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

2731

Vragen van het lid **Slootweg** (CDA) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «Steekspel rond mysterieuze datadiefstal; Bedrijven delen data van klanten met hun leveranciers, maar hoe veilig is dat?»* (ingezonden 13 april 2023).

Antwoord van Minister **Weerwind** (Rechtsbescherming) mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 30 mei 2023).

Vraag 1
Bent u bekend met het bericht «Steekspel rond mysterieuze datadiefstal; Bedrijven delen data van klanten met hun leveranciers, maar hoe veilig is dat?»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u een update geven van het datalek bij Nebu en het aantal klanten en bedrijven en organisaties dat in Nederland getroffen is?

Antwoord 2
Op dit moment is het onduidelijk hoeveel klanten, bedrijven en organisaties in Nederland zijn getroffen door het datalek. Wel is bekend dat een van de klanten van Nebu, marktonderzoeker Blauw, een kort geding is gestart tegen Nebu. In dat kort geding heeft Blauw nadere informatie van Nebu gevorderd over de aanval, de gevolgen ervan en de door Nebu getroffen maatregelen. Ook heeft zij om een onafhankelijk forensisch onderzoek gevraagd. De voorzieningenrechter heeft in het vonnis van 6 april 2023 een groot deel van de vorderingen van Blauw toegewezen. Nebu moet Blauw uitgebreid informatie verschaffen over het datalek en vragen van Blauw beantwoorden. Daarnaast moet Nebu een onafhankelijk forensisch onderzoek naar het datalek laten uitvoeren.
Ten aanzien van Rijksoverheidsorganisaties is het volgende bekend. Binnen de rijksoverheid zijn voor zover bekend 16 organisaties geraakt, een aantal

[1] De Telegraaf, 8 april 2023, via https://www.telegraaf.nl/financieel/1167818643/steekspel-rond-mysterieuze-datadiefstal-alles-wat-fout-kan-gaan-gaat-fout

ah-tk-20222023-2731
ISSN 0921 - 7398
's-Gravenhage 2023

daarvan maken gebruik van meerdere bureaus voor marktonderzoek. De geraakte rijksorganisaties zijn het Ministerie van Economische Zaken en Klimaat, de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO), de Rijksdienst voor Ondernemend Nederland (RVO), het College ter beoordeling van Geneesmiddelen (CBG), het Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG), het Rijksinstituut voor Volksgezondheid en Milieu (RIVM), het Sociaal en Cultureel Planbureau (SCP), het Ministerie van Onderwijs, Cultuur en Wetenschap, de Koninklijke Bibliotheek, de Huurcommissie (DHC), de Dienst Publieke Communicatie (DPC) en de Raad voor Rechtsbijstand (RvR).
Betrokkenen binnen de rijksoverheid zijn burgers, eigen medewerkers, en medewerkers van reisbureaus, werkgeversorganisaties, onderwijsinstellingen, bedrijven en klanten. Gelekte gegevens betreffen naam, e-mailadres, telefoonnummer, (telefonische) enquêteresultaten/inhoud onderzoek. Waar relevant is melding gedaan bij de Autoriteit Persoonsgegevens. De omvang van het datalek varieert per organisatie. Zo zijn bij één van de organisaties de gegevens van één medewerker gelekt. En bij een andere organisatie, een onderzoeksbureau, zijn gegevens van 22.000 burgers gelekt met naam, emailadres en de resultaten van een onderzoek.
Met het antwoord op deze vraag wordt tevens tegemoetgekomen aan de toezegging uit het debat Informatiebeveiliging bij de overheid met de Staatssecretaris van Koninkrijksrelaties en Digitalisering van 5 april 2023 om de Tweede Kamer te informeren over het onderzoek naar getroffenen bij de rijksoverheid van het datalek bij Nebu.

Vraag 3
Klopt het dat een bedrijf of (overheids)organisatie zelf verantwoordelijk is voor de data die een klant met het bedrijf deelt, ook als het bedrijf die data met een externe partij deelt?

