Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020 **Aanhangsel van de Handelingen**

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2648

Vragen van het lid **Pia Dijkstra** (D66) aan de Ministers van Volksgezondheid, Welzijn en Sport en voor Medische Zorg over *het datalek van het Donorregister* (ingezonden 11 maart 2020).

Antwoord van Minister **De Jonge** (Volksgezondheid, Welzijn en Sport), mede namens de Minister voor Medische Zorg (ontvangen 30 april 2020).

Vraag 1
Klopt het dat u op 9 maart 2020 op de hoogte bent gesteld over het datalek dat zich heeft voorgedaan bij het Donorregister, of was u hierover al eerder geïnformeerd?[1]

Antwoord 1
Mijn ministerie is vrijdag 6 maart mondeling door de algemeen directeur van het CIBG geïnformeerd over een waarschijnlijk datalek. Tijdens dit gesprek zijn afspraken gemaakt over het aanmelden van het datalek bij de Autoriteit Persoonsgegevens (AP) en is het CIBG gevraagd een brief op te stellen waarin zij uitleg geven over dit datalek. Ik heb deze brief van het CIBG op maandag 9 maart ontvangen waarna ik de Kamer op 10 maart heb geïnformeerd.

Vraag 2
Op welk moment zijn precies de persoonsgegevens overgezet naar de twee harde schijven?

Antwoord 2
Het inscannen van de papieren registratieformulieren was onderdeel van het digitaliseringsproject van het Donorregister. Voor dit project heeft het CIBG de Belastingdienst gevraagd om 6,9 miljoen donorkeuzeformulieren, zoals geregistreerd of gewijzigd in de periode van februari 1998 tot juni 2010, in te scannen. De Belastingdienst is hiermee op 1 december 2012 gestart en was op 25 oktober 2013 klaar. In deze periode heeft de Belastingdienst de externe harde schijven aangemaakt. In augustus 2015 zijn de externe harde schijven door de Belastingdienst overhandigd aan het CIBG.

[1] Brief van het agentschap CIBG «Onvindbare externe gegevensdrager Donorregister», 9 maart 2020. Bijlage bij Kamerbrief 2020Z04660, 10 maart 2020.

ah-tk-20192020-2648
ISSN 0921 - 7398
's-Gravenhage 2020

Vraag 3
Op welk moment was het CIBG voor het eerst op de hoogte van de vermissing van de twee externe harde schijven? Was deze ontdekking al begin 2020 gedaan, op het moment dat begonnen werd met de vernietiging van het papieren archief?

Antwoord 3
Conform het Vervangingsbesluit Donor archief 1998–2010 CIBG zijn alle papieren gegevens vervangen door digitale kopieën. Hierdoor was het bewaren van een digitaal of papieren archief niet meer nodig. In februari 2020 is gestart met het vernietigen van het papieren archief door Doc-Direkt en het vernietigen van het digitale archief door het CIBG zelf. De vernietiging van het papieren archief was op 26 februari 2020 afgerond. Met betrekking tot het digitale archief heeft het CIBG op 20 februari 2020 ontdekt dat de externe harde schijven niet in de kluis lagen. Het CIBG heeft toen een interne zoekactie opgestart. Op 4 maart 2020 heeft het CIBG geconcludeerd dat de externe harde schijven vermist waren. Deze vermissing is op diezelfde dag door de privacy officer van het CIBG als datalek aangemerkt.

Vraag 4
Klopt het dat, na aanmerking van de vermissing als een datalek door de privacy officer van het CIBG, dit direct gemeld is aan de Autoriteit Persoonsgegevens (AP) en dit dus op 6 maart 2020 plaatsvond?

Antwoord 4
De vermissing van de externe harde schijven is door het CIBG op 4 maart 2020 als een datalek aangemerkt. Een datalek moet, binnen de wettelijke termijn van 72 uur na aanmerking, worden gemeld bij de Autoriteit Persoonsgegevens (AP). De privacy officer van het CIBG heeft het datalek op 6 maart 2020, binnen deze wettelijke termijn, gemeld bij de AP.

Vraag 5
Wat was de reactie van de AP op het datalek? Heeft de AP aanbevelingen gedaan over mogelijke vervolgstappen en worden deze opgevolgd? Zo ja, wat waren deze aanbevelingen precies en hoe wordt hier gevolg aan gegeven? Zo nee, waarom niet?

Antwoord 5
De AP doet geen uitspraken over het verloop en de inhoud van onderzoek dat door hen wordt uitgevoerd. Conform mijn toezegging informeer ik uw Kamer over de uitkomsten van het onderzoek van de AP en de Audit Dienst Rijk (ADR).

Vraag 6
Van hoeveel unieke personen stonden hun persoonsgegevens op de twee vermiste harde schijven? Worden deze mensen persoonlijk van het datalek op de hoogte gesteld?

