Ministerie van Volksgezondheid,
Welzijn en Sport

TER BESLISSING

Programmadirectie NC-19

Opgesteld door
5.1.2e
5.1.2e @minvws.nl

Datum
1 september 2021

Kenmerk

Uw kenmerk

Zaaknummer

Bijlage(n)
2

Deze nota is bedoeld om openbaar gemaakt te worden: ☐ **JA** ■ **NEE**

Aan 5.1.2e Deadline: 7 september 2021

nota

Akkoord gevraagd op levering van VWS-data aan Deloitte i.h.k.v. het aanvullend onderzoek naar de inkoop PBM

1. Aanleiding

In de kamerbrief van 18 juni heeft de minister voor Medische Zorg en Sport een aanvullend onderzoek toegezegd naar mogelijke onregelmatigheden bij de inkoop van Persoonlijke Beschermingsmiddelen (PBM). Dit onderzoek wordt uitgevoerd door Deloitte Forensic & Dispute Services B.V. (hierna: Deloitte). In deze kamerbrief heeft de Minister MZS aangegeven openheid over de gang van zaken van groot belang te vinden; in een aantal kamerdebatten heeft ze laten weten dat "de onderste steen boven moet komen". Deloitte heeft daarmee de opdracht om in drie fases alle signalen van mogelijke tekortkomingen bij afgesloten overeenkomsten te onderzoeken.
Deze nota bevat per geïdentificeerde databron een voorstel voor het leveren van de gevraagde data bij het VWS-concern, aan Deloitte; daar waar relevant komen ook de risico's aan de orde.

2. Geadviseerd besluit

- U wordt gevraagd per databron een besluit te nemen over welke data VWS-concern aan Deloitte zal leveren.
- U wordt voorts gevraagd of u wel of niet wil wachten tot de accreditatie voltooid is alvorens de data wordt geleverd.
-

Hierbij wordt u geadviseerd de onderstaande adviezen van de FG, CISO, CIO, WJZ mee te nemen.

3. Kernpunten

3.1 Vooraf

Deloitte heeft de voor het onderzoek binnen VWS 7 relevante databronnen geïnventariseerd en geïdentificeerd. Ook heeft Deloitte een inventarisatie gemaakt van welke personen bij de inkoop van PBM, in de periode van 1 januari 2020 t/m 1 juni 2021, betrokken zijn geweest. Drie van de databronnen zijn toe te wijzen aan een persoon (met aanduiding 'persoonlijk'), vier databronnen zijn van algemene, gemeenschappelijke, aard (met aanduiding 'algemeen'). Dit onderscheid is van belang omdat het in de rede ligt dat u aan VWS-concern medewerkers die beschikken over voor het onderzoek relevante persoonlijke databronnen een brief of e-mail stuurt waarin u hen gegeven de context van het onderzoek vraagt medewerking te verlenen aan het onderzoek (het weigeren van medewerking heeft geen arbeidsrechtelijke consequenties). Dit geldt ook voor

``

voormalige medewerkers en externen. Daarnaast is het van belang dat u de directeuren van de voor het onderzoek relevante directies informeert dat de algemene databronnen (gegeven de door u te nemen besluiten) aan Deloitte ter beschikking zullen worden gesteld.

VWS en Deloitte onderschrijven het uitgangspunt dat de onderzoekers van Deloitte over alle voor het onderzoek relevante informatie dienen te beschikken. Gegeven dit uitgangspunt is er bij een aantal van de door Deloitte geïdentificieerde databronnen een principiële vraag: wie maakt de selectie om te komen van de bruto- naar de nettodataset, waarbij een brutodataset een ongefilterde dataset betreft, die ook zeer waarschijnlijk data bevat van niet voor het onderzoek relevante onderwerpen of (bijzondere) persoonsgegevens van medewerkers en burgers:

- maakt VWS die selectie vòòr de data-overdracht aan Deloitte (dan is er volgens Deloitte geen sprake van onafhankelijk onderzoek en kan niet worden gegarandeerd dat de set relevante data compleet is (een reden hiervoor is dat VWS-concern over minder geavanceerde zoek-software beschikt dan Deloitte).
-
- maakt Deloitte die selectie (geautomatiseerd op basis van trefwoorden) na de data-overdracht door VWS (dan is er volgens de privacy-officers en de functionaris gegevensbescherming van VWS sprake van onrechtmatige verstrekking van persoonsgegevens aan Deloitte en onrechtmatige verwerking door Deloitte. VWS en Deloitte voldoen in dat geval niet aan de privacy wet- en regelgeving. In bijlage 1 bij deze nota geeft Deloitte aan hoe het proces van dataverwerking bij hen eruit ziet en dat zij gedurende het gehele proces maatregelen nemen die de privacy en vertrouwelijkheid van de verkregen gegevens borgen ("proportionaliteit" en "subsidiariteit"). WJZ merkt hierbij op dat ook de verstrekking door VWS dient te worden bezien, de werkwijze van Deloitte ontslaat VWS niet van haar eigen verantwoordelijkheid in dezen.

5.1.2e Concern merken hierbij op:
Het is nog onduidelijk waarom bij selectie vòòr de dataoverdracht aan Deloitte geen sprake zou zijn van onafhankelijk onderzoek. Mogelijkheden en waarborgen om onafhankelijk onderzoek wel te garanderen, zijn onvoldoende onderzocht, zoals:
- veilig stellen gebeurt in bijzijn van en op instructie van Deloitte
- inzet van andere forensische tooling
- inzet van een mogelijke stand-alone pc bij VWS

WJZ onderschrijft de opmerking van 5.1.2e en merkt op dat dat verstrekking van de gevraagde databronnen aan Deloitte alleen binnen de wettelijke kaders kan plaatsvinden, wat betekent dat een totale overheveling van alle bronnen (bruto) niet mogelijk is.
Er dient een nadere verkenning te worden gedaan van alternatieven waarbij er een inventarisatie en beoordeling van de in de bruto-dataset aanwezige bijzondere persoonsgegevens (van medewerkers of burgers) plaatsvindt voorafgaand aan verstrekking. Denk daarbij aan een selectie binnen VWS op een stand alone PC. De risico's vanuit privacy en security perspectief dienen hiertoe in kaart te worden gebracht om de afweging inzichtelijk te maken. Hiertoe dient een DPIA gedaan te worden.

NC-19 merkt hier bij op:
De hierboven genoemde opties zijn in het overleg met Deloitte besproken, maar stuiten op het bezwaar dat de zoekfuncties van de VWS-systemen beperkingen kennen en de zoek-software van Deloitte niet eenvoudig binnen de muren van VWS is te brengen. De kosten voor een onderzoeksomgeving (een stand-alone pc is een te simpele weergave van wat nodig is gezien de grote hoeveelheid data) binnen de muren van VWS opbouwen bedragen tussen de 150k en de 500k. Tevens vraag dit de nodige maanden aan ontwikkel- en doorlooptijd die ook een beslag zal leggen op de capaciteit van SSC-ICT.

3.2 Databronnen

De 7 databronnen worden nu separaat besproken:

1. Afdeling netwerkschijf en project netwerkschijf (G-schijf, O-schijf en P-schijf bij VWS-Concern), algemeen.

Voorstel programmadirectie NC-19 (1):
De bij het onderzoek betrokken directies (dit wordt nog bepaald) stellen alle documenten op de G-schijf, O-schijf en P-schijf zonder nadere selectie beschikbaar. Het is immers niet ondenkbaar dat er weliswaar mappen "inkoop PMB" zijn aangemaakt, maar dat onder tijdsdruk voor het onderzoek relevante documenten helaas toch in andere mappen zijn opgeslagen.

Risico's, met integraal de opmerkingen van 5.1.2e WJZ, 5.1.2e en BVA:

Opmerkingen 5.1.2e

In dit kader is ook de eerder door VWS opgestelde proportionaliteitstoets nog steeds relevant, zie bijlage 2 bij deze nota.

