Ministerie van Volksgezondheid,
Welzijn en Sport

5.1.2e
Directie Bestuurlijke en
Politieke Zaken
Bureau BVA en 1.2

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
Postbus 20350
2500 EJ Den Haag
www.rijksoverheid.nl

Inlichtingen bij
5.1.2e
5.1.2e

Datum
15 februari 2022

Aantal pagina's
3

memo

Advies 1.2 VWS DPIA Onderzoek Deloitte naar inkoop PBM

Inleiding

5.1.2e) is op grond van het bepaalde in artikel 35, tweede lid, van de Algemene verordening gegevensbescherming (AVG) geraadpleegd over gegevensbeschermingseffectbeoordeling - GEB, hierna te noemen DPIA. Onderstaand advies heeft betrekking op de DPIA Onderzoek Deloitte naar inkoop PBM ontvangen 11 februari 2022.

De AVG legt verantwoordelijkheid bij de organisatie om aan te tonen dat aan de privacyregels is voldaan. Deze verantwoordingsplicht (accountability) houdt in dat de organisatie moet kunnen aantonen dat de verwerkingen aan de regels van de (U)AVG voldoen. Het uitvoeren van een data privacy impact assessment (DPIA) voor gegevensverwerkingen met een hoog privacy risico is een verplichte maatregel voor de verantwoordingsplicht van een organisatie. Door te voldoen aan haar verantwoordingsplicht (accountability) levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

Een DPIA is een verplicht hulpmiddel om bij een voorgenomen verwerking van persoonsgegevens, de privacy risico's (dit wil zeggen de risico's voor de rechten, vrijheden en de effecten voor de betrokkenen) op een gestructureerde en heldere wijze in kaart te brengen en te beoordelen. Zodat op basis hiervan in een vroeg stadium maatregelen getroffen kunnen worden om deze effecten voor betrokkenen te voorkomen of te verkleinen. De DPIA dient de voornaamste (rest)risico's te benoemen, zodat de verwerkingsverantwoordelijke deze kan afwegen, waar mogelijk adresseren en eventueel accepteren.

Bronbestanden

- DPIA Onderzoek Deloitte naar inkoop PBM

Advies

De DPIA wordt de werkwijze beoordeeld die de minister heeft ontwikkelend beoordeeld die de minister heeft ontwikkeld voor het mogelijk maken van een onafhankelijk onderzoek door Deloitte naar eventuele onregelmatigheden bij de inkoop van PBM.

Ten aanzien van de onderliggende DPIA zijn de volgende opmerkingen te maken.

5.1.2e
Directie Bestuurlijke en Politieke Zaken
Bureau BVA en 1.2

Datum
1 februari 2022

1 Voorstel – H2

1.1 Aangegeven staat op pagina 3: 'In de eerste plaats worden (onderdelen van) databronnen met een persoonlijk karakter van de beperkte dataset uitgesloten. Deze eerste filtering wordt door VWS uitgevoerd.' Het is onduidelijk wat hier mee bedoeld wordt. Betekent dit dat een databron als de persoonlijke netwerkschijf (H-schijf bij VWS-kern) in zijn geheel uitgesloten wordt?

2 Gegevensverwerkingen – Randnummer 2.3

2.1. Uitlezen telefoons; (randnummer 2.3.13). Tijdens de stappen veilig stellen, selecteren is aangegeven dat de werkzaamheden door Deloitte plaatsvinden, zie tekst '.... overhandigt de betreffende medewerker zijn telefoon, inclusief toegangscode aan een medewerker van Deloitte'. Het advies is om de beschreven werkzaamheden van veilig stellen en selecteren door VWS plaats te laten vinden al dan niet in aanwezigheid van en of afstemming met Deloitte. Dit geeft helderheid ten aanzien van het moment van het ter beschikking stellen aan Deloitte.

2.2. In samenhang met voorgaande opmerking is het onduidelijk wat verstaan wordt bij stap 3 aanleveren: 'de gegevensdragers met daarop de geselecteerde gegevens worden overgedragen aan VWS. De gegevensdragers zijn toch immers al in het bezit van VWS en worden overdragen aan Deloitte.

