Ministerie van Volksgezondheid,
Welzijn en Sport

5.1.2e

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e
Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T
F 5.1.2e
www.rijksoverheid.nl
Inlichtingen bij
5.1.2e
M 06 5.1.2e
5.1.2e @minvws.nl

Datum
9 september 2021

Aantal pagina's
11

memo

Risicoanalyse gegevenslevering onderzoek 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 zijn de relevante gegevens nodig en zijn er 7 bronnen geïdentificeerd door Deloitte voor het geplande onderzoek.

- Netwerkschijven van directies en projecten (G-schijf, O-schijf en P-schijf bij VWS-kern)
- Samenwerkingsruimten (Intern en Extern)
- Marjolein (document management systeem bij VWS-kern)
- E-mailboxen van medewerkers
- Persoonlijke netwerkschijf van medewerkers (H-schijf bij VWS-kern)
- Gegevens van mobiele telefoons
- 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.

De BVA heeft gevraagd om CISO Kern, Privacy Officer Kern en CISO Concern per direct een risicoanalyse (RA) te maken waar het buiten de overheid brengen van bijzondere informatie, het opleveren van de specifieke data en het analyseren van data knelpunten oplevert uitgaande van bestaande regelgeving en/of verplichtingen. Op basis van deze hoofdpunten wordt in de RA aangegeven;

- Welke mitigerende maatregelen er getroffen kunnen worden (theorie)
- Welke mitigerende maatregelen er getroffen gaan worden (praktijk / gezien beperkte doorlooptijd / terugkoppeling Deloitte)
- Wat te accepteren (rest)risico's zijn
- Waar de werkelijkheid strijdig is met regelgeving (maar wel een showstopper als het niet gedaan wordt)

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e

Datum
9 september 2021

De risicoanalyse wordt opgebouwd vanuit de aangeleverde bewijslasten vanuit de onderzoekers of het projectteam en door het project in stappen op te delen. De aangeleverde bewijzen worden beoordeeld en gekoppeld aan de stappen van het project.
Dit heeft geresulteerd in de volgende analyse stappen:

1. Vaststelling van het onderzoeksteam en controle op bevoegdheden.
2. Compliance van Deloitte op de wet en regelgeving (BIO, BVR, VIR, VIR-BI en AVG) op gebied van mensen, middelen en organisatie.
3. Risico's van de dataverstrekking vanuit het perspectief van dataclassificatie, zodat er inzicht kan worden gegeven over de risico's van de over te dragen informatie.
4. Analyse op het transport van data en de beveiligingswaarborgen.
5. Fysieke en logische beveiligingsmaatregelen van de onderzoekslocatie van Deloitte.
6. Risicoanalyse op de onderzoeksmethode.
7. Waarborgen afronding van het onderzoek en de eindsituatie, inclusief de data-archivering en vernietiging.

In de risicoanalyse is een advies opgesteld voor de onderzoeksmethode met de minste impact voor de organisatie.

Het advies is om methode 1 van de data selectie methoden niet in te zetten, omdat dit maximaal conflicteert met genoemde wet- en regelgeving. Ook al heeft deze methode de voorkeur van Deloitte gaat dit echt in strijd met de privacygedragscode, zoals beschreven in hoofdstuk 1. Deze privacygedragscode is goedgekeurd door de Autoriteit Persoonsgegevens en houdt in dat een particulier onderzoeksbureau verplicht is om proportionaliteit (evenredigheid van doel en middelen) en subsidiariteit (gematigdheid bij de inzet van middelen en methoden) in acht te nemen bij de gekozen onderzoeksmethoden- en middelen. Tevens spreekt dit het Data Processing Protocol (bijlage 6A) van Deloitte tegen waarin hun eerste doelstelling is "Selectie van veilig te stellen data wordt afgestemd met de opdrachtgever en er wordt expliciet besproken of dit in lijn is met (eventueel) toepasselijk intern beleid;". Het uit handen geven van de volledige bruto dataset is per definitie een datalek of incident omdat er geen inzicht is in de informatie die buiten de organisatie wordt gebracht.