Opmerkingen WJZ

Alle data is door VWS veiliggesteld. Daarmee zou een selectie van data in eerste instantie moeten voldoen aan de onderzoeksvoorwaarden van Deloitte. Mocht er aanleiding zijn om diepergaand gericht (persoonsgericht)onderzoek te doen, dan kan deze data in tweede instantie beschikbaar gemaakt worden. Zie juridische haalbaarheid (onderdeel 4d van deze nota) voor juridische risico's en handelingsperspectief.

Opmerkingen 5.1.2e

De organisatie dient de risico's te verkennen en te benoemen. Onderstaande geldt voor alle bronnen.

Alvorens een besluit genomen kan worden dient inzichtelijk te zijn welke personen en hiermee de directies dit betreft. Zodat inzichtelijk kan worden welke privacyrisico's aan de orde zijn en hoe groot het vraagstuk ten aanzien van verstrekking betreft.

Denk bij de risico's **onder andere** aan:

Risico: Binnen de verwerking worden meer gegevens verzameld dan strikt noodzakelijk en gevoelig (overtreding art. 5 lid 1 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 op onrechtmatige verwerking of de publiciteit zoekt. Denk ook aan gegevens die meekomen bij verstrekking van alle documenten van de directie waarbij medewerker gestationeerd is. Dit kan leiden tot een boete van de toezichthouder en/of reputatieschade VWS.

Risico: Ongeoorloofde toegang door derden, bijv. door Deloitte.

Risico: De gegevens worden gedeeld met andere partijen (zoals Deloitte of nog weer anderen) zonder dat een wettelijke grondslag bestaat of dat dit is opgenomen als één van de doelen van de verwerking.

Risico: bij de verstrekking zullen tevens bijzondere persoonsgegevens die niet ter zaken dienend zijn worden verstrekt zonder dat een uitzondering op het verwerkingsverbod van gezondheidsgegevens toepasselijk zijn. Op basis van de AVG is het verwerken van bijzondere persoonsgegevens **verboden** tenzij dat je je kunt beroepen op een uitzondering in het tweede lid.

Het verkennen van alternatieven dient gezien de complexiteit door de organisatie (VWS) zelf te worden ingeschat/ uitgevoerd.

Alternatieve werkwijze zou kunnen zijn:
- Gelegenheid bieden tot het uitsluiten van bijzondere niet relevante persoonsgegevens, zoals ook bij een wob-proces hiervoor een tijdstermijn wordt gehanteerd. Al dan niet onder toezicht van onafhankelijk persoon/Deloitte (voorstel 1a)

<u>Opmerkingen BVA</u>

Het is aannemelijk dat er op de betreffende schijven bijzonder informatie is opgeslagen en dat deze bijzondere informatie als bruto-dataset aan Deloitte zal worden verstrekt. Voor wat betreft de beveiliging van bijzondere informatie zijn de volgende passages uit het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIR-BI) relevant:

- Artikel 3 (Beveiligingsbeleid), lid 1.c, Het beveiligingsbeleid dat door de secretaris-generaal wordt vastgesteld omvat ten minste de ministeriële uitgangspunten voor de beveiliging van, de toegang tot, het omgaan met en verwerken van bijzondere informatie zoals bedoeld in dit voorschrift en de wijze waarop *'de secretaris-generaal vooraf toestemming verleent voor het verwerken van bijzondere informatie'*.
- Artikel 6 (Eisen aan de Beveiliging), Lid 1.b, geeft aan dat bijzondere informatie zodanig beveiligd wordt dat 'inbreuken op de beveiliging worden gedetecteerd en gedegen onderzoek naar (mogelijke) inbreuken mogelijk is'.
- Artikel 7 (Buiten de Rijksdienst brengen van informatie), lid 1a, geeft aan dat bij het buiten de rijksdienst brengen van bijzondere informatie, anders de op grond van een wettelijke verplichting tot openbaarmaking, 'de eisen aan de beveiliging en het toezicht daarop onverkort van kracht' blijven.

``

Er is op dit moment geen door de CISO Kern opgestelde risicoanalyse beschikbaar van de Informatiesystemen van Deloitte waaruit blijkt dat voldaan kan worden aan de eisen zoals opgenomen in de artikelen 6 en 7 van het VIR-BI. Er blijkt niet dat na overdracht van de bijzondere informatie VWS haar toezichtrol kan (blijven) uitoefenen, inbreuken op beveiliging kan waarnemen en gedegen onderzoek kan doen. De risico's die hier uit voortvloeien dienen geaccepteerd te worden of er dienen aanvullende afspraken met Deloitte gemaakt te worden.

In de dienstverleningsovereenkomst met Deloitte (kenmerk 2846242), punt 6.1 (Artikel 8.1 wordt gewijzigd en krijgt de navolgende aanvulling), heeft 5.1.2e 5.1.2e al 'vooraf' toestemming aan Deloitte gegeven om de verstrekte bijzondere informatie te verwerken in Informatiesystemen. Aangegeven is 'daarnaast stemt Opdrachtgever ermee in dat Opdrachtnemer voor de uitvoering van de Diensten gebruik maakt van specialistische forensische technologie die Opdrachtnemer in licentie c.q. gebruik heeft'. Daarmee is voldaan aan Artikel 3 van het VIR-BI en is accreditatie overbodig omdat impliciet de (rest)risico's – die de CISO Kern nog moet beschrijven en vastleggen in een risicoanalyse – al geaccepteerd zijn.

De passage in de dienstverleningsovereenkomst met Deloitte (kenmerk 2846242): 'Opdrachtgever stemt ermee in dat Opdrachtnemer specifieke expertise inschakelt die is belegd in aan Opdrachtnemer gelieerde entiteiten (binnen de eigen groep van Opdrachtnemer)' levert als (rest)risico op dat bijzondere informatie van VWS in handen kan komen, gezien het feit dat Deloitte vestigingen in het buitenland heeft, van buitenlandse overheden. Er blijkt niet dat er bij Deloitte sprake is van compartimentering van data om te voorkomen dat een buitenlandse overheid, op basis van eigen nationale wetgeving, data kan vorderen. Dit risico dient ook transparant opgenomen te worden in de (nog) door de CISO Kern op te stellen risicoanalyse.

Kanttekening daarbij is dat VWS alle eigenaren van de bijzondere informatie die van andere departementen ontvangen zijn, en waar bij verstrekking uit is gegaan van de veronderstelling dat VWS zich aan artikel 6 en artikel 7 van het VIR-BI zou houden, dient te informeren over dit risico. Omdat er een bruto-dataset aan Deloitte verstrekt zal worden is ook niet duidelijk welke bijzondere informatie buiten de invloedsfeer van VWS – de rijksdienst – terecht zal komen. Dit is een (te accepteren) risico tenzij er een inventarisatie en beoordeling van de in de bruto-dataset aanwezige bijzondere informatie plaatsvindt voor verstrekking en er geen bijzondere informatie van andere departementen gevonden wordt.

Zoals hierboven al genoemd dient de 5.1.2e Kern een risicoanalyse op te stellen waarin aan 5.1.2e aangegeven wordt welke risico's zijn geaccepteerd met de dienstverleningsovereenkomst. En welke risico's verder een rol spelen.

Gevraagd besluit:
- Gaat u akkoord met voorstel 1 of met voorstel 1a? [n.b. indien er een alternatief voorstel is, is de check nodig of dit haalbaar is]

-

2.Samenwerkingsruimten (Intern en Extern), algemeen.

``

Voorstel NC-19 (2):
De bij het onderzoek betrokken directies (dit wordt nog bepaald) stellen de informatie op alle onder hun verantwoordelijkheid opgerichte interne en externe samenwerkingsruimtes zonder nadere selectie beschikbaar.