Antwoord 6
Het CIBG heeft vastgesteld dat het om 6.058.250 unieke personen gaat, inclusief personen die thans overleden zijn. Op de externe harde schijven waren 6,9 miljoen gescande registratie- en wijzigingsformulieren opgeslagen; sommige personen hebben meerdere formulieren ingediend, waardoor het aantal formulieren en het aantal unieke personen niet overeenkomt.
Het CIBG heeft besloten om via de website van het donorregister de burgers te informeren over het datalek en de mogelijke gevolgen. Het CIBG heeft daarnaast een apart telefoonnummer ingesteld waar burgers met vragen terecht kunnen.

Vraag 7
Kunt u toelichten wat precies bedoeld wordt met de passage «hoogstwaarschijnlijk niet zijn beveiligd»? Waarom is het niet bekend of deze externe harde schijven beveiligd zijn?

Antwoord 7
Het CIBG heeft aangegeven dat na verder intern onderzoek duidelijk is geworden dat de externe harde schijven inderdaad niet waren beveiligd. Nog onbekend is waarom de externe harde schijven niet zijn beveiligd. Deze vraag zal ook in het onderzoek van de ADR worden meegenomen. Zoals toegezegd wordt de Kamer geïnformeerd over de uitkomst van dit onderzoek.

Vraag 8
Kunt u aangeven wanneer precies de twee verhuizingen van het Donorregister, waarover gesproken wordt in de brief, plaatsvonden? Is de kluis waarin de externe harde schijven zich bevonden tijdens beide verhuizingen meeverhuisd?

Antwoord 8
Het CIBG geeft aan dat op 18 en 19 februari 2016 de verhuizing van de CIBG-vestiging in Kerkrade plaatsvond naar de nieuwe vestiging in Heerlen. Bij deze verhuizing zijn de externe harde schijven meeverhuisd maar is de betreffende kluis in Kerkrade niet meeverhuisd. Het CIBG heeft in Heerlen beschikking gekregen over een andere kluis. De andere verhuizing vond plaats op 17 en 18 mei 2018 binnen hetzelfde gebouw in Heerlen. Tijdens deze interne verhuizing is de kluis waarvan het CIBG gebruikmaakt in Heerlen niet verplaatst.

Vraag 9
Hoeveel beveiligingsprotocollen en werkinstructies zijn er precies? Kunt u per protocol en instructie aangeven wanneer deze voor het laatst geëvalueerd zijn en welk proces is ingericht om deze instructies en protocol bijgewerkt te houden?

Antwoord 9
Het CIBG volgt ten aanzien van (informatie)beveiliging de Rijksbrede richtlijnen die gebaseerd zijn op de Baseline Informatiebeveiliging Overheid 2019 (BIO). De BIO bevat zeer uitgebreide personele, technische, organisatorische en fysieke maatregelen, procedures en ondersteunende producten. De vraag hoeveel protocollen en werkinstructies het CIBG heeft ten aanzien van dit onderwerp, wanneer deze geëvalueerd zijn en welke ondersteunende processen zijn ingericht, wordt meegenomen in het onderzoek van de ADR waarover ik de Kamer zal informeren.

Vraag 10
Klopt het, gezien het feit dat geschreven wordt dat «aanwezige beveiligingsprotocollen en (werk)instructies onvoldoende zijn nageleefd», dat het datalek niet plaats had kunnen vinden indien de beveiligingsprotocollen en (werk)instructies wel waren nageleefd? Zo ja, waarom wordt dan ook gesproken over een herziening en aanscherping van deze instructies en protocollen?

Antwoord 10
In het onderzoek dat de ADR gaat uitvoeren zal worden ingegaan op de naleving van de beveiligingsprotocollen en werkinstructies binnen het CIBG rondom dit onderwerp. Ik zal de Kamer informeren over de uitkomst van dit onderzoek.

Vraag 11
Kunt u aangeven wanneer de eventuele aanscherping en herziening van de beveiligingsprotocollen en (werk)instructies gereed is?

Antwoord 11
De ADR en de AP gaan onafhankelijk onderzoek doen naar het datalek, het CIBG zal deze onderzoeksresultaten meenemen in de evaluatie en waar nodig aanscherping van bestaande beveiligingsprocedures en werkinstructies.
Het CIBG zal vooruitlopend op de uitkomsten van deze onafhankelijke onderzoeken, de komende periode reeds onderzoeken welke interne veranderingen met voorrang doorgevoerd kunnen worden.

Vraag 12
Wie ziet toe op de naleving van de beveiligingsprotocollen en (werk)instructies?

Antwoord 12
Naleving van de beveiligingsprotocollen bij het CIBG is in de reguliere managementlijn belegd en valt onder de verantwoordelijkheid van de waarnemend Chief Information Officer (CIO) van het CIBG. Bij het CIBG zijn de Chief Security Information Officer (CISO) en Privacy Officer van het CIBG belangrijke kaderstellers. In het onderzoek van de ADR zal de vraag worden meegenomen wie welke rol en verantwoordelijkheid heeft in de naleving van de beveiligingsprotocollen.

Vraag 13
Was de kluis waarin de externe harde schijven zich bevonden afgesloten of had iedereen toegang tot deze kluis?