Ons dringende advies is om methode 4 of 5 van de data selectie methoden te kiezen, omdat duidelijk is dat de volledige brondata doorzocht moet kunnen worden met als uitgangspunt dataminimalisatie en zoveel mogelijk risico's te kunnen mitigeren. Wanneer op deze wijze data wordt geselecteerd en gemonitord, kunnen eigenaren van de data vooraf geïnformeerd worden dat de betreffende informatie wordt overgedragen voor onderzoek aan Deloitte.

De bevindingen uit deze risicoanalyse zijn een voorlopige en globale inschatting. Een volledige DPIA dient nog te worden uitgevoerd.

5.1.2e

5.1.2e

Risicoanalyse Forensisch Onderzoek Deloitte

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e

Datum
9 september 2021

In opdracht van de BVA wordt een risicoanalyse uitgevoerd m.b.t. het voorgenomen onderzoek inkoop PBM door Deloitte. In de RA wordt aangegeven waar het buiten de overheid brengen van bijzondere informatie, het opleveren van de specifieke data en het analyseren van data knelpunten oplevert uitgaande van bestaande regelgeving en/of verplichtingen. Op basis van deze hoofdpunten wordt in de RA aangegeven;

- Welke mitigerende maatregelen er getroffen kunnen worden (theorie)
- Welke mitigerende maatregelen er getroffen gaan worden (praktijk / gezien beperkte doorlooptijd / terugkoppeling Deloitte)
- Wat te accepteren (rest)risico's zijn
- Waar de werkelijkheid strijdig is met regelgeving (maar wel een showstopper als het niet gedaan wordt)

1. Controle bevoegdheden Deloitte

Deloitte is een particulier onderzoeksbureau met een POB-vergunning en heeft zich daardoor te houden aan de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr) en de Regeling en Beleidsregels particuliere beveiligingsorganisaties en recherchebureaus (Rpbr en Bpbr). Daarnaast zijn zij ook gehouden aan de Algemene verordening gegevensbescherming (AVG) en de privacygedragscode sector particuliere onderzoeksbureaus van de Nederlandse Veiligheidsbranche. Deze privacygedragscode is goedgekeurd door de Autoriteit Persoonsgegevens en houdt in het kort in dat een particulier onderzoeksbureau verplicht is om proportionaliteit (evenredigheid van doel en middelen) en subsidiariteit (gematigdheid bij de inzet van middelen en methoden) in acht te nemen bij de gekozen onderzoeksmethoden- en middelen.

Vaststelling

Deloitte staat vermeld in de meest recente lijst van vergunninghouders uitgegeven door Justis (Ministerie van J&V) met POB-nummer 689 (pagina 62 van bijlage A).

Documenten

- Deloitte - Bijlage 1A - Justis lijst vergunninghouders WPBR dd 03-04-2018.pdf
- Deloitte - Bijlage 1B - Privacygedragscode sector particuliere onderzoeksbureaus van de Nederlandse Veiligheidsbranche dd 17-11-2015.pdf
- Deloitte - Bijlage 1C - Staatscourant bekendmaking_besluit privacygedragscode sector particuliere onderzoeksbureaus dd 09-03-2016.pdf
- Deloitte - Bijlage 1D - Autoriteit Persoonsgegevens - advies gedragsregels particuliere onderzoeksbureaus dd 07-12-2020.pdf

Risico's

- Particulier Onderzoeksbureau (POB) vergunning op de gepubliceerde lijst van Justis dateert uit 2018. Daarop is vermeld dat Deloitte een vergunning heeft tot 01-01-2020. We kunnen op dit moment geen actuele situatie vaststellen.
- Deloitte gebruikt in diverse stukken andere bedrijfsnamen als identiteit. Door deze inconsistentie is het niet duidelijk met welke entiteit data gedeeld wordt. Het is niet uit te sluiten dat data gedeeld wordt met internationale onderdelen van Deloitte via mens of techniek.
    - Deloitte Bijzonder onderzoek en integriteit BV
    - Deloitte Group
    - Deloitte IT & Workplace Services
    - Deloitte Forensic & Dispute Services BV
    - Deloitte Financial Advisory BV