Risico's:
Opmerkingen gemaakt onder het kopje 'risico's bij punt 1 zijn ook veelal hier van toepassing.

Gevraagd besluit:
- Gaat u akkoord met voorstel 2?

3.Marjolein, algemeen

Voorstel NC-19 (3):
De bij het onderzoek betrokken directies (dit wordt nog bepaald) **stellen alle** marjolein-documenten die onder hun directie vallen ter beschikking met uitzondering van als "staatsgeheim" gerubriceerde informatie.

Risico's:
Opmerkingen gemaakt onder het kopje 'risico's bij punt 1 zijn ook veelal hier van toepassing.

Aanvullende opmerkingen BVA

> Staatsgeheime informatie mag niet in Marjolein verwerkt worden. Als deze informatie toch wordt aangetroffen door Deloitte dan is er sprake van een incident, en dit incident dient direct onder aandacht van de BVA te worden gebracht. De BVA kan geen opdrachten aan Deloitte geven voor het treffen van noodmaatregelen en de BVA kan ook geen onderzoek bij Deloitte uitvoeren naar de compromittering en de impact daarvan. Dit zal geaccepteerd moeten worden, inclusief het risico dat Deloitte het incident niet waarneemt en/of niet zal melden. Dit risico is te minimaliseren als er een inventarisatie en beoordeling van de in de bruto-dataset aanwezige bijzondere informatie plaatsvindt voor verstrekking.

Gevraagd besluit:
- Gaat u akkoord met voorstel 3?

4.E-mailboxen van medewerkers, persoonlijk.

Voorstel NC-19 (4):
Deloitte heeft reeds een inventarisatie gemaakt van bij het onderzoek betrokken personen. VWS zal uit deze lijst de medewerkers van VWS-concern selecteren (evenals voormalige VWS-medewerkers en door VWS ingehuurde externen die met een VWS-account gewerkt hebben). Zoals hiervoor al is aangegeven zult u deze medewerkers per brief vragen om medewerking te verlenen aan het onderzoek.
Na toestemming wordt de e-mailbox vervolgens zonder verdere selectie integraal beschikbaar gesteld aan Deloitte.
Bij door Deloitte als relevant aangemerkte dienstpostbussen, zal de eigenaar (contactpersoon?) van de dienstpostbus om toestemming worden gevraagd.

``

Risico's:
Opmerkingen gemaakt onder het kopje 'risico's bij punt 1 zijn ook veelal hier van toepassing.

Aanvullende opmerkingen van WJZ:

> Als de selectie van de lijst met medewerkers niet zorgvuldig afgewogen wordt, zal dit een aanzienlijk risico opleveren in het kader van de proportionaliteit. Indien het vooral sleutelfiguren of dossiereigenaars betreft is het risico aanzienlijk lager, aangezien deze reeds eerder in het kader van de Wob toegang hebben moeten verlenen. Het is nu niet duidelijk om hoeveel mensen het gaat en welke functie zij bekleden (en daarmee de hoeveelheid gegevens). Dit is noodzakelijk om te weten om een accurate afweging te maken.
> De omstandigheid dat vooraf toestemming wordt gevraag heeft eveneens een mitigerend effect. Toestemming in de gezagsverhouding werkgever en werknemer kan in principe alleen als de toestemming geweigerd kan worden zonder dat daar consequenties aan zijn verbonden (zie o.a. 3.1). Vanwege de gezagsverhouding tussen werkgever en werknemer is de eis uit de AVG dat de toestemming in vrijheid moet zijn gegeven altijd een discussiepunt in de arbeidsrechtelijke context.

Gevraagd besluit:
- Gaat u akkoord met voorstel 4?

-
-

5.Persoonlijke Netwerkschijf (H-schijf bij VWS-Kern), persoonlijk.

Voorstel NC-19 (5):
Zoals hiervoor en bij voorstel 4 al is aangegeven zult u de betreffende medewerkers per brief vragen om medewerking te verlenen aan het onderzoek. Na toestemming wordt de H-schijf met uitzondering van eventuele submappen die als "privé" zijn gelabeld zonder verdere selectie integraal beschikbaar gesteld aan Deloitte.

Risico's:
Opmerkingen gemaakt onder het kopje 'risico's' bij punt 1 zijn ook veelal hier van toepassing.

Aanvullende opmerking WJZ

> Het feit dat dit aanzienlijke aantallen bijzondere persoonsgegevens betreft, is overheveling van de schijf een risicoverzwarend element. Zeker als dat gebeurt zonder dat op een adequate manier alternatieven zijn onderzocht, zoals een twee traps systeem. Kan Deloitte bijvoorbeeld starten met het archiefsysteem (zoals Marjolein en Zylab) en vervolgens verder werken naar andere bronnen als dat noodzakelijk blijkt te zijn?

Aanvullende opmerking FG

> Goed om bij de vraag om toestemming aan te geven dat het weigeren van medewerking heeft geen arbeidsrechtelijke consequenties heeft. Mocht het gaande weg een persoonsgericht onderzoek worden dan kan een mogelijke toestemming wel een knelpunt worden.

Alternatieve werkwijze zou kunnen zijn:
- Bevriezing van de h-schijf, waarbij deze nog niet wordt overgedragen. Mocht hier naar aanleiding van het verloop van het onderzoek noodzaak toe blijken, dan kan Deloitte hier een gericht informatieverzoek toe doen (voorstel 5a).
- Een tussenstap kan zijn om de medewerker opdracht te geven om relevante documenten op de afdelingsschijven te plaatsen. In combinatie met het bevriezen van de H-schijven kan dan, indien aan de orde, later worden gereconstrueerd of relevante documenten niet op de afdelingsschijven zijn geplaatst (voorstel 5b).

Gevraagd besluit:
- Gaat u akkoord met voorstel 5 of voorstel 5a? [n.b. indien er een alternatief voorstel is, is de check nodig of dit haalbaar is]

6.Gegevens van mobiele telefoons, persoonlijk.

Voorstel NC-19 (6):
Deloitte krijgt toegang tot de reeds door NC19 veilig gestelde en door de gegevenseigenaar gevalideerde whatsappdata van mobiele telefoons van medewerkers. Het betreft hier data, die in een zorgvuldig en door de FG getoetst proces tot stand zijn gekomen. Deloitte kan verzoeken om de telefoon van een nader te bepalen medewerker nader uit te lezen wanneer daar in het onderzoek aanleiding toe blijkt. Dan zal opnieuw aan de betrokken medewerker toestemming worden gevraagd.

Risico's:
Dit proces is reeds zorgvuldig ingericht en afgestemd met de FG in het kader van de wob.

Gevraagd besluit:
- Gaat u akkoord met voorstel 6?

7.3F (financiële systeem), algemeen.

Voorstel NC-19 (7):
De directie FEZ heeft de door Deloitte gevraagde informatie gereed gezet. Deze stukken worden vervolgens zonder verdere selectie integraal beschikbaar gesteld aan Deloitte.

Risico's:
Opmerkingen gemaakt onder het kopje 'risico's bij punt 1 zijn ook deels ook hier van toepassing. Waarbij wordt aangetekend dat het de verwachting is dat er in het financiele systeem weinig persoonsgegevens staan opgeslagen.

Gevraagd besluit:
- Gaat u akkoord met voorstel 7?

3.3 Beveiliging en integriteit van de gegevens tijdens en na overdracht aan Deloitte

De afgelopen weken heeft intensief contact plaatsgevonden tussen VWS en Deloitte over de beveiliging van gegevens tijdens en na overdracht aan Deloitte en welke waarborgen Deloitte daarbij heeft ingeregeld.
Het is van belang dat Deloitte de data vanuit VWS verwerkt in een door de Rijksoverheid geaccrediteerd systeem om te kunnen voldoen aan de Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI). Daarnaast dient Deloitte zich te kunnen conformeren aan de Baseline Informatiebeveiliging Overheid (BIO).

