Ministerie van Volksgezondheid,
Welzijn en Sport

Programmadirectie COVID 19

Secretaris Generaal / plv. Secretaris Generaal
Directie Wetgeving en Juridische Zaken
5.1.2e5j1.2e

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 5.1.2e
F 5.1.2e

www.rijksoverheid.nl

Inlichtingen bij
5.1.2e
5.1.2e
T 5.1.2e
M 5.1.2c
5.1.2e @minvws.nl

Datum
27 september 2020

Aantal pagina's
5

memo

Appreciatie juridische aspecten Saltro

Aanleiding

Saltro/Unilabs heeft op 25/9 verschillende gegevens aangeleverd. Dit betreft onder meer:

- Interne data protection governance van Unilabs. Dit betreft het interne privacy beleid, maar geen goedgekeurde binding corporate rules.
- Verwerkersovereenkomst tussen Saltro en de GGD utrecht.
- Een mailwisseling met Bird en Bird aangaande de privacywetgeving in de 5.1.2a
- Brief van Saltro met een beschrijving van hetgeen zij allemaal aan privacy maatregelen hebben genomen en een voorstel tot een oplossing voor het risico van toegang door de autoriteiten in 5.1.2a (een internationale overeenkomst tussen, waarbij regeringen medeondertekenen).

Appreciatie privacy aspecten

1. Als de minister besluit om de deal door te zetten
2. Dan is het noodzakelijk extra maatregelen overeen te komen bovenop het modelcontract voor doorgifte. Nu door Bird en Bird is aangegeven dat de 5.1.2a geen data protectie wetgeving en geen toezichthouder kent op het gebied van privacy, is er geen sprake van een vergelijkbaar regime danwel een vangnet met basisregels op privacy gebied.
3. Dit manifesteert zich ook in het feit dat de 5.1.2a autoriteiten de bevoegdheid hebben zich toegang te verschaffen tot alle lokaal beschikbare gegevens, zonder dat dit risico kan worden afgedekt (=restrisico)

Autoriteiten (risico kan niet worden afgedekt)

Gezien de huidige wetgeving hebben de autoriteiten in 5.1.2a juridisch de bevoegdheid om toegang te krijgen tot de in de 5.1.2a verwerkte gegevens. Dit risico kan niet worden afgedekt. Het risico van toegang door autoriteiten kan ook niet worden afgedekt door genomen en te nemen IT-security maatregelen. Dit wordt ook bevestigd door Bird en Bird en er blijft dus een aanzienlijk restrisico, dat contractueel niet gemitigeerd kan worden. Dit was ook een van de issues waarover het Europees Hof van justitie zich in de zaak Schrems II heeft uitgelaten en waardoor persoonsgegevens niet meer mogen worden doorgegeven aan bijvoorbeeld de VS.

Contractueel kan overeen gekomen worden:

- Unilab 5.1.2a dient per ommegaande melding te maken aan Saltro (en Saltro aan VWS) van alle bindende verzoeken van autoriteten voor verstreken van materiaal of data.
- Dat Unilab 5.1.2a zich moet onthouden van het verstrekken van persoonsgegevens en/of genetisch materiaal aan de autoriteiten.
- In ieder geval totdat ze daar in hoogste instantie toe veroordeeld/gehouden zijn.

Secretaris Generaal / plv. Secretaris Generaal
Directie Wetgeving en Juridische Zaken
5.1.2e

Datum
25 september 2020

Voorgaande maatregelen bieden echter onvoldoende soelaas. . Het hof stelt immers in de zaak Schrems II dat rekening gehouden moet worden met zowel de contractuele bepalingen die zijn overeengekomen als, in hoeverre de overheidsinstanties van dat derde land toegang tot de doorgegeven gegevens kunnen krijgen gezien de relevante aspecten van het rechtsstelsel van dat land.

Internationale overeenkomst geen directe oplossing
Saltro stelt voor om een bilaterale overeenkomst te sluiten, waarbij de regering van Nederland en 5.1.2a ook mede ondertekenen. Doel is dan dat het schenden van de afspraken ook internationaal rechtelijke consequenties heeft. Dit traject vergt nog veel uitzoekwerk vanuit juridisch oogpunt, dat dient te worden gecheckt bij BuZa:

- Zeer waarschijnlijk kwalificeren dergelijke afspraken als een verdrag. Een verdrag kan een instrument zijn voor doorgifte conform artikel 46, tweede lid onder a AVG, Echter dit instrument is bedoeld voor doorgifte tussen overheidsorganen. Daar is hier geen sprake van.
- Bovendien zullen ook niet snel afspraken kunnen worden gemaakt die voldoen aan de standaarden die de EDPB aan een dergelijk instrument stelt.[1] Met enkel diplomatieke afspraken kan vanuit privacy optiek het restrisico niet worden afgedekt.
- Het feit dat er een verdrag gesloten wordt betekent dat er ook allerhande procedures gelden, waaronder wellicht goedkeuring door het parlement.[2]

NB Overleg met BuZa is cruciaal. Zij heeft expertise op dit gebied.