Antwoord 3
Ja, dat klopt. In de Algemene Verordening Gegevensbescherming (AVG) wordt een onderscheid gemaakt tussen de rol van «verwerkingsverantwoordelijke» en de rol van «verwerker».
Het bedrijf dat of de (overheids)organisatie die het doel en de middelen van een verwerking van persoonsgegevens bepaalt, is de «verwerkingsverantwoordelijke».
De verwerkingsverantwoordelijke is verantwoordelijk voor de verwerking van persoonsgegevens in overeenstemming met de AVG. Dit omvat ook de verplichting om passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen.
In de praktijk schakelen veel verwerkingsverantwoordelijken andere partijen in om voor hen persoonsgegevens te verwerken. Een dergelijke partij is de «verwerker». Ook verwerkers moeten passende technische en organisatorische maatregelen nemen om de persoonsgegevens te beveiligen, maar de verwerkingsverantwoordelijke blijft (eind)verantwoordelijk voor de naleving van de AVG.

Vraag 4
Wie is er volgens u aansprakelijk voor dit datalek? Is dat het bedrijf aan het begin van de keten die klantdata deelt of de externe partij bij wie het lek plaatsvindt?

Antwoord 4
Het is nog niet duidelijk welke partij aansprakelijk is voor het datalek bij Nebu. Er zijn meerdere partijen betrokken. In het geval van Nebu moet goed worden onderzocht wat er is afgesproken over de beveiliging en wat er nu feitelijk is gebeurd.
De rollen van verwerkingsverantwoordelijke en verwerker zijn omschreven in de AVG, maar partijen kunnen in een (verwerkers)overeenkomst nadere of andere afspraken maken over de aansprakelijkheid bij bijvoorbeeld een datalek. Partijen die betrokken zijn bij een datalek kunnen zich eventueel wenden tot de civiele rechter om de aansprakelijkheid en de omvang daarvan te laten vaststellen. In de vaststelling van aansprakelijkheid is geen rol voor de overheid weggelegd. Het is dan ook niet aan mij om hierover uitspraken te doen.

Vraag 5
Deelt u de mening dat het gevaar op datalekken vooral in de keten zit van partijen die samenwerken met bedrijven zoals IT-leveranciers, onderzoeksbureaus en andere partijen met wie (klant)data wordt gedeeld?

Antwoord 5
(Overheids)organisaties en bedrijven dienen de bepalingen die betrekking hebben op hun privacyrechtelijke rol van verwerkingsverantwoordelijke of verwerker uit de AVG na te leven, waaronder de bepalingen die zien op het beveiligen van persoonsgegevens. In de praktijk komt het voor dat de verwerker een sub-verwerker inschakelt voor de verwerking van (een deel van de) persoonsgegevens. Hiermee ontstaat de keten verwerkingsverantwoordelijke – verwerker – sub-verwerker. De AVG schrijft voor dat verwerkingsverantwoordelijke en verwerker afspraken dienen te maken over de verwerking van persoonsgegevens, maar ook dat de verwerker afspraken moet maken met de sub-verwerker voor de verwerking van persoonsgegevens, waaronder de beveiliging van persoonsgegevens.
Een verwerkingsverantwoordelijke of verwerker kan er bewust voor kiezen (een deel van de) verwerkingen uit te besteden aan een (sub-)verwerker met meer expertise op het gebied van onder meer beveiliging. Ook kan het voorkomen dat een (sub-)verwerker gecertificeerd is op het gebied van informatiebeveiliging terwijl de verwerkingsverantwoordelijke of verwerker die de sub-verwerker inschakelt, dit niet is. Het inschakelen van een andere partij biedt in een dergelijk geval voordelen. Ook wanneer de ingeschakelde (sub-)verwerker niet over een bepaalde expertise of certificering beschikt, betekent dit niet dat daarom de kans op datalekken toeneemt. Iedere ingeschakelde (sub-)verwerker dient immers de verplichtingen uit de AVG na te leven, waaronder het treffen van voldoende passende maatregelen om de persoonsgegevens te beschermen.
In zijn algemeenheid kan aldus niet worden gesteld dat het gevaar op datalekken vooral zit in de keten van partijen.

Vraag 6
Welke verantwoordelijkheid hebben bedrijven en (overheids)organisaties volgens u om digitaal verantwoord ondernemen in de keten te waarborgen?