VWS heeft de gegevensuitwisselingsovereenkomst en aanvullende informatie ontvangen, daarnaast zijn de beveiligingsmaatregelen toegelicht. De beschrijvingen zijn echt niet afgedekt door een audit of anderzijds een onafhankelijk onderzoek die de risico analyse kan ondersteunen. Een accreditatie is een vereiste om de data te mogen ontvangen, verwerken en na filtering en behandeling voor langere tijd op te slaan.

In de opdrachtverlening heeft 5.1.2e akkoord gegeven voor het verwerken van bijzondere gegevens door Deloitte. Deze accreditatie had daaraan vooraf moeten gaan, zodat dit meegenomen had kunnen worden in het advies aan 5.1.2e om wel of niet akkoord te gaan.

Voorstel is om alsnog de accreditatie rond te krijgen, maar verdere besluitvorming ten aanzien van de daadwerkelijke levering van data aan Deloitte hier niet door te laten ophouden. Dit, aangezien de accreditatie nog wel de nodige stappen en daarmee de nodige doorlooptijd kent.

Risico's (BVA)
Het restrisico dat bijzondere informatie bij statelijke actoren terecht komt, gezien de door de SG gegeven toestemming dat Opdrachtnemer (Deloitte) '*specifieke expertise inschakelt die is belegd in aan Opdrachtnemer gelieerde entiteiten (binnen de eigen groep van Opdrachtnemer). Daarnaast stemt Opdrachtgever ermee in dat Opdrachtnemer voor de uitvoering van de Diensten gebruik maakt van specialistische forensische technologie die Opdrachtnemer in licentie c.q. gebruik heeft*' kan niet door VWS geaccepteerd worden zonder afstemming met de Rijks BVA en toestemming van andere departementen die (deels) eigenaar van de informatie zijn. Het verstrekken van bijzondere informatie aan Deloitte, met de wetenschap dat deze verwerkt kan worden buiten de invloed sfeer van Nederland, kan een strafbaar feit opleveren (misdrijf) als het informatie van andere departementen is en deze departementen geen toestemming hebben gegeven om de gerubriceerde informatie (Dep V) binnen de (mogelijke) invloedsfeer van andere statelijke actoren te brengen. De departementen die eigenaar van informatie zijn mogen er vanuit gaan dat VWS de verplichtingen die uit het VIR-BI voortvloeien naleeft en geen toevoegingen op het ARVODI 2018 accepteert.
De aanpassing van het ARVODI, waardoor een inbreuk op beveiligingseisen voor bijzondere informatie is gemaakt, zal de BVA moeten melden bij de Rijks BVA.

3.4 Gegevensuitwisselingsovereenkomst

In een gegevensuitwisselingsovereenkomst worden de afspraken vastgelegd met betrekking tot de werkwijze van Deloitte ten aanzien van de door VWS aan

Deloitte ter beschikking gestelde data. Een deel van de inhoud van deze overeenkomst hangt af van de besluitvorming aangaande de datalevering. Deze gegevensuitwisselingsovereenkomst zal daarom t.z.t. apart aan u worden voorgelegd.

3.5 Zienswijze FG

De vraag is hoe de gegevensverstrekking van VWS aan Deloitte zich verhoudt tot het recht op bescherming van de persoonlijke levenssfeer van de (voormalige) bewindspersonen en (voormalige) ambtenaren als wel die van de burger[1].

Waarbij het zeer aannemelijk is dat de gegevensbronnen meer gegevens bevatten dan noodzakelijk zijn voor het onderzoek, waaronder bijzondere persoonsgegevens dan wel privégegevens (denk aan de mailboxen, h-schijf) en dat deze persoonsgegevens als bruto-dataset aan Deloitte zal worden verstrekt en hiermee buiten de omgeving en de verwerkingsverantwoordelijkheid van VWS wordt gebracht.

Het verzamelen, verwerken, en delen van informatie zijnde (bijzondere) persoonsgegevens tussen verschillende partijen is vanuit wetgeving alleen toegestaan met inachtneming van de beginselen van onder andere:

- verbod verwerking van bijzondere categorieën persoonsgegevens[2]
In beginsel is de verwerking van bijzondere persoonsgegevens verboden, tenzij een uitzondering in het tweede lid artikel 9 AVG van toepassing is. Daarbij moeten de gegevens noodzakelijk zijn om het doel te bereiken en mag er niet meer gegevens verwerkt worden dan strikt noodzakelijk. Het is onduidelijk op basis van welke doorbrekingsgrond verstrekking van bijzondere persoonsgegevens zijnde voor het onderzoek niet relevante informatie vertrekt worden aan derden.

- noodzakelijkheid, evenredigheid[3] en dataminimalisatie[4]; Dit komt op verschillende wijzen in de AVG tot uitdrukking, zoals met name bij de vereiste rechtsgrondslagen voor verwerking[5] en in de beginselen[6] van doelbinding, dataminimalisatie en opslagbeperking. Deze beginselen eisen dat de hoeveelheid persoonsgegevens én het aantal betrokken personen tot het noodzakelijke worden beperkt. Het is onduidelijk hoe de afweging is gemaakt
De gegevensverstrekking moet daarbij voorts de proportionaliteits- en subsidiariteitstoets kunnen doorstaan;

- proportionaliteit; De proportionaliteitsvraag betreft in de kern de afweging of de beperkingen van het recht op bescherming van persoonsgegevens en het doel dat met de verstrekking wordt beoogd voldoende met elkaar in balans zijn. Het is onduidelijk of deze proportionaliteitstoetsing is uitgevoerd.

---

[1] Denk hieraan burgerbrieven, klachten, claims, aansprakelijkheidsstellingen, schikkingen, maatregelen tegen medici die niet aan de het onderzoek gerelateerd zijn.
[2] artikel 9 AVG
[3] artikel 8, tweede lid EVRM
[4] artikel 5, eerste lid, onder c AVG
[5] artikel 6, eerste lid AVG
[6] artikel 5, eerste lid AVG

- **subsidiariteit;** de eis van subsidiariteit betreft de vraag of er geschikte alternatieven zijn waarmee het genoemde doel niet op een andere minder ingrijpende wijze kan worden bereikt. Het is onduidelijk of er alternatieven verkent zijn.

- **doelbinding**[7]**;** Het doelbindingsbeginsel brengt met zich mee dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens niet verder op een met die doeleinden onverenigbare wijze mogen worden verwerkt. Gelet op het beginsel van doelbinding zal moeten worden nagegaan of de verstrekking van de meer dan voor het onderzoek noodzakelijke gegevens welke tevens meekomen bij verstrekking van gehele directieschijven, gehele mailboxen ten behoeve van het feitenrelaas verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld.

Een situatie waarin (bijzondere) persoonsgegevens verstrekt worden aan derden terwijl dit niet noodzakelijk is, is niet verenigbaar met deze beginselen. En is daarmee onrechtmatig. Daarnaast ontbreken beperkingen en waarborgen op het delen van bijzondere persoonsgegevens welke meekomen bij de verstrekking in het voorstel. Dit gezien het voorstel om de bronnen na notificatie aan de medewerker zonder verdere uitsluiting van mogelijke niet ter zake dienende bijzondere persoonsgegevens beschikbaar te stellen. Denk hierbij bijvoorbeeld aan gegevens als informatie-uitwisselingen met bedrijfsarts, als wel gegevens die mogelijke op de directie schijf staan en met name van de directies waarbij een medewerker die betrokken is geweest bij het inkoopproces maar bij een ander directie gesitueerd was. Waardoor informatie van andere werkzaamheden van de betreffende directie van de medewerker ook worden verstrekt.

Het advies is om alternatieven en waarborgen te verkennen waarbij niet ter zake dienende bijzondere persoonsgegevens en privégegevens voor de verstrekking uitgesloten kunnen worden.