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e

Datum
9 september 2021

2. Controle compliance informatiebeveiliging Deloitte

Het Ministerie van VWS is gehouden te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO), het Beveiligingsvoorschrift Rijksdienst (BVR), het Voorschrift Informatiebeveiliging Rijksdienst (VIR), het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI) en de Algemene verordening gegevensbescherming (AVG). De onderzoekaanpak en systemen van Deloitte zullen aan deze wet- en regelgeving moeten voldoen.

Vaststelling

Deloitte is gecertificeerd volgens de standaard ISO/IEC 27001:2013 en beproefd gevonden door een onafhankelijke auditor, Lloyd's Register (bijlage 2A).

Documenten

- Deloitte - Bijlage 2A - ISO IEC 27001 - LRQA Certificate of approval ISMS dd. 22-12-2018.PDF
- Deloitte - Bijlage 2B - ISO IEC 27001 - Statement of Applicability v 1.0.pdf
- Deloitte - Bijlage 2C - Factsheet Risk & Security Deloitte-NL 2021.pdf
- Deloitte - Bijlage 2D - Toets VIR-BI - Departementaal Vertrouwelijk t.b.v. systemen Deloitte.docx

Risico's

- Volgens de Certificate of Approval (bijlage 2A) is de volledige scope van de ISO 27001 van toepassing. Echter na het bekijken van de Statement of Applicability (bijlage 2B) is niet te herleiden dat deze bijlage afkomstig is van Lloyd, zoals deze wel te herleiden is van het certificaat zelf. Er kan ook niet vastgesteld worden of deze statement de volledige maatregelen conform ISO 27001 omvat.
  - Wanneer dit wel vast te stellen is benadert Deloitte de maatregelen van de BIO.
- Er is geen onderbouwing met een privacy statement, er is een minimale beschrijving in onderzoekwerkwijze.
- De inventarisatie van maatregelen VIR-BI toets zijn ingevuld door Deloitte welke niet kunnen worden vastgesteld. Dit betekent dat Departementaal Vertrouwelijke informatie onrechtmatig buiten de organisatie wordt gebracht.

3. Dataselectie

Om tot de bronbestanden te komen heeft een selectieprocedure plaatsgevonden. De selectieprocedure leverde een lijst op waarop de te onderzoeken bronnen konden worden geselecteerd. De selectieprocedure heeft informatie opgeleverd die niet gewaarborgd is op gebied van privacy, security en juridische kaders.

Uit deze selectieprocedure zijn 7 bronnen geïdentificeerd door Deloitte voor het geplande onderzoek.

- Netwerkschijven van directies en projecten (G-schijf, O-schijf en P-schijf bij VWS-kern)
- Samenwerkingsruimten (Intern en Extern)
- Marjolein (document management systeem bij VWS-kern)
- E-mailboxen van medewerkers
- Persoonlijke netwerkschijf van medewerkers (H-schijf bij VWS-kern)
- Gegevens van mobiele telefoons
- 3F (financiële systeem)

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e

Datum
9 september 2021

In de "Beslisnota datalevering" (bijlage 3I) en "Memo proportionaliteitstoets gegevensverstrekking aan Deloitte" (bijlage 3H) zijn de risico's aangegeven op het gebied van privacy, integriteit en juridische gevolgen. Deze bevindingen zijn een voorlopige en globale inschatting en een volledige DPIA dient nog te worden uitgevoerd.
Gezien vanuit het oogpunt van informatiebeveiliging wordt aanvullend de nodige risico's gezien voor het leveren voor de hoeveelheid gevraagde data.