Antwoord 6
Er zijn wettelijke kaders die reguleren hoe organisaties en bedrijven met bepaalde gegevens moeten omgaan. In de AVG zijn verschillende beginselen opgenomen die gelden bij iedere verwerking van persoonsgegevens.
Een van die beginselen is dat persoonsgegevens moeten worden verwerkt op een manier dat door het nemen van passende technische of organisatorische maatregelen een passende beveiliging ervan is gewaarborgd en dat persoonsgegevens onder neer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Ieder bedrijf en elke (overheids)organisatie die onder het toepassingsbereik van de AVG valt, dient uitvoering te geven aan dit beginsel door invulling te geven aan alle verplichtingen voor die partij zoals opgenomen in de AVG, zoals de verplichting om persoonsgegevens te beveiligen.
Binnen de kaders van de wet is het de eigen verantwoordelijkheid van bedrijven om hun weerbaarheid te verhogen. De overheid kan deze verantwoordelijkheid niet overnemen. Wel zet het Digital Trust Center («DTC») zich op verschillende manieren in om bedrijven te helpen met verantwoord digitaal ondernemen. Het DTC stimuleert en faciliteert ondernemers om zelfstandig of in samenwerkingsverband aan de slag te gaan met het verbeteren van hun cyberweerbaarheid. De doelgroep van ruim twee miljoen ondernemers in de zogenoemde «niet vitale» sectoren is zeer uiteenlopend. Via het DTC helpt het Ministerie van Economische Zaken en Klimaat deze ondernemers om hun digitale veiligheid te verhogen. Om bedrijven te informeren, deelt het DTC via website en social mediakanalen laagdrempelige kennis, informatie en advies over digitaal veilig ondernemen waar ondernemers zelf mee aan de slag kunnen. Ondernemers kunnen via verschillende tools inzicht krijgen in de cyberweerbaarheid van hun bedrijf, en kunnen via een zelfscan inventariseren in welke risicoklasse ze vallen. De uitkomsten van deze scans kan een bedrijf delen met een IT-dienstverlener, ketenpartners of een verzekeraar.

Om de digitale weerbaarheid in de keten te verhogen zet het DTC in op samenwerking. Via een landelijk dekkend netwerk van samenwerkingsverbanden worden bedrijven gestimuleerd de cyberweerbaarheid te vergroten en de risico's in de keten te verkleinen. In een cyberweerbaarheidsnetwerk werken ondernemers samen met andere organisaties aan het vergroten van de cyberweerbaarheid, binnen en tussen niet-vitale branches, sectoren en regio's. Het DTC stimuleert deze samenwerkingsverbanden in niet-vitale sectoren en kan in bepaalde gevallen ook ondersteunen door middel van een subsidie.
De DTC Community is een online community waarbij ondernemers zich vrijblijvend kunnen aansluiten. Deze omgeving biedt ondernemers de kans om, in een besloten omgeving, actuele en relevantie informatie over cybersecurity uit te wisselen. De DTC Community stimuleert op deze manier informatie-uitwisseling tussen ondernemers en cyberprofessionals. Meldingen van bedrijfsspecifieke kwetsbaarheden waar het DTC kennis van heeft, deelt het direct met betrokken bedrijven. Dit biedt bedrijven de mogelijkheid om snel te reageren en mitigerende maatregelen te treffen. In 2023 zijn al ruim 13.000 notificaties naar Nederlandse bedrijven verzonden over digitale kwetsbaarheden.

Vraag 7
Schiet de huidige regelgeving niet tekort als een externe partij waar een datalek plaatsvindt niet meewerkt aan onderzoek en geen informatie deelt over het datalek? Hoe kan een externe partij gedwongen worden om informatie te delen, zodat consumenten weten waar zij aan toe zijn? Deelt u de mening dat de consument in dit geval onvoldoende wordt beschermd?

Antwoord 7
De verwerkingsverantwoordelijke is op grond van de AVG verplicht een melding te doen van een datalek bij de nationale toezichthouder (de Autoriteit Persoonsgegevens), tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. In sommige gevallen moet de verwerkingsverantwoordelijke het datalek ook melden aan de betrokkenen. Voor het doen van deze melding(en) heeft de verwerkingsverantwoordelijke informatie nodig over de omvang en de aard van het datalek. Als het datalek bij een verwerker heeft plaatsgevonden, is de verwerker de aangewezen partij om de verwerkingsverantwoordelijke in te lichten. De verwerker is dat ook verplicht op grond van de AVG.
Naast deze wettelijke verplichting die op de verwerker rust, worden er in de praktijk vaak afspraken gemaakt in de verwerkersovereenkomst over de wijze waarop de verwerker de informatie aan de verwerkingsverantwoordelijke dient te verschaffen en binnen welke termijn. Omdat de termijn waarbinnen de verwerkingsverantwoordelijke de melding aan de gegevensautoriteit moet doen slechts 72 uur bedraagt nadat de verwerkingsverantwoordelijke kennis geeft genomen van het datalek, worden doorgaans ook korte termijnen aangehouden in de verwerkersovereenkomst. Partijen kunnen in de overeenkomst afspreken dat wanneer een partij de contractuele afspraken schendt, deze partij boetes moet betalen aan de andere partij.
Indien de verwerker desondanks het voorgaande geen informatie verstrekt, kan de verwerkingsverantwoordelijke zich wenden tot de civiele rechter. Afhankelijk van de door de verwerkingsverantwoordelijke ingestelde vorderingen, kan de civiele rechter bepalen dat de verwerker nadere informatie moet verschaffen over de aard en de omvang van het datalek. De civiele rechter kan een dergelijke veroordeling versterken met fikse dwangsommen. Gelet op het bovenstaande is geen reden om te veronderstellen dat het huidig kader tekortschiet.