Antwoord 13
Zowel de kluis op de locatie Kerkrade, als de kluis op de locatie Heerlen, waren afgesloten. In Kerkrade werd de sleutel beheerd door de afdeling Functioneel Beheer van het CIBG. In Heerlen werd de sleutel beheerd door twee aangewezen medewerkers van het CIBG. CIBG-medewerkers konden met toestemming van de personen met een sleutel toegang krijgen tot de kluis. De (naleving van de) procedure m.b.t. de toegang tot de kluizen wordt meegenomen in het onderzoek van de ADR.

Vraag 14
Kunt u toelichten wat wordt bedoeld met de passage «de zoektocht naar de externe schijven wordt voortgezet»? Wie voert deze zoektocht uit en is er aangifte gedaan bij de politie?

Antwoord 14
Het CIBG heeft geen aangifte gedaan bij de politie, er zijn geen aanwijzingen of vermoedens dat de externe harde schijven zijn ontvreemd. Enkele medewerkers van het CIBG zijn tot en met 12 maart ingezet voor de aanvullende zoektocht, deze is inmiddels afgerond. De schijven zijn echter nog steeds vermist.

Vraag 15
Bent u bereid de Kamer te informeren op het moment dat u meer weet over hoe deze datalek precies heeft kunnen gebeuren?

Antwoord 15
Ja, zoals ik in mijn brief van 10 maart jl. heb aangegeven, ben ik voornemens om de Kamer van de uitkomsten van de onderzoeken van de AP en de ADR op de hoogte te stellen.

Vraag 16
Kunt u toelichten wat u bedoelt met het feit dat u «geen signaal ontvangen van onbevoegde kennisname van de gegevens op de externe harde schijven»? Op welke wijze zou u hiervan signalen ontvangen?

Antwoord 16
Het CIBG heeft nauw contact met het Centraal Meldpunt Identiteitsfraude en -fouten van de Rijksdienst voor Identiteitsgegevens (RvIG). Tot op heden zijn bij dit meldpunt geen meldingen gedaan van identiteitsfraude waarbij een verband kan worden gelegd met dit datalek.
Het CIBG en de Nederlandse Transplantatie Stichting monitoren daarnaast of er ongebruikelijke of ongewone berichten worden ontvangen waarin wordt verwezen naar gegevens die ook op de externe harde schijven stonden. Ook monitort het CIBG via het klantencontactcentrum of er signalen binnenkomen die verband kunnen houden met het datalek. Tot slot wordt berichtgeving door de media nauwlettend gevolgd. Tot op heden heeft de monitoring nog geen vermoeden van onbevoegde kennisname van de gegevens opgeleverd.

Vraag 17
Wat is de precieze onderzoeksvraag die aan de Auditdienst Rijk (ADR) is meegegeven voor hun onderzoek? Is al bekend wanneer dit ADR-onderzoek gereed is?

Antwoord 17
De ADR is verzocht een onafhankelijk onderzoek uit te voeren naar de wijze waarop binnen het CIBG wordt omgegaan met externe gegevensdragers. Zowel de opzet van het beleid als het bestaan van beheersmaatregelen ten aanzien van het huidige en toekomstige donorregister.
De ADR is bereid dit onderzoek uit te voeren en zal naar verwachting uiterlijk eind mei 2020 een rapportage opleveren.

Vraag 18
Welke stappen wilt u en/of het CIBG zetten om het geschade vertrouwen in het Donorregister en de zorgvuldige omgang van persoonlijke gegevens van mensen te herstellen, aanvullend aan de stappen die reeds in de brief staan?

Antwoord 18
Het is vanuit het oogpunt van het publieke vertrouwen heel belangrijk dat er openheid van zaken is, niet alleen over wat er is gebeurd en de (mogelijke) consequenties die dit kan hebben, maar ook over wat er wordt gedaan om eenzelfde fout in de toekomst te voorkomen. Ik zal de Kamer daarom informeren over de uitkomsten van de onderzoeken door de ADR en AP en het CIBG vragen om eventueel te nemen vervolgstappen aan mij te rapporteren en deze openbaar te maken.
Het CIBG zal zoals gezegd, vooruitlopend op de uitkomsten van de onafhankelijke onderzoeken door de ADR en AP, de komende periode zelf onderzoeken welke interne veranderingen met voorrang doorgevoerd kunnen worden. Overigens is bij de bouw van het nieuwe Donorregister begin 2019 security by design en privacy by design in de infrastructuur ingeregeld. Persoonsgegevens kunnen in het nieuwe donorregister alleen opgevraagd worden via een gecontroleerd proces. Een voorbeeld hiervan is dat persoonsgegevens in het nieuwe donorregister versleuteld worden opgeslagen. Hierdoor kan zelfs een systeembeheerder niet bij deze persoonsgegevens.

Vraag 19
Kunt u deze vragen voor de inbrengdatum van het door de commissie Volksgezondheid, Welzijn en Sport afgesproken schriftelijke overleg apart beantwoorden?

Antwoord 19
Nee, in verband met de COVID-19 uitbraak is het mij niet gelukt deze vragen voorafgaand aan het schriftelijke overleg aan de Kamer te zenden.