1. Er is in eerste instantie uitgegaan van 120 personen waarvan de mail en de persoonlijke netwerkschijven veilig gesteld zullen worden. Er is op dit moment sprake van 250 personen die in het onderzoek betrokken worden. Het risico is dat een te groot aantal medewerkers onderhavig zijn aan het onderzoek en geleidelijk aan naar gelang het onderzoek vordert vermeerdert.
2. De databronnen zullen naast de privacy gevoelige informatie mogelijk ook informatie bevatten waarvan het niet wenselijk is dat deze informatie buiten de organisatie wordt gebracht. Hierbij valt te denken aan:

Informatie	**Enkele voorbeelden**
Gerubriceerde informatie hoger dan DepV welke niet op de juiste manier of plaats is opgeslagen.	Ministerraad notulen zijn gevonden in Marjolein, netwerkschijven of e-mail tijdens zoekopdrachten voor WOB-verzoeken.
Informatie (DepV of hoger) met betrekking tot bestuurlijke of politieke onderwerpen die geen relatie hebben tot dit onderzoek.	Deze informatie kan gevonden worden in E-mailboxen van de bewindslieden, ambtelijke leiding en/of directeuren, op het netwerk of in Marjolein.
Juridische en straf- of tuchtrechtelijke informatie (WJZ en ESTT)	Alle juridische informatie bij WJZ; Beheer tuchtzaken nav een klacht tegen BIG geregistreerden (ESTT)
Medische of andere gevoelige informatie van burgers	Burgervragen met medische gegevens en/of zeer privacygevoelige gegevens (hele levensverhaal) zijn te vinden in dienstpostbussen en Marjolein (Unit Complexe Zorgvragen); Beoordelen, door euthanasiecommissie, van door een arts uitgevoerde euthanasie (ESTT) Beoordelingen van commissie late zwangerschapsafbreking en levensbeëindiging pasgeborenen (ESTT)
Persoonlijke informatie van medewerkers	Salarisstroken, functioneringsgesprekken, opleidingen, medische informatie (bedrijfsarts, WIA), foto's, persoonlijke privé bestanden, etc.
Commercieel (concurrent)gevoelige informatie	Samenstelling van geneesmiddelen of medisch hulpmiddelen (CCMO).
Informatie van of over concernonderdelen van VWS,	Contracten, verwerkersovereenkomsten,

ministeries of (overheids)organisaties	verwerkersafspraken, vertrouwelijke documenten, geheimhoudingsverklaringen, jaarplannen, projectinformatie, aanbestedingen, beleidvorming etc.
Informatie over (tekortkomingen aan) fysieke beveiliging, informatiebeveiliging en privacy	Kerndepartment en Concernonderdelen VWS zoals dreigingsanalyses (PLATO), DPIA's, risicoanalyses, pentest informatie, TLP amber/red (NCSC), verbeterplannen IB etc) te vinden op het netwerk, samenwerkruimten, Marjolein en E-mailboxen

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e

Datum
9 september 2021

3. Het is nog niet duidelijk welke directies bij het onderzoek betrokken worden. Er zijn directies die niets met de inkoop van PBM te maken hebben, zoals o.a. ESTT, CCMO, de raden, OBP etc. Ook is nog niet duidelijk welke bronnen toegevoegd worden, zoals de SWF/e-SWF omgevingen waar samenwerkruimten kunnen worden opgevraagd aan de hand van een overzicht van alle samenwerkruimten namen en mappen.
4. Alle overhandigde data zal minimaal in drie kopieën bij Deloitte staan, waarvan twee kopieën 5 jaar zullen worden opgeslagen. De zorg blijft dat er niet gewaarborgd kan worden dat er meer kopieën gemaakt worden.