Het is onduidelijk hoe de afweging is gemaakt dat het belang zo hoog is dat zelfs bijzondere persoonsgegevens in grote hoeveelheden niet relevante informatie aan een derde partij zal worden verstrekt. Mijn advies is om dit zeer goed te onderbouwen.

De vraag die speelt is: Hoe kan de verwerkingsverantwoordelijke in deze de minister verdedigen als betrokkenen van bijzondere persoonsgegevens zijnde voor het onderzoek niet gerelateerde informatie klachten, claims indienen ten aanzien van het verstrekken bijzondere persoonsgegevens aan derden.

Op basis van deze beperkte informatie is door de FG niet in te schatten of de privacy risico's voldoende in beeld zijn, normaal gesproken staat dit uitgewerkt in een DPIA die in dit geval ontbreekt.

3.6 Zienswijze Integriteitscoördinator Concern (ICC)

Nut en noodzaak van het onderzoek staan uitdrukkelijk niet ter discussie, maar de voorgestelde aanpak van de selectie en overdracht van data is onvoldoende proportioneel en levert daarmee ook ernstige risico's op vanuit het perspectief van

[7] artikel 5, eerste lid, onder b AVG

integriteitsmanagement. De ICC kan niet volgen dat de selectie en analyse van de data niet binnen de beveiligde dataomgeving van VWS zelf kan plaatsvinden, in ieder geval van bruto- naar netto-dataset. Deze bewerking kan uiteraard onder regie van Deloitte plaatsvinden, zodat de onafhankelijkheid van het onderzoek niet wordt geschaad. Indien Deloitte zelf niet over de middelen/expertise hiertoe beschikt kan deze worden ingehuurd.

Toelichting:

- De ICC gaat hieronder met name in op de in de nota genoemde (4.) 'E-mailboxen van medewerkers' en (5.) 'Persoonlijke Netwerkschijf' (H-schijf bij VWS-Kern). Hierbij wordt opgemerkt dat ook de andere databronnen zowel privacy gerelateerde als bijzondere informatie zullen bevatten, maar om herhalingen van de BVA, FG en CISO te beperken/voorkomen wordt hier niet nader op ingegaan.
- Wat (6.) 'Gegevens van mobiele telefoons' betreft wordt opgemerkt dat hier al een beperking is gemaakt tot Whatsapp-data en dat hier al een proces voor is ingericht van veiligstellen en archiveren. Hoewel is gebleken dat in dit proces onbedoeld privé-informatie kan worden betrokken, is het natuurlijk wel een keuze van de medewerker zelf om Whatsappverkeer via het zakelijke telefoonnummer ook voor niet-zakelijk of privé doeleinden te gebruiken.
- Door zonder nadere selectie data uit de persoonlijke databronnen (4. en 5.) voor onderzoek over te dragen aan een externe partij worden de rechten van individuele medewerkers - die geen subject zijn van een strafrechtelijk onderzoek of een feitenonderzoek vanwege een vermoeden van een integriteitsschending - onvoldoende gewaarborgd en onvoldoende rekening gehouden met hun belangen. Hierdoor wordt ook data overgedragen die met aan zekerheid grenzende waarschijnlijkheid niet relevant is voor het onderzoek is, maar wel vertrouwelijk is vanuit de functie (denk hierbij aan andere beleidsdossiers of personeelszaken), privé (zoals medische gegevens, contact met vakbond, vertrouwenspersoon, etc.) of andere persoonlijke gevoelige aangelegenheden.
- Daarbij is het voor de ICC tot op heden niet duidelijk welke personen – namen noch functies – tot de groep behoren van wie data aan Deloitte wordt overgedragen. Hierdoor is ook niet duidelijk of het bijvoorbeeld medewerkers betreft die een rol vervullen als lid van de (D)OR, vertrouwenspersoon of lokale integriteitscoördinator. Deze medewerkers beschikken over rol-gerelateerde vertrouwelijke informatie die gegarandeerd buiten de overdracht behoort te vallen.
- Aanvankelijk was aangegeven dat er een freeze heeft plaatsgevonden van de H-schijven en persoonlijke e-mailboxen, dit blijkt echter wat de persoonlijke schijven betreft nog niet het geval te zijn. Door een freeze toe te passen wordt de volledige werkelijke digitale situatie vastgelegd. Als hierna de in het onderzoek betrokken medewerkers worden genotificeerd dat zij functioneel betrokken worden in het onderzoek, kunnen deze de gelegenheid krijgen om bepaalde – niet voor onderzoek relevante – informatie op de H-schijven en persoonlijke e-mailboxen uit te sluiten of om aan te geven welke submappen buiten de overdracht moeten vallen (bijv. 'privé', 'vertrouwenspersoon', 'P&O'). Hiermee is de overdracht al voor een deel ingeperkt en wordt beter – niet volledig overigens – tegemoet gekomen aan de rechten en belangen van deze medewerkers. Indien later een vermoeden bestaat dat de medewerker van deze gelegenheid misbruik heeft gemaakt door data te verwijderen/verplaatsen die relevant is voor het onderzoek van Deloitte

ontstaat een nieuwe situatie. Er is dan een vermoeden van een integriteitsschending of strafbaar feit. Dat geeft aanleiding tot het instellen van een persoonsgericht intern onderzoek of een strafrechtelijk onderzoek waarbij alle data – die zijn veilig gesteld door de freeze – kunnen worden betrokken. In dat geval gelden de waarborgen zoals genoemd in de Baseline Intern Persoonsgericht Onderzoek bij een integriteits- of beveiligingsincident (BIPO). Hierbij wordt wederom opgemerkt dat het onderhavige onderzoek de reconstructie van het inkoopproces als doel heeft en niet het karakter mag krijgen van een persoonsgericht onderzoek zonder dat er sprake is van een vermoeden van integriteitsschending of strafbaar feit.

- De BVA, CISO en FG hebben aangegeven dat met het huidige voorstel sprake is van het willens en wetens niet volgen van geldende wet- en regelgeving. Dit kan een onrechtmatige daad, integriteitsschending of strafbaar feit opleveren. In ieder geval kunnen personen op wie de data betrekking heeft - zowel medewerkers als derden (waaronder burgers) - aanleiding zien een schadeclaim in te dienen of hiervan melding of aangifte te doen.
- Verder is de vraag nog niet beantwoord wat de lijn is indien uit de data (vermoedens van) integriteitsschendingen of strafbare feiten buiten de scope van het onderzoek van Deloitte aan het licht komen. Wordt deze 'bijvangst' genegeerd of wordt hier opvolging aan gegeven? Welk afwegingskader bestaat hiervoor?
- De aanleiding tot het onderzoek is uitzonderlijk en er is begrip voor dat er geen kant en klare volledig afgewogen aanpak ligt. Maar de voorgestelde aanpak van het onderzoek kan ook grote gevolgen hebben en leidt tot een zeer ernstig afbreukrisico voor individuele personen, maar ook het departement als geheel. De ICC is er onvoldoende van overtuigd dat de departementsleiding op dit moment voldoende is geïnformeerd om deze gevolgen te kunnen overzien en hierover een weloverwogen beslissing te kunnen nemen.
- De ICC stelt dat het in dit soort uitzonderlijke gevallen noodzakelijk is om (de voorzitter van) de DOR tijdig en voldoende te informeren voor de onderdelen die de rechten en belangen van medewerkers kunnen raken. Dit was tot het overleg van woensdag 1 september nog niet het geval, terwijl de noodzaak door de ICC al eerder is benadrukt.
- Tijdens het overleg van 1 september werd duidelijk dat de opzet van het onderzoek al voor het zomerreces is aangevangen. Doordat de BVA, FG, CISO en ICC pas in een laat stadium – medio augustus – zijn betrokken is kostbare tijd verloren. Hierdoor komen de risico's van de huidige voorgestelde aanpak van het onderzoek van met name de selectie en overdracht van data pas in een laat stadium aan het licht.