Mogelijke extra maatregelen die contractueel af te dekken zijn
Wel kunnen contractueel op andere vlakken extra waarborgen worden ingebouwd. Naar aanleiding van de uitspraak Schrems II is het noodzakelijk extra waarborgen op te nemen in aanvulling op het bestaande modelcontract voor gegevensuitwisseling met derde landen. Recent gaf een Duitse gegevensbeschermingsautoriteit (van Baden-Württemberg) als eerste meer concrete richtlijnen over hoe om te gaan met de uitspraak in deze context.[3]Mede op basis van deze uitwerking kom ik tot de volgende extra maatregelen:

IT Veiligheid

- Ten eerste de **encryptie (versleuteling)** van de gegevens aan de Nederlandse kant erg belangrijk. Zorg er in dat geval voor dat aan de Nederlandse kant de partij de enige is met een 'sleutel' om de gegevens te ontcijferen en dat de encryptie niet zomaar kan worden ontsleuteld. Gebruik hiervoor een TTP.
- Ten tweede **pseudonimisering** van de gegevens. Zorg ervoor dat Unilabs Abu Dhabi niet zomaar kan weten over wie het nu werkelijk gaat. Dit gebeurt door codering van het materiaal.
- Ten derde betreft dit een **Beveiligde verbinding (VPN).** In de brief van Saltro wordt een dergelijke verbinding ook benoemd. Dus neem dit ook op in de overeenkomst. Het betreft dan het feit dat Saltro voor de verwerking van de materialen in Unilabs 5.1.2a tussen Saltro en Unilabs 5.1.2a

[1] Guidelines 2/2020 EDPB, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v1.pdf
Een dergelijk verdrag dient afdwingbare waarborgen inzake privacybescherming te bevatten inclusief toezichtmechanisme. Denk ook aan het falen van de afspraken tussen de EC en de VS inzake privacy shield.
[2] Artikel 7 van de goedkeuringswet bepaalt in welke gevallen we geen parlementaire goedkeuring hoeven te vragen.
[3] https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/Orientierungshilfe-Was-jetzt-in-Sachen-internationaler-Datentransfer.pdf

Secretaris Generaal / plv. Secretaris Generaal
Directie Wetgeving en Juridische Zaken
5.1.2e

Datum
25 september 2020

5.1.2a een beveiligde dataconnectie gebruikt, een zogenaamde VPN, te hebben.
- Ten Vierde gaat het om **het waarborgen van geen koppeling tussen systemen.** Het gaat dan om het feit dat er geen koppeling bestaat tussen het LIS systeem van Unilabs 5.1.2a het systeem van Saltro en Coron IT. Kan er bijvoorbeeld gewerkt worden met een soort dropbox, waardoor de gegevens niet in directe verbinding/koppeling geleverd worden?
- Ten vijfde betreft dit de **Locatie en monitoring server**
  Server buiten 5.1.2e mogelijk? Waar staat de centrale server? Kan van daaruit gemonitord worden of het systeem misbruikt wordt.
- Bewijs van **Audit** op IT veiligheid/ISO certificering.

Wellicht zijn er meer maatregelen in te bouwen aangaande veiligheid (dit dient te worden gecheckt bij Buza aangaande mobiele posten voor visa).

Veiligheid algemeen
- Ten eerste dat Saltro/Unilab zich verplicht **zelfstandig te melden** als zij denken dat veiligheid niet gewaarborgd is, danwel de verwerking stopzetten als dit aan de orde is en het geven van een bericht niet direct mogelijk is.
- Werken **conform de privacy governance** en eens in de X periode bewijs van een audit.

Vrijwaring voor claims/schade van derde partijen, veroorzaakt door Unilabs

Overige aanvullingen
Vervolgens stelt de gegevensbeschermingsautoriteit van Baden-Württemberg een aantal concrete aanpassingen en aanvullingen voor op het modelcontract[4] die we ook in dit geval moeten opnemen:

- Een verplichting voor de gegevensexporteur om de betrokkene te informeren dat zijn of haar gegevens naar een derde land gaan dat geen passend beschermingsniveau biedt;
- Een verplichting voor de gegevensimporteur om zowel de exporteur als de betrokkene op de hoogte te brengen van elk verzoek tot inzage van de gegevens. Als dit niet mogelijk is, de verplichting om de nationale gegevensbeschermingsautoriteit van de exporteur hiervan op de hoogte te brengen;
- Een verplichting voor de gegevensimporteur om juridische stappen te nemen tegen elk verzoek om inzage en deze uit te putten;
- De toekenning van meer rechten aan de betrokkene in een geschil met de gegevensimporteur
- De toevoeging van een compensatieclausule.