Documenten

- Deloitte - Bijlage 3A - Offerteaanvraag inclusief de conceptopdracht van Opdrachtgever.pdf
- Deloitte - Bijlage 3B - Offerte Deloitte Onderzoek inkoop PBM voor VWS dd 17-06-2021.pdf
- Deloitte - Bijlage 3C - VWS - Deloitte arvodi overeenkomst onderzoek inkoop PBM def versie 19-7-2021.docx
- Deloitte - Bijlage 3D - Nota ter beslissing ondertekenen DVO Deloitte door SG 20210719.docx
- Deloitte - Bijlage 3E - Opdrachtbevestiging Deloitte project Onderzoek inkoop PBM.pdf
- Deloitte - Bijlage 3F - Concept Gegevensdelingsovereenkomst.docx
- Deloitte - Bijlage 3G - Nota voor akkoord levering persoonlijke netwerkschijven aan Deloitte incl opmerkingen.docx
- Deloitte - Bijlage 3H - Memo proportionaliteitstoets gegevenslevering aan Delotte.docx
- Deloitte - Bijlage 3I - Beslisnota datalevering met geintegreerde toevoegingen van BVA, CISO, ICC, FG, WJZ, CIO defconcept.docx

Risico's

- Het grootste risico van het verstrekken van alle data aan Deloitte is dat het voor VWS niet mogelijk is om de data-veiligheid en integriteit te waarborgen, omdat deze zich buiten de overheidsomgeving bevindt. De informatie in de dataset reikt onnoemelijk verder dan nodig is om aan de onderzoeksvraag te voldoen en worden in meerdere kopieën voor de duur van 5 jaar bewaard bij een externe organisatie.
- Deze departementaal vertrouwelijke informatie is zeer interessant voor statelijke actoren, die gezien het meest recente dreigingsbeeld van het NCSC, actief op zoek zijn naar informatie van de overheid.
- Aangegeven in de proportionaliteitstoets van de CPO concern is het niet duidelijk welke data er verstrekt gaat worden. Vervolgvragen voor het leveren van data zal via een 4-ogen principe telkens opnieuw behandeld moeten worden (proportionaliteitstoets IB&P) en het risico hierop is dat het advies van de CPO niet wordt gevolgd.
- Er zijn personen geselecteerd voor het onderzoek die omgaan met informatie van hoge mate van vertrouwelijkheid waardoor het risico

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e

Datum
9 september 2021

ontstaat op de ondermijning van het ministerie. Zie kopje gevolgen en schade.
- Er zijn personen geselecteerd die geen betrokkenheid hebben in de te onderzoeken activiteiten.
- Er is niet vast te stellen of de lijst van betrokkenen volledig is.

4. Transport van de data

Deloitte heeft aangegeven dat wanneer er overdracht van de data plaatsvindt naar het onderzoekplatform van Deloitte er gebruik gemaakt wordt van de middelen die goedgekeurd zijn door het NBV.

1. Het is nog niet duidelijk om hoeveel data het gaat en of deze hoeveelheid over te zetten is op een veilige transportdrager. Er wordt op dit moment uitgegaan van twee terabyte aan data bij aanvang van het onderzoek.
2. Het is nog niet duidelijk welke transportdrager gebruikt gaat worden. Deloitte heeft aangegeven hierin afhankelijk te zijn van de keuze van de transportdrager door SSC-ICT.
3. Het is nog niet duidelijk met welke methode of techniek de integriteit van de data gewaarborgd wordt tijdens het transport.
4. Het is nog niet duidelijk of Deloitte gerechtigd is om deze data mee te nemen naar de eigen locatie. De VIR-BI geeft aan dat deze persoon een geautoriseerde medewerker of overheidskoerier moet zijn.

Risico's

- Er is geen procesbeschrijving beschikbaar gesteld die stapsgewijs het transport proces beschrijft. Ook is onduidelijk hoe de auditeerbaarheid blijft gewaarborgd van de stappen.
- De data kan verloren gaan tijdens het transport.
- De integriteit van de data kan aangetast worden tijdens het transport.
- SSC-ICT beschikt mogelijk niet over de juiste transportdragers.
- Het proces van dataoverdracht op de transportdrager en verzegeling wordt niet voldoende gewaarborgd.