4. Toelichting

a. Draagvlak politiek
Het onderzoek kan op veel aandacht van de Kamer (media) rekenen. De minister heeft aangegeven transparant te willen zijn over het gehele traject.

b. Draagvlak maatschappelijk en eenduidige communicatie
Bij publicatie van het rapport moet er rekening mee worden gehouden dat naast de AP dat ook privacy deskundigen en organisaties die de bescherming van de privacy nastreven kritische vragen zullen stellen en hiermee de nodige aandacht zullen genereren.

``

c. Financiële en personele gevolgen
n.v.t.

d.Juridische aspecten haalbaarheid
Voor zover dat hierboven bij de bespreking per databron nog niet aan de orde is gekomen, merkt WJZ op:

Hoewel gezien van het ontbreken van een deel van de informatie (zoals de lijst van sleutelfiguren en dossiereigenaars) een definitief oordeel nog niet gegeven kan worden, kan wel worden gezegd dat indien de volledige overdracht van data plaatsvindt zoals wordt voorgesteld, u bewust besluit de wet te overtreden.

Het in strijd met de (beginselen van) de AVG verstrekken van de persoonsgegevens aan Deloitte is onrechtmatig en leidt tot een onrechtmatige verstrekking door VWS en onrechtmatige gegevensverwerking door Deloitte. Zie hiertoe tevens de opmerkingen die de FG reeds gemaakt heeft in haar zienswijze. We wijzen in dit verband ook op de discussie omtrent het sleepnet zoals geïntroduceerd in het kader van de nieuwe wet op de inlichtingen en veiligheidsdiensten. In het verband van het Deloitte onderzoek wordt feitelijk met een sleepnet zeer veel informatie overdragen die voor een groot deel niet relevant is voor het onderzoek en bovendien zeer gevoelige informatie bevat over medewerkers en burgers. Denk aan gegevens over personeelszaken, Arbozaken, claims en klachten van burgers waarin het hun gezondheid of geloofsovertuiging betreft (bijvoorbeeld bijwerkingen vaccins of weigeren vaccinatie).

Er bestaat een reëel risico op handhaving door de AP dan wel Europese toezichthouder. Burgers en medewerkers kunnen een klacht indienen en de AP kan uit eigen beweging handhaven. Het gaat immers om potentieel zeer veel gevoelige persoonsgegevens die buiten de omgeving van de overheid worden gebracht. Ook maatschappelijk en politiek kan deze werkwijze grote discussie opleveren. Tevens zou VWS aansprakelijk kunnen worden gesteld door betrokkenen doordat hun gegevens onrechtmatig ter beschikking zijn gesteld.

Het ter beschikking stellen van de bruto informatie aan Deloitte zonder grondig onderzoek en afweging van alternatieven en proportionaliteit, maakt de overtreding van de wet nog ernstiger en daarmee neemt het risico op (strikte) handhaving van de AP (boete) en mogelijk de Europese toezichthouder aanzienlijk toe.

Het dringende advies is alternatieve werkwijzen nader te verkennen, waarbij de (bijzondere) persoonsgegevens van medewerkers, burgers die in de databronnen opgenomen zijn, niet worden verstrekt. Denk bijvoorbeeld aan een stand alone/inhouse selectie (eventueel door Deloitte) in plaats van verstrekking van alle bruto databronnen.

Tot slot kan ook overwogen worden om met de AP in gesprek te gaan om te bezien in hoeverre zij zouden kunnen instemmen met de voorgestelde werkwijze. Hierbij geven we aan dat de inschatting is dat de totale doorlooptijd (onder ideale omstandigheden) 2 tot 4 weken zal zijn. De AP zal informatie nodig hebben om tot een afgewogen oordeel te kunnen komen. Zij zal ook inzicht moeten worden verschaft in de reikwijdte van de data transfer.

e.Afstemming (intern, interdepartementaal en met veldpartijen)

Er is binnen VWS afstemming geweest met de CIO Kern, CIO Concern, de CISO Kern, de CISO Concern, ICC, de FG, de BVA en WJZ.

f. Gevolgen administratieve lasten
n.v.t.

g. Toezeggingen
n.v.t.

h. Fraudetoets
n.v.t.

5. Informatie die niet openbaar gemaakt kan worden
Het betreft geen beslisnota voor de bewindspersoon. Dus (actieve) openbaarmaking is niet aan de orde.

``

Bijlage 1: Van Deloitte

Protocol digitaal onderzoek

Bij aanvang van het dataonderzoek worden de potentieel relevante informatiebronnen en datahouders geïdentificeerd door het onafhankelijke onderzoekers van Deloitte. Het elektronische bewijsmateriaal en daarmee samenhangende handelingen worden bij verkrijging en gedurende het gehele proces gedocumenteerd (hierna: audit trail) ten einde de authenticiteit en integriteit van het bewijsmateriaal te kunnen waarborgen. De audit trail bestaat uit het volgende:

a) Een actuele documentatie over de beheersmatige handelingen met betrekking tot het bewijsmateriaal ("*chain of custody*"). De documentatie omvat tenminste de oorspronkelijke kenmerken van het object, de individuen verantwoordelijk voor het object en de uitgevoerde handelingen met betrekking tot het object; en

b)

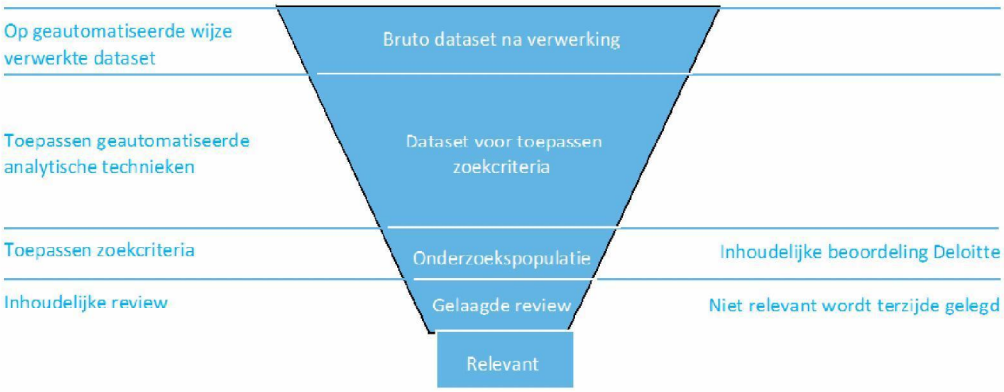
c) een actuele documentatie over de locatie en bewegingen van het object vanaf het moment van verkrijgen tot aan het moment van presentatie ("*chain of evidence*"). De documentatie omvat gegevens over de data houder, beschrijving van het object, type object, kenmerken van het object en methode van veilig stellen.

d)

e) Deloitte hanteert een geautomiseerd proces dat de veiliggestelde gegevens op een controleerbare, verdedigbare en herhaalbare wijze verwerkt en doorzoekbaar maakt. Het proces borgt daarmee dat de gegevens op een betrouwbare en verifieerbare wijze beschikbaar worden gemaakt voor het analyse door het toepassen van zoekcriteria. Door het toepassen van betrouwbare en geautomatiseerde analytische technieken wordt de dataset voorafgaand aan analyse verder vernauwd ten behoeve van het efficiënt uitvoeren van het onderzoek. Voor de analyse zal het onderzoeksteam van Deloitte werken met zoekcriteria die door de onderzoeker van Deloitte op proportionaliteit en subsidiariteit worden getoetst. Na het toepassen van de zoekcriteria worden de documenten, die een treffer opleveren op de zoekcriteria, geselecteerd en toegankelijk gemaakt voor een inhoudelijke review in meerdere lagen door medewerkers uit het onderzoeksteam van Deloitte. Niet relevant bevonden documenten worden terzijde gelegd. De documenten die geen treffer opleveren op de zoekcriteria worden aantoonbaar niet toegankelijk gemaakt. Gedurende het gehele proces worden maatregelen genomen die de privacy en vertrouwelijkheid van de verkregen gegevens borgen.

