een datalek gemeld moeten worden.	Zie Risicobeheersing CISO office.	Zie Risicobeheersing CIO office.	

	van de toezichthouder en/of reputatieschade voor RIVM.					
34.	***De handhaving van de bewaartermijnen is (nog) niet geïmplementeerd binnen de Verwerking of het informatiesysteem*** (overtreding artikel 5 lid 1 sub e AVG). Dit kan leiden tot een boete van de toezichthouder en/of reputatieschade voor RIVM.		EPI/ procedure bewaartermijnen	**Laag**; het langer bewaren van de gegevens is niet of slechts in beperkte mate van invloed op de persoonlijke levenssfeer of andere rechten van de betrokkene.	**Midden**; er wordt niet voldaan aan een wettelijke verplichting dus bij een eventuele controle van de toezichthouder kan dit naar voren komen.	
35.	*Binnen RIVM zijn de daarvoor in aanmerking komende BiO-controls geduid als 'privacy-relevant'.* Indien het gebruikte Informatiesysteem niet voldoet aan één of meerdere van deze controls kan dit leiden tot een inbreuk op de beveiliging (hetgeen kan leiden tot een datalek), een boete van de toezichthouder en/of reputatieschade (overtreding artikel 25 lid 1 AVG).		ACTIE SSC Binnen de fit/gap-analyse zoals die is uitgevoerd voor <naam> in <jaar> is bepaald aan welke BIO-controls wel of niet wordt voldaan. Met uitzondering van de volgende normen wordt voldaan aan de privacy-relevante BIO controls: a. @@opsomming middels het beschrijving van de controls/clusteren indien mogelijk. Zie risicobeheersing CIO-O BIJZONDER AANDACHTSPUNT LOGGING & MONITORING CONFORM BIO !!!!!!!!!!!!	**Midden**; het is onvoldoende inzichtelijk in welke mate wordt voldaan aan de BIO2017-controls	**Midden:** (1) gezien het aantal en de aard van de ontbrekende controls en (2) de grote hoeveel	