5. Datacenter Deloitte

De dataset zal verwerkt gaan worden op locatie van Deloitte, het datacenter in Amsterdam. De dataset bevat informatie met rubricering Departementaal Vertrouwelijk (en mogelijk hoger) en zal minimaal beveiligd moeten worden conform basisbeveiligingsniveau BBN2+ van de BIO. Het gebouw zal ingericht moeten zijn conform de standaarden van beveiligde zones conform Kader Rijkstoegangsbeleid 2010, Normenkader Beveiliging Rijkskantoren (NkBR) 2016, Beveiligingsvoorschrift Rijksdienst (BVR) 2013 en de BIO (Hfst 11).

Het is mogelijk om het datacenter te bezoeken en fysiek de maatregelen te zien/bekijken. Echter mogen bezoekers niet de labruimte binnenkomen waar het forensisch onderzoek wordt uitgevoerd. Het heeft daarom niet veel zin om dit bezoek af te leggen. Deloitte levert een foto van de ruimte en heeft de volgende beschrijving van logische en fysieke maatregelen aangeleverd:

> De gegevens worden getransporteerd naar het datacentrum van Deloitte waar fysieke- en omgevingsbeveiligingsmaatregelen van toepassing zijn.
> *Zone 0* - Het terrein van hetdatacentrum is afgeschermd met een hek en er vindt toegangscontrole en registratie plaats.

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e

Datum
9 september 2021

Zone 1 - Toegang tot datacentrum en de publieke ruimten is mogelijk voor geautoriseerde personen. Er vindt toegangscontrole en registratie plaats.
Zone 2 - Het kantoorgedeelte tot aan de labruimte is alleen toegankelijk voor geautoriseerde personen.
Zone 3 - Labruimte is voorzien van aanvullende toegangscontrole en beveiligingsmaatregelen. Voorafgaand aan het betreden van de ruimte zal alarm voor labruimte door beveiliger uitgeschakeld worden. Instrueren beveiliger voor het uitschakelen van alarm op de labruimte is alleen toegestaan voor bevoegde Deloitte Forensic medewerkers. Toegang tot de fysieke labruimte is geschied door aanbieden toegangspas in combinatie met intoetsen toegangscode. De ruimte bevat fysieke kluizen voor opslag van opslagmedia. Labruimte is ingericht met een aantal werkplekken, gespecialiseerde apparatuur en werkstations. Logische toegangsbeveiliging is van toepassing op de werkstations. Werkstations worden gebruikt voor uploaden van dataset naar servers in het datacentrum van Deloitte.
Zone 4 - Servers bevinden zich in een separate serverruimte van het datacentrum. Serverruimte is toegankelijk voor zeer selecte groep van IT specialisten van Deloitte.

Documenten

Deloitte - Bijlage 5A - Deloitte datacenter security CC- Dynamostraat Amsterdam.pdf
Deloitte - Bijlage 5B - Foto LabruimteJPG

Risico's

- Het is niet met zekerheid vast te stellen dat deze beschrijving van de verschillende zones klopt.
- Het is niet met zekerheid vast te stellen dat de genoemde zones voldoen aan de standaarden conform Kader Rijkstoegangsbeleid 2010, NkBR 2016, BVR 2013 en de BIO.
- Fysieke beveiligingsmaatregelen lijken niet solide genoeg, zoals bijvoorbeeld de deur naar de labruimte (foto toont houten deur, houten kozijn, toegangspaneel zou logischerwijs aan de andere kant moeten zitten, deurklink/slot is dan niet logisch, ruimte onder de deur etc.).
- Geen informatie over de serverruimte in zone 4 waar de data verwerking en backup in plaats vindt.
- Geen informatie over de gebruikte kluis voor opslag informatiedragers/kopieën data ontvangen.