Vraag 8
Zijn er regels voor bedrijven ten aanzien van het bewaren van klantgegevens binnen het bedrijf of bij een externe partij? Zo nee, waarom niet?

Antwoord 8
De AVG bepaalt dat persoonsgegevens niet langer mogen worden bewaard dan nodig voor het doel waarvoor ze verzameld zijn. In de AVG zijn geen concrete bewaartermijnen omschreven omdat dit in zijn algemeenheid niet mogelijk is; daar wordt in de praktijk invulling aan gegeven. De verwerkings-

verantwoordelijke kan met inachtneming van de regels van de AVG dus zelf bewaartermijnen vaststellen. In sommige gevallen zijn wel wettelijke bewaartermijnen voorgeschreven. Een medisch dossier moet door een zorgverlener bijvoorbeeld 20 jaar bewaard worden op basis van de Wet op de geneeskundige behandelingsovereenkomst.
Is geen sprake van een wettelijke bewaartermijn, dan legt de verwerkingsverantwoordelijke zelf vastgestelde bewaartermijnen op aan de externe partij (de verwerker). De verwerker mag niet zelf bepalen hoe lang de persoonsgegevens van de verwerkingsverantwoordelijke worden bewaard.
In de AVG is bepaald dat na afloop van de verwerkingsdiensten door de verwerker, de verwerker alle persoonsgegevens moet wissen of aan de verwerkingsverantwoordelijke moet terugbezorgen. Ook moeten alle kopieën door de verwerker worden gewist. Naast deze wettelijke plicht kunnen verwerkingsverantwoordelijke en verwerker in de verlichte verwerkersovereenkomst nadere afspraken maken over de bewaartermijnen. Partijen kunnen bijvoorbeeld afspreken dat bij het schenden van de contractuele afspraken ten aanzien van de bewaartermijnen, contractuele boetes zullen worden verbeurd.

Vraag 9
Hoe zorgt u ervoor dat in ieder geval binnen de overheid altijd wordt samengewerkt met partijen die hun informatiebeveiliging op orde hebben?

Antwoord 9
De overheid mitigeert risico's door het uitvoeren van een zorgvuldig inkoopproces. Met geselecteerde (keten)partijen wordt vervolgens een verwerkersovereenkomst of overeenkomst gegevensdeling overeengekomen. In deze overeenkomsten worden de afspraken vastgelegd hoe een (keten)partij de persoonsgegevens dient te beschermen, welk beveiligingsniveau met elkaar is overeengekomen en hoe een (keten)partij moet handelen in geval van een datalek.

Vraag 10
Klopt het dat er Europese regelgeving aankomt, zoals de Digital Operational Resilience Act en de Netwerk- en Informatiebeveiligingsrichtlijn 2, die ervoor zorgen dat er meer eisen aan de beveiliging van klantdata gesteld worden? Zo ja, om welke regels gaat het en hoe zorgt dit ervoor dat data-uitwisseling tussen bedrijven en (overheids)organisaties en externe partijen in de keten beter wordt beveiligd?

Antwoord 10
Europese regelgeving, zoals de Netwerk- en Informatiebeveiligingsrichtlijn 2 (NIS-2) en de Digital Operational Resilience Act, stelt nadere eisen aan de beveiliging van netwerk- en informatiesystemen. Zij hebben echter betrekking op specifieke en vast gedefinieerde sectoren en organisaties. Daarmee zorgen ze er niet voor dat in generieke zin er nadere eisen aan de beveiliging van klantdata worden gesteld.