Omgang met materiaal/kwaliteit
Ook ten aanzien van de omgang met het materiaal en de labkwaliteit zullen eisen moeten worden gesteld.
- Ten aanzien van de omgang met het materiaal is het belangrijk vast te stellen dat de vergunningplicht uit de WVKL (artikel 7) niet van toepassing is. Echter, er zullen wel voorwaarden dienen te worden gesteld aan de omgang met materiaal (kijk hierbij naar de richtlijn 2004/23/eg).
- Vernietiging van het materiaal na testen en de bevestiging van die vernietiging periodiek verstrekken.
- een verbod tot gebruik voor andere doelen.
- Laboratoriumkwaliteit

NB Hierbij zal het RIVM kunnen helpen te bepalen welke voorwaarden noodzakelijk zijn.

[4] Deze zijn gericht op de VS, maar kunnen ons ook helpen.

Secretaris Generaal / plv. Secretaris Generaal
Directie Wetgeving en Juridische Zaken
5.1.2e

Datum
25 september 2020

Tot slot nog enkele opmerkingen over de verwerkingsgrondslag, het vraagstuk of toestemming van de betrokkene is vereist en de noodzakelijk PIA en security toets die moet worden gedan.

Grondslag
De grondslag voor de gegevensverwerking bestaat uit de geneeskundige behandelovereenkomst van de GGD met betrokkene (artikel 6, eerste lid onder b AVG). De betrokkene vraagt en ondergaat zelf de test en vraagt de diagnose aan. Daarmee valt het onder de geneeskundige behandelovereenkomst tussen de betrokkene en de GGD (- hulpverlener) om de test uit te voeren de noodzakelijke persoonsgegevens te verwerken. Betrokkene hoeft dus niet nog extra van tevoren bijvoorbeeld te tekenen om toestemming te geven. Voorts is van belang dat de (bijzondere) persoonsgegevens die worden verzameld ten behoeve van het testen, worden gebruikt om een epidemie van een infectieziekte te bestrijden. Dit is een publieke taak zoals in de Wet publieke gezondheid neergelegd. De GGD is volgens die wet verplicht bij dit soort ziektes gegevens vast te leggen, te controleren en op te volgen:

- Artikel 9, tweede lid, aanhef en onder h en i, AVG jo. artikel 6, eerste lid, aanhef en onder e, AVG bepaalt dat de verwerking van bijzondere gegevens (in dit geval gezondheidsgegevens) is toegestaan indien de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van volksgezondheid ter uitvoering van een publieke wettelijke taak. Voorwaarde is dat de verwerking is uitgewerkt in een Unierechtelijke of lidstatelijke bepaling waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van anderen (met name het beroepsgeheim). De Wet publieke gezondheid bevat dergelijke wettelijke grondslagen ter bescherming van zwaarwegende algemene belangen van volksgezondheid (Artikel 6, 28 en 29 Wpg; infectieziektebestrijding, registratie meldingen en doorsturen naar het RIVM).
- Voor de behandelrelatie tussen de te testen burger en de GGD-hulpverlener is ook een geheimhoudingsplicht geregeld. Daarmee is voldaan aan de verplichting uit de AVG dat dat bij de verwerking van persoonsgegevens ter bescherming van een zwaarwegend algemeen op het gebied van volksgezondheid het beroepsgeheim geborgd moet zijn.

Wel geldt er vanuit de AVG een informatieplicht die maakt dat betrokkene vooraf duidelijk en in heldere taal moeten worden geïnformeerd over wat er met zijn persoonsgegevens gebeurt. Dit betreft dus ook het feit dat de kans bestaat dat zijn test in 5.1.2a geanalyseerd wordt. Daarbij is de vraag te stellen of burgers dan nog steeds bereid zijn zich te laten testen. Tevens is de vraag of GGD 'n bereid zullen zijn de door haar afgenomen samples naar de 5.1.2a te sturen, omdat zij verwerkingsverantwoordelijke in de zin van de AVG zijn voor de verzending van het materiaal en de gegevens. Wanneer Saltro/Unilabs de analyse in 5.1.2a laat verrichten, functioneert dit lab in 5.1.2a als onderaannemer van Saltro en tevens als subverwerker van persoonsgegevens. De GGD dient voor deze subverwerking buiten de EU vooraf toestemming te geven.

PIA/voorafgaande raadpleging AP
Voorts dient er door VWS (en Saltro) een PIA gedaan te worden over de gehele keten, waarop de FG advies kan geven. Dit is een verplichting op grond van de AVG. Wanneer er een te groot restrisico geconstateerd wordt dat niet te mitigeren valt, is er een verplichting tot voorafgaande raadpleging van de AP (op grond van artikel 36 AVG). Dit betreft een formele beoordelingsprocedure door de AP, waarin de AP beslist of er ondanks het grote risico (al) gestart mag worden met de verwerking. Om dit risico te mitigeren, dient een zorgvuldige PIA gemaakt te worden.

Security
Op advies van de security officer, dient er een veiligheidstoets te worden gedaan. Voorwaardelijk is dat deze security toets (NCTV/BZK) is afgerond.

5.1.2e
5.1.2e

Secretaris Generaal / plv. Secretaris Generaal
Directie Wetgeving en Juridische Zaken
5.1.2e

Datum
25 september 2020