6. Risicoanalyse op de onderzoeksmethode

Deloitte beschrijft een onderzoeksmethode die op basis van een selectie tot de eerder genoemde bronnen komt inclusief de personen of functie in onderzoek, ook wel de 'custodians' genoemd. Er is een aantal keuzes voorhanden aan de invulling van dit onderzoek die van significante invloed zijn op de hoogte van de risico's op dataveiligheid. Deze keuzes worden hier geschetst in de vorm van scenario's waarop het onderzoek kan worden uitgevoerd:

Methode 1: Deloitte verwerkt bruto dataset.

De preferente methode van Deloitte draagt de data over in de meest ruime vorm. De overdracht gebeurt binnen SSC-ICT op een datadrager. Deze wordt getransporteerd naar Deloitte. Daar wordt de data in onverwerkte toestand verdeeld over een backup (inclusief gehashed) en een werkkopie. De backup en de originele datadrager wordt gesealed en in een kluis opgeslagen. De werkkopie wordt vervolgens ingelezen ter verwerking op het onderzoeksplatform. De niet

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e

Datum
9 september 2021

relevante informatie wordt uit de werkkopie verwijderd. En het onderzoek kan van start gaan.

De voordelen zijn dat de meest ideale werkwijze voor Deloitte hier wordt gehanteerd. Het nadeel is dat voor 5 jaar na afloop van het onderzoek er minimaal twee kopieën buiten de Rijksoverheid aanwezig zijn. Relevant is dat het grootste nadeel van deze keuze ligt in de opslag van data die geen relatie heeft tot het onderzoek, maar wel een hoog risico profiel heeft (zie risicoanalyse 3 Dataselectie).

Methode 2: Deloitte verwerkt netto dataset

Deloitte filtert met behulp van de zoek-en-vind tool/Zylab de data tot de relevante selectie. Vervolgens wordt deze data overgezet op een datadrager. De vervolg stappen zijn gelijk aan die van methode 1.

De voordelen zijn dat VWS enkel relevante informatie deelt en te verwachte bijvangsten uitsluit. De nadelen van deze keuze zijn dat Deloitte niet het volledige speelveld kan overzien en daarmee niet de volledigheid kan aantonen. Een nadeel blijft dat de gegevens die geselecteerd zijn voor 5 jaar in minimaal twee kopieën tijd opgeslagen blijven bij Deloitte ten behoeve van de verantwoording en behoudt van bewijslast.

Methode 3: Medewerkers worden actief gevraagd te delen

Dit voorbeeld is gelijk aan methode 2, inclusief de voor en nadelen, alleen nu zijn het de VWS-medewerkers die zelf de juiste gegevens aanreiken. Een uitgangspunt hier is het vertrouwen in de zorgvuldigheid, volledigheid en medewerking van de medewerkers.

Methode 4: Bruto data wordt op overheidslocatie verwerkt door Deloitte

Deloitte kan ook de benodigde faciliteiten meenemen en het onderzoek ter plaatse uitvoeren. De data kan dan in bruto worden verwerkt binnen de faciliteiten van de rijksoverheid (on-premise).

Het voordeel is dat diverse risico's en bezwaren wegvallen, omdat de data niet buiten de rijksoverheid komt. Ook de langere termijnsopslag kan binnen de Rijksoverheid blijven. Het nadeel is dat Deloitte hun diensten in mobiele vorm moeten kunnen aanbieden en dat er hulp nodig is van SSC-ICT om een tijdelijke onderzoekruimte in te richten.

Methode 5: Bruto data wordt op overheidslocatie geselecteerd door een andere externe partij

Deze methode lijkt op methode 2 en methode 4 wat betreft de data selectiebeperking binnen de rijksoverheid. In dit scenario wordt gebruik gemaakt van alle bronnen en gefilterd door een andere partij die reeds tooling beschikbaar heeft binnen SSC-ICT.