Datum
1 september 2021

Kenmerk



``

Datum
1 september 2021

Kenmerk

Bijlage 2 de door VWS opgestelde proportionaliteitstoets tav levering van data aan Deloitte

Beste collega,

In het debat rond de ontwikkelingen van het coronavirus d.d. 3 juni 2021 heeft de minister voor Medische Zorg en Sport een extern onderzoek aangekondigd naar de inkoop van persoonlijke beschermingsmiddelen (PBM). Het externe onderzoek is gegund aan Deloitte en wordt uitgevoerd door de forensische tak van Deloitte.

Voor de uitvoering van het onderzoek heeft Deloitte de relevante gegevens nodig. In voorbereidende gesprekken is onderscheid te maken in vijf gegevensbronnen:
1. Afdeling netwerkschijf en project netwerkschijf (G-schijf, O-schijf en P-schijf bij VWS-Kern)
2. Samenwerkingsruimten (Intern en Extern)
3. Marjolein
4. E-mailboxen van medewerkers
5. Persoonlijke Netwerkschijf (H-schijf bij VWS-Kern)
6. Gegevens van mobiele telefoons
7. 3F (financiële systeem)

In de reeds gevoerde gesprekken is besproken dat deze gegevensbronnen meer gegevens bevatten dan noodzakelijk zijn voor het onderzoek, waaronder gerubriceerde documenten met verschillende niveaus van rubricering. Deze bronnen bevatten bovendien persoonsgegevens waarvan het zeer waarschijnlijk is dat in deze bronnen ook bijzondere persoonsgegevens zijn opgenomen. Van belang is om een rechtmatigheid en proportionaliteitstoets uit te voeren op de uit te leveren gegevens uit de gevraagde bronnen.

Om persoonsgegevens te mogen verwerken is een grondslag nodig. De gegevens die VWS onder zich heeft voor de verschillende onderwerpen vallen onder de grondslag voor de specifieke uitvoering van die taak. Een dergelijk onafhankelijk onderzoek door een extern partij is geen standaard onderdeel van de uitvoering van de taak waarvoor de persoonsgegevens worden verwerkt. Wel is het zo dat de minister conform artikel 68 Grondwet kortgezegd verplicht is inlichten te geven aan de afzonderlijke of verenigde Kamers indien een van de Kamers daarom vraagt. Voor zover de verwerking van persoonsgegevens verder gaat dan de reeds geldende grondslag toestaat, is voor het verdere voor wat betreft dit onderzoek het uitvoeren van een wettelijk plicht van de verwerkingsverantwoordelijke (artikel 6, eerste lid, sub e van de AVG) van toepassing.
Bovenstaande uiteenzetting richt zich enkel op de grondslag van VWS voor het verzamelen en overdragen van gegevens aan Deloitte. Het onafhankelijke onderzoek brengt met zich mee dat Deloitte zelfstandig verwerkingsverantwoordelijk is voor de gegevens die zij verwerken in het kader van het uitvoeren van het onderzoek. Het is aan Deloitte om de grondslag voor de verwerking van persoonsgegevens vast te stellen. Het ligt voor de hand dat artikel 6, eerste lid, onder b van de AVG (noodzakelijk voor de uitvoering van de overeenkomst) als grondslag wordt aangemerkt. Ik merk hierbij op dat de grondslag 'noodzakelijk voor de uitvoering van de overeenkomst' opgenomen is in artikel 6 van de AVG die de algemene grondslag voor de verwerking van

persoonsgegevens biedt, maar niet voorkomt als grondslag in artikel 9 van de AVG dat ziet op het doorbreken van het verwerkingsverbod voor bijzondere persoonsgegevens.

Onderstaand is de proportionaliteitstoets per bron kort beschreven.

Proportionaliteit gegevensbronnen:

1. Afdeling netwerkschijf en project netwerkschijf (G-schijf, O-schijf en P-schijf bij VWS-Kern)
2. Samenwerkingsruimten (Intern en Extern)

Voor deze gegevensbronnen zijn in deze fase nog geen specifieke documenten opgevraagd. Het voorstel is om een overzicht te verstrekken van de mappenstructuur waarna Deloitte aangeeft welke mappen zij nodig achten voor het onderzoek.
Ook voor de samenwerkingsruimten is een overzicht van de bestaande samenwerkingsruimten gevraagd om op basis daarvan te bepalen uit welke samenwerkingsruimten gegevens worden opgevraagd.
Aangezien in deze fase het enkel de mappenstructuur betreft en geen documenten is het onwaarschijnlijk dat er persoonsgegevens worden verstrekt. Mogelijke uitzondering is een mapnaam die een verwijzing naar een persoon betreft.
Het uitgeven van dit overzicht is in deze fase proportioneel. De eigenlijke proportionaliteitstoets kan pas uitgevoerd worden zodra Deloitte op basis van de verstrekte mappenstructuur en samenwerkingsruimte aangeeft vanuit welke mappen en samenwerkingsruimten zij gegevens willen ontvangen voor het onderzoek. Een inhoudelijke proportionaliteitstoets is op dat moment vereist vóórdat die opgevraagde gegevens daadwerkelijk worden verstrekt.

Proportionaliteit gegevensbron:

3. Marjolein

Deloitte heeft in de gevoerde gesprekken aangegeven dat de zoekfunctie in Marjolein niet de gewenste resultaten oplevert. De zoekfunctie lijkt beperkt en niet duidelijk is of gerubriceerde documenten worden getoond op basis van de zoektermen.

Marjolein is opgebouwd in een mappenstructuur. Voorstel is om dezelfde werkwijze toe te passen als bij de netwerkschijven en samenwerkingsruimten; het inzichtelijk maken van de mappenstructuur zodat Deloitte aan kan geven vanuit welke mappen zij de documenten willen ontvangen. Zodra dit verzoek is ontvangen kan vervolgens de daadwerkelijke een gerichte proportionaliteitstoets uitgevoerd worden alvorens de documenten ter beschikking worden gesteld.

Proportionaliteit gegevensbron:

4. E-mailboxen van medewerkers en bewindspersonen

Het voorstel van Deloitte is om de persoonlijke e-mailboxen van de betreffende medewerkers in zijn volledigheid door SSC-ICT veilig te laten stellen voor de periode van 1 januari 2020 en 1 juni 2021 en ter beschikking te stellen aan Deloitte.

``

Waar in de voorgaande drie toetsen het voornemen lijkt te zijn om te selecteren van relevante informatie is deze schifting hier niet voorzien. Hoewel het zeer waarschijnlijk is dat de persoonlijke e-mailboxen van de betreffende medewerkers relevante informatie bevat is het evenzeer zeer waarschijnlijk dat de e-mailboxen veel groter deel aan informatie bevat die niet relevant is voor het onderzoek. De genoemde periode is dusdanig lang dat de aangenomen moet worden dat in ieder geval een aantal van de betreffende personen voor, naast of na hun taak die relevant is voor het onderzoek ook werkzaamheden heeft verricht die geen verband houden met het onderzoek. Ook het feit dat personen niet in de gelegenheid worden gesteld om de relevante informatie zelf aan te dragen is opmerkelijk. Alleen vanuit deze overwegingen is het overdragen van de gehele e-mailbox van een persoon voor de betreffende periode niet proportioneel voor het uitvoeren van het onderzoek.