3 Bewaartermijnen – Randnummer 2.10

3.1 Bewaartermijnen: het is onduidelijk hoe de bewaartermijn zich verhoudt tot de basis selectie lijst van de archiefwet. Daarnaast ontbreekt de bewaartermijnen van de gegevens in de steekproef. Verduidelijk dit.

4 Techniek en methode van gegevensverwerking

4.1 Aangegeven staat: 'In de eerste plaats worden (onderdelen van) databronnen met een persoonlijk karakter van de beperkte bruto dataset uitgesloten. Deze eerste filtering wordt door VWS uitgevoerd op basis van een zoekslag met een geselecteerd aantal zoektermen.' Het is onduidelijk wat hiermee bedoeld wordt. Vindt de selectie van de e-mails op basis van een zoektermenlijst plaats die e-mails uitsluit of juist de ter zake dienende e-mails selecteert? Wordt voor de selectie van de e-mails gebruik gemaakt van de reeds voor het Wob-proces ingericht proces? Verduidelijk dit.

5.1.2e
Directie Bestuurlijke en Politieke Zaken
Bureau BVA en 5.1.2e

Datum
1 februari 2022

5 Rechten van de betrokkene – Randnummer 3.5

5.1 Het is onduidelijk hoe invulling wordt gegeven aan de rechten van de betrokkenen. Verwezen wordt naar de webpagina <rijksoverheid.nl/privacy> waar betrokkenen terecht kunnen voor nadere informatie over de uitoefening van de bovengenoemde rechten. Echter dit is vrij algemeen en geeft geen duidelijkheid over de invulling van de rechten in relatie tot onderliggende verwerking.

6 Risico's – Randnummer 4

6.1 Risico 1; 'gegevens die moeten worden verwijderd, worden toch aan Deloitte verstrekt.' Hierbij staat aangegeven: 'De eerste maatregel is dat de bruto dataset wordt teruggebracht tot een beperkte bruto dataset, waarvan worden uitgesloten: persoonlijke datasets. Wat wordt verstaan onder persoonlijke datasets? Wordt hier de E-mailboxen van medewerkers die een relevante rol hebben gespeeld bij de inkoop van PBM (persoonlijk); en Persoonlijke Netwerkschijf (H-schijf bij VWS-kern) (persoonlijk) bedoeld? En zo ja, betekent dit dat deze beiden van uitgesloten worden? In de DPIA wordt niet ingegaan op de privacyrisico's rondom het raadplegen van e-mailboxen van de medewerkers. Op welke wijze vindt de selectie van e-mails plaats en welke maatregelen worden getroffen om te voorkomen dat niet ter zake dienende informatie (waaronder privé)zaken in het onderzoek onterecht meekomen.

6.2 Risico 2: Bij de maatregel staat aangegeven dat 'voor zover Deloitte onderzoek uitvoert voorafgaand aan de feitelijke overdracht van de dataschijven gebeurt dat op een locatie van VWS waarbij CISO toezicht houdt.' Het is onduidelijk wat hiermee bedoeld wordt.

6.3 Risico 4: Als maatregel staat aangegeven: 'De onderzoeker kan indien gewenst deze selectie direct toepassen op de laptop voordat de medewerker zelf start met de selectie van relevant chatverkeer per applicatie [onderlijning aangebracht door 5.1.2e . Het advies is om deze handeling niet door de onderzoeker maar door VWS te laten plaatsvinden. Dit draagt bij aan helderheid ten aanzien van het moment ter beschikking stellen van de aan Deloitte.

Bevindingen
5.1.2e onderschrijft de bevinding in de DPIA dat een onderbouwing ontbreekt dat is voldaan aan het subsidiariteitsvereiste. Waarmee onderbouwd wordt dat in redelijkheid niet gebruik gemaakt kan worden van een andere werkwijze die in minder vergaande mate inbreuk maakt op de rechten en vrijheden van betrokkenen. De FG adviseert de DPIA op bovenstaande punten aan te passen.

Acties naar aanleiding van Advies 5.1.2e
Leg vast welke acties naar aanleiding van het advies van 5.1.2e zijn uitgevoerd.

5.1.2e