Een bijkomend voordeel, naast de mogelijke tijdswinst, is dat VWS middels aantoonbaar en transparant kan handelen middels een vierogen principe. Deloitte kan hiermee geen zoekopdrachten geven die buiten de scope van het onderzoek vallen door de controlerende werking van een tweede bureau.

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e

Datum
9 september 2021

Documenten

Deloitte - Bijlage 6A - Data Processing Protocol NL.pdf
Deloitte - Bijlage 6B - Protocol digitaal onderzoek.pdf

Onberekende informatie (op moment van verwerking in dit rapport)

Wanneer de gegevens onverhoopt toch uitlekken kan dit grote gevolgen hebben. De volgende informatie is nog niet beschikbaar:

- Behandelingswijze van de data kopieën (overdracht/origineel, seal-bag backup en de ingeladen data op het e-Discovery platform) is onduidelijk.
    - Ook geen verzekering op wel/niet cloud gebruik of het voorkomen hiervan. In de offerte staat gespecificeerd dat tooling gehost op Amazone Web Services (AWS) wordt toegepast. In de communicatie is wel verklaard dat dit geen onderdeel zal vormen van het onderzoek, maar dit is niet objectief vast te stellen.

Gevolgen en schade

Wanneer de gegevens onverhoopt toch uitlekken kan dit grote gevolgen hebben voor het Ministerie van VWS. De data laat zich niet omvatten in enkel PBM-gerelateerde gegevens.
Kan bij langdurig falen van een of meer beveiligingsmaatregelen leiden tot langdurige (imago)schade van VWS of Rijksdienst:

- Financiële schade, voor de staat en door misbruik van bedrijfsinformatie.
- Imago schade voor VWS
- Diplomatieke schade
- Politieke schade

Lijnmanagers zijn verantwoordelijk voor de beveiliging van hun data volgens de VIR. Dit moet kunnen worden aangetoond in de jaarlijkse In Control Verklaring (ICV). Doordat de data buiten de rijksoverheid wordt geplaatst zal dit de verantwoording bemoeilijken.

Advies

Het advies is om methode 1 van de data selectie methoden niet in te zetten, omdat dit maximaal conflicteert met genoemde wet- en regelgeving. Ook al heeft deze methode de voorkeur van Deloitte gaat dit echt in strijd met de privacygedragscode, zoals beschreven in hoofdstuk 1. Deze privacygedragscode is goedgekeurd door de Autoriteit Persoonsgegevens en houdt in dat een particulier onderzoeksbureau verplicht is om proportionaliteit (evenredigheid van doel en middelen) en subsidiariteit (gematigdheid bij de inzet van middelen en methoden) in acht te nemen bij de gekozen onderzoeksmethoden- en middelen. Tevens spreekt dit het Data Processing Protocol (bijlage 6A) van Deloitte tegen waarin hun eerste doelstelling is "Selectie van veilig te stellen data wordt afgestemd met de opdrachtgever en er wordt expliciet besproken of dit in lijn is met (eventueel) toepasselijk intern beleid;".

Het uit handen geven van de volledige bruto dataset is per definitie een datalek of incident omdat er geen inzicht is in de informatie die buiten de organisatie wordt gebracht.

Ons dringende advies is om methode 4 of 5 van de data selectie methoden te kiezen, omdat duidelijk is dat de volledige brondata doorzocht moet kunnen worden met als uitgangspunt dataminimalisatie en zoveel mogelijk risico's te kunnen mitigeren. Wanneer op deze wijze data wordt geselecteerd en gemonitord, kunnen eigenaren van de data vooraf geïnformeerd worden dat de betreffende informatie wordt overgedragen voor onderzoek aan Deloitte.

De bevindingen uit deze risicoanalyse zijn een voorlopige en globale inschatting. Een volledige DPIA dient nog te worden uitgevoerd.

5.1.2e
Directie Informatiebeleid / CIO
5.1.2e

Datum
9 september 2021