Meer specifiek gericht op persoonsgegeven is onderstaande eveneens van belang. Persoonlijke e-mailboxen kunnen een divers scala aan persoonsgegevens bevatten. Van de personen zelf, maar ook van andere personen die al dan niet onder de verantwoordelijkheid van VWS vallen. Voor personen met een leidinggevende functie zijn verslagen van functioneringsgesprekken, (langdurige) ziekteverloop van hun medewerkers en/of integriteitsmeldingen voorbeelden van bijzondere persoonsgegevens die in de mappen zouden kunnen staan. Voor alle betrokken personen zijn wederom functioneringsgesprekken, integriteitsmeldingen, contact met vertrouwenspersonen en/of bedrijfsartsen bijzondere gegevens die in de e-mail boxen kunnen staan.

Het mag duidelijk zijn dat een dergelijke algemene overdracht van e-mailboxen niet aan de orde kan zijn. Er zijn echter wel mogelijkheden om de relevante informatie binnen afzienbare tijd aan te leveren aan Deloitte. Hieronder staat een naar oordeel van VWS afgewogen model voor verstrekking van relevante gegevens

1. Betreffende medewerkers verzoeken om de relevante gegevens vanuit hun e-mailbox en submappen aan te leveren. Dit verzoek kan kracht bijgezet worden door het te versturen vanuit de departementale leiding. Hen tegelijkertijd informeren over het onderzoek en dat hun e-mail box doorzocht wordt kan worden met 'zoek en vind'.
2. Inzetten van 'zoek en vind' met zoekwoorden die relevant zijn voor het onderzoek.
3. Als beschermende maatregel voor de bescherming van persoonsgegevens de betrokken personen de gelegenheid geven om voordat hun e-mailbox wordt doorzocht de voor het onderzoek niet relevante e-mails die persoonlijk of vertrouwelijk zijn uit de zoekresultaten te houden door deze in een map te plaatsen die niet doorzocht wordt door 'zoek en vind'.
4. Als aanvullende maatregel voor de bescherming van persoonsgegevens medewerkers inzage te geven in de uit hun e-mailbox gevonden e-mails te bekijken en e-mails die niet relevant zijn kunnen verwijderen uit de verzamelde gegevens.
5.
6. De relevante e-mailboxen in het geheel veilig te stellen onder beheer van VWS om zo in een latere fase van het onderzoek mogelijke gerichte vragen vanuit Deloitte naar gegevens die bij medewerkers van VWS op te pakken. Een nader aan te wijzen medewerker van VWS zal betrokken moeten worden bij degelijke verzoeken van Deloitte. Enkel de CISO van VWS Kern

``

en de CIO van VWS Kern kunnen opdracht geven aan SSC-ICT om dergelijke gegevens vervolgens op te vragen bij SSC-ICT.

Proportionaliteit gegevensbron:

5. Persoonlijke Netwerkschijf (H-schijf bij VWS-Kern)

Initieel werd VWS verzocht om de persoonlijke netwerkschijven van de betreffende medewerkers veilig te stellen en over te dragen aan Deloitte voor het onderzoek. Na de gevoerde gesprekken tussen VWS en Deloitte is het verzoek beperkt tot het verzoek aan de betreffende personen om de relevante gegevens aan te leveren. Om het verzoek kracht bij te zetten kan dat verzoek verzonden worden vanuit de departementale leiding.
Verder wordt verzocht om de persoonlijke schijven veilig te stellen om op een later moment, indien nodig in een concreet geval, te onderzoeken.

De persoonlijke schijven van medewerkers van VWS kan allerlei informatie bevatten. Dit loopt van informatie die betrekking heeft op de privé situatie van de personen, foto's, gezondheidsgegevens (al dan niet werk gerelateerd) functioneringsgesprekken, integriteitsmeldingen etc. de verwachting is dat de informatie veelal niet gerelateerd is aan het onderzoek. Integraal overdragen van deze informatie is daarmee überhaupt niet aan de orde.

Het verzoeken van relevante informatie is de voor de hand liggende optie. Het veilig stellen alle gegevens op de persoonlijke schijven van de betrokken medewerkers is een verregaande maatregel. De noodzaak daartoe is niet onderbouwd. Ik acht het mogelijk dat daar arbeidsrechtelijk beperkingen aan verbonden kunnen zijn die meegewogen moeten worden. Ik zal WJZ en de integriteitscoördinator VWS vragen hierover advies uit te brengen. De adviesvraag zal de vraag omvatten of het aanbieden van een persoonlijke schijf aan een werknemer de werkgever in een voorliggend vraagstuk beperkt om de gegevens op die schijf in zijn geheel veilig te stellen.

Proportionaliteit gegevensbron:

6. Gegevens van mobiele telefoons

In algemene zin is gevraagd om gegevens van mobiele telefoon. Veelgebruikt voorbeeld hierin is de gegevens van whatsapp op de telefoon van betreffende medewerkers. Onduidelijk is welke wijze van verzamelen wordt voorgestaan.

Het is mogelijk dat medewerkers relevante gegevens hebben op hun mobiele telefoon. Dit betekent niet dat iedereen van de betreffende medewerkers relevante gegevens heeft op zijn of haar mobiele telefoon. De voorgestelde werkwijze is om:

- Aan de betreffende medewerkers of zij relevante gegevens op hun mobiele telefoon hebben staan. Dit kan whatsapp zijn. Dit kan ook een andere communicatieapp of opslagfunctionaliteit op hun telefoon zijn.
- Als dit het geval is deze gegevens met behulp van SSC-ICT veilig te stellen.
- De betreffende medewerkers vervolgens de gelegenheid te geven om voor het onderzoek niet relevante informatie te verwijderen.
- De overgebleven gegevens vervolgens te verstrekken aan Deloitte.

Proportionaliteit gegevensbron:

7. 3F (financiële systeem)

``

Datum
1 september 2021

Kenmerk

In 3F staan hoofdzakelijk financiële gegevens. Hier zullen ontegenzeggelijk persoonsgegevens in voorkomen. Het is niet aannemelijk dat dit bijzondere of anderzijds gevoelige persoonsgegevens zullen zijn. Wel is van belang dat enkel gegevens worden verstrekt die zien op het doel van het onderzoek en dat er geen integrale uitdraai van het hele systeem wordt overgedragen.

Bovenop bovenstaande waarborgen zien op het voldoen aan het proportionaliteitsvereiste op het gebied van privacy en daarmee de eerste schifting te maken naar het komen van een selectie die zo dicht mogelijk is gelegen bij het enkel overdragen van voor het onderzoek relevante gegevens. Deze toets is niet de enige toets die plaats moet vinden voordat gegevens overgedragen kunnen worden. Er zijn aanvullende waarborgen nodig die onder ander gelegen zijn op het gebied van security. Uiteraard is de beveiliging vanaf de gegevens overdracht tot aan de vernietiging van de gegevens van groot belang. Ook rijksbrede voorwaarden rondom gerubriceerde informatie kan de gegevensoverdracht beperken. Hiervoor is nader advies nodig van de BVA van VWS.

Verder is van belang om te vermelden dat dit een eerste en zeer algemene proportionaliteitstoets is. Zoals eerder vermeld zal op de eerste drie punten een inhoudelijke proportionaliteitstoets plaats moeten vinden zodra Deloitte heeft aangegeven vanuit welke mappen zij informatie wensen. Een nadere proportionaliteitstoets is eveneens nodig zodra meer specifieke informatie over het onderzoek beschikbaar komt. Een voorbeeld hiervan is de lijst van geselecteerde personen en de prioritering die daarin is aangebracht. Deze lijst is tot op heden niet verstrekt. Hierdoor kan niet bepaald worden op welk niveau de betrokken personen werkzaam zijn en of zij überhaupt nog werkzaam zijn voor VWS. Deze eerste en hoog over proportionaliteitstoets is daarom bedoeld om het gesprek aan te gaan en biedt geen groen licht om persoonsgegevens over te dragen zonder nadere proportionaliteitstoets en zonder een nader advies van de in dit stuk genoemde functionarissen zoals de BVA, CISO Concern en integriteitscoördinator VWS

Met vriendelijke groet,

5.1.2e

5.1.2e