Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023 **Aanhangsel van de Handelingen**

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

2583

Vragen van de leden **Minhas** en **Rajkowski** (beiden VVD) aan de Staatssecretarissen van Infrastructuur en Waterstaat en van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «NS waarschuwt honderdduizenden klanten vanwege datalek»* (ingezonden 29 maart 2023).

Antwoord van Staatssecretaris **Van der Burg** (Justitie en Veiligheid) (ontvangen 15 mei 2023).

Vraag 1
Bent u bekend met het bericht «NS waarschuwt honderdduizenden klanten over mogelijk lekken van persoonsgegevens»?[1]

Antwoord 1
Ja, ik ben bekend met dit bericht.

Vraag 2
Wat is uw reactie op het feit dat de privégegevens van honderdduizenden klanten op deze manier op straat zijn komen te liggen?

Antwoord 2
Ik betreur dat persoonsgegevens van NS-klanten mogelijk onderdeel zijn van een hack bij een betrokken partij bij reizigerstevredenheidsonderzoeken. De privacy van reizigers die hun medewerking verlenen aan deze onderzoeken, moet beschermd zijn.

Vraag 3
Is inmiddels bekend op welke wijze de gegevens op straat zijn beland? Komt dit door een hack bij de softwareleverancier of door onzorgvuldige beveiliging van de persoonsgegevens?

Antwoord 3
Marktonderzoeker Blauw is door NS ingeschakeld voor het uitvoeren van verschillende reizigerstevredenheidsonderzoeken. Subverwerker Nebu uit Wormerveer levert het softwareplatform waarop Blauw haar onderzoeken uitvoert. Nebu is, volgens Blauw, gehackt en tijdens die hack is alle data van

[1] NOS, 28 maart 2023, «NS waarschuwt honderdduizenden klanten vanwege datalek,» https://nos.nl/artikel/2469236-ns-waarschuwt-honderdduizenden-klanten-vanwege-datalek.

ah-tk-20222023-2583
ISSN 0921 - 7398
's-Gravenhage 2023

klanten en onderzoeken gedownload (geëxfiltreerd). Het is echter nog niet zeker welke data precies zijn gelekt en of ook NS-data onderdeel waren van het datalek.

Vraag 4
Het datalek is volgens de berichtgeving niet ontstaan bij NS zelf, maar bij een softwareleverancier van het ingehuurde marktonderzoeksbureau dat klanttevredenheidsonderzoek doet in opdracht van NS. Kunt u aangeven welke afspraken NS maakt met externe partijen, teneinde de veiligheid van klantdata te maximeren?

Antwoord 4
Om de veiligheid van klantdata te beschermen, sluit NS met externe partijen een verwerkersovereenkomst. Daarin worden ook afspraken gemaakt over het inschakelen van een subverwerker.
Dit heeft NS ook met marktonderzoeksbureau Blauw gedaan. Deze verwerkersovereenkomst is afgesloten conform artikel 28 lid 3 AVG. In deze verwerkersovereenkomst zijn afspraken gemaakt over de verwerking van persoonsgegevens door Blauw en de beveiliging van persoonsgegevens. Ook zijn in deze verwerkersovereenkomst afspraken gemaakt over de inschakeling van een subverwerker door Blauw.

Vraag 5
Wat is de wettelijke grondslag op basis waarvan persoonsgegevens zijn verwerkt door NS, het marktonderzoeksbureau en diens softwareleverancier?

Antwoord 5
In het Privacystatement op de website van NS[2] is beschreven welke grondslag van toepassing is (zie onder «Marktonderzoek en wetenschappelijk onderzoek»). NS hanteert voor het NS panel onderzoek en het reizigersonderzoek de grondslag «toestemming» en voor het contactbelevingsonderzoek en overige klantonderzoeken de grondslag «gerechtvaardigd belang».

Vraag 6
Is er op enig moment een DPIA (data protection impact assessment) uitgevoerd voordat de gegevensverwerking tot stand werd gebracht? Zo nee, waarom niet?

Antwoord 6
NS heeft mij laten weten dat er een DPIA is uitgevoerd door NS. Deze verwerking is opgenomen in het register van verwerkingen van NS.

Vraag 7
Wist de NS op elk moment wie er van de softwareleverancier inzage had in de persoonsgegevens die werden verwerkt? Zo nee, wat vindt u daarvan?

Antwoord 7
NS was ervan op de hoogte dat Blauw subverwerker Nebu heeft ingeschakeld. NS heeft Blauw in de verwerkersovereenkomst specifieke schriftelijke toestemming gegeven om Nebu in te schakelen. Hieraan zijn evenwel specifieke condities verbonden. Bij NS is niet bekend welke medewerkers van Nebu inzage hebben (gehad) in persoonsgegevens.

Vraag 8
Vindt u dat er voldoende regels zijn omtrent de veiligheid van klantdata van publieke instellingen en bedrijven die met externe partijen werken en hun klantdata met deze partijen delen? Zo ja, waarom? Zo neen, waarom niet?

Antwoord 8
De Algemene Verordening Gegevensbescherming (AVG) verplicht ertoe dat wanneer persoonsgegevens worden verwerkt, de verwerkingsverantwoordelijke maatregelen neemt om te zorgen dat de verzamelde gegevens niet langer bewaard worden dan nodig is en dat organisatorische en technische

[2] www.ns.nl/privacy

maatregelen getroffen worden, zodat gegevens goed beveiligd en vertrouwelijk blijven. De verwerkingsverantwoordelijke moet kunnen aantonen dat aan deze zorgvuldigheidsnormen is voldaan. Wanneer voor de verwerking een externe partij wordt ingeschakeld, dan moeten diens taken in een overeenkomst worden vastgelegd. De genoemde zorgvuldigheidsnormen zijn ook dan onverkort van toepassing. Het ontbreekt dan ook niet aan regels omtrent de veiligheid van klantdata van publieke instellingen en bedrijven die met externe partijen werken en hun klantdata met deze partijen delen.

Vraag 9
Wat gaat u doen om te voorkomen dat kritieke data van klanten in de toekomst zonder strenge regels door externe partijen wordt gebruikt?

Antwoord 9
Elke organisatie die persoonsgegevens verwerkt is er in de eerste plaats zelf verantwoordelijk voor om dit volgens de regels te doen en er scherp op toe te zien dat dit ook daadwerkelijk gebeurt. De Autoriteit Persoonsgegevens (AP) heeft daarnaast een voorlichtende taak. Het Ministerie van Justitie en Veiligheid zorgt dat de AP beschikt over voldoende financiering voor de uitvoering van alle taken die samenhangen met de AVG, zo ook deze. In het Coalitieakkoord is daarom extra budget voor de AP opgenomen.