Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

Aanhangsel van de Handelingen

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

1560

Vragen van de leden **El Boujdaini** en **Schoonis** (beiden D66) aan de Minister van Economische Zaken en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «Hack bij Odido, gegevens miljoenen klanten in handen van criminelen»* (ingezonden 17 februari 2026).

Antwoord van Staatssecretaris **Van Bruggen** (Justitie en Veiligheid) en de Staatssecretaris van Economische Zaken en Klimaat (ontvangen 8 april 2026). Zie ook Aanhangsel Handelingen, vergaderjaar 2025–2026, nr. 1305.

Vraag 1
Bent u bekend met het bericht van de NOS over de cyberaanval bij Odido waarbij gegevens van circa 6,2 miljoen accounts zijn buitgemaakt door criminelen?[1]

Antwoord 1
Ja.

Vraag 2
Hoe beoordeelt u de omvang en ernst van dit datalek, mede gezien het feit dat ook gevoelige persoonsgegevens, zoals identiteitsdocumentnummers en rekeningnummers, mogelijk zijn gelekt?

Antwoord 2
De schaal van dit datalek, de hoeveelheid getroffen burgers en de soms gevoelige aard van de gelekte persoonsgegevens maken dit tot een bijzondere situatie. Het maakt duidelijk dat datalekken grote gevolgen kunnen hebben. Zonder iets te willen of kunnen zeggen over de oorzaken van het onderhavige datalek, maakt dit in meer algemene zin duidelijk dat een goede bescherming van persoonsgegevens zoals onder meer vereist in de Algemene Verordening Gegevensbescherming (AVG) noodzakelijk is en een integraal onderdeel moet zijn van primaire bedrijfsprocessen. De gevraagde beoordeling van dit datalek is uiteindelijk aan de Autoriteit Persoonsgegevens (AP) en Rijksinspectie Digitale Infrastructuur (RDI) als onafhankelijke toezichthouders. Daarnaast doet de politie onder leiding van het Landelijk Parket onderzoek naar de aanval en de daders.

[1] NOS.nl, 12 februari 2026, «Hack bij odido, gegevens miljoenen klanten in handen van criminelen»

ah-tk-20252026-1560
ISSN 0921 - 7398
's-Gravenhage 2026

Vraag 3
In hoeverre heeft deze cyberaanval gevolgen voor de digitale veiligheid en weerbaarheid van Nederland, gezien de maatschappelijke rol van telecomproviders?

Antwoord 3
De precieze gevolgen voor de digitale veiligheid en weerbaarheid van Nederland zullen nog moeten blijken. Odido heeft klanten gewaarschuwd waar zij alert op moeten zijn om misbruik zoveel mogelijk te voorkomen. Vanwege hun maatschappelijk rol hebben telecomoperators zoals Odido een zorgplicht onder de Telecommunicatiewet. Onder die zorgplicht moeten zij passende technische en organisatorische maatregelen nemen om risico's voor de beveiliging van hun netwerken of diensten te beheersen, naast de vergelijkbare verplichting die ook voortvloeit uit de AVG. Hieronder vallen ook bijbehorende diensten zoals een klantsysteem. De RDI houdt hier toezicht op. De Staatssecretaris van Economische Zaken heeft op dit moment geen signalen dat andere telecomoperators ook kwetsbaar zijn door deze specifieke hack. RDI blijft scherp kijken naar de verplichtingen op basis van de zorgplicht.

Vraag 4
Hoe beoordeelt u het risico dat de bij Odido gestolen persoonsgegevens in de toekomst alsnog openbaar worden gemaakt, en welke gevolgen kan dit hebben voor de veiligheid en privacy van betrokken burgers?

Antwoord 4
De bij Odido gestolen persoonsgegevens zijn inmiddels gepubliceerd.[2] In algemene zin geldt dat een dergelijke grootschalige publicatie in ieder geval het risico verhoogt op diverse vormen van oplichting en fraude zoals gerichte phishing en social engineering. Onder andere Odido, Veiliginternetten.nl, de politie en de AP communiceren naar aanleiding van het datalek actief waarvoor gestolen gegevens kunnen worden misbruikt en geven tips om gevolgen van het datalek zoveel mogelijk tegen te gaan.[3]

Vraag 5
Heeft Odido het datalek tijdig gemeld bij de Autoriteit Persoonsgegevens en andere relevante instanties, en bent u op de hoogte van eventuele lopende onderzoeken?

Antwoord 5
De AP heeft laten weten dat Odido het datalek tijdig heeft gemeld bij de AP. Odido geeft aan daarnaast proactief relevante overheidsinstanties, waaronder de RDI, te hebben geïnformeerd. De RDI is op basis van de verkregen informatie mogelijke vervolgstappen aan het onderzoeken. De AP meldt op haar website dat zij aanleiding ziet om tot formeel onderzoek over te gaan.[4]

Vraag 6
Is er volgens uw inschatting sprake van nalatigheid of onvoldoende naleving van de Europese privacy- en beveiligingsverplichtingen, zoals de Algemene verordening gegevensbescherming (AVG), door Odido?

Antwoord 6
Het is niet aan het kabinet om dit te beoordelen. Dit is in eerste instantie aan de AP. De taken en bevoegdheden om op te treden tegen overtredingen zijn vastgelegd in de AVG. De AP kan daartoe handhaven, advies verstrekken, samenwerken met andere toezichthoudende autoriteiten en klachten behandelen over een inbreuk op de bescherming van persoonsgegevens. De AP toetst daarnaast of sprake is van strijdigheid met de Europese gegevensbeschermingsregels.

---

[2] NOS.nl, 1 maart 2026, «Odido hackers publiceren resterende klantdata, ook miljoenen ID-nummers»

[3] https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/slachtoffer-van-een-datalek-dit-kunt-u-doen

[4] https://www.autoriteitpersoonsgegevens.nl/actueel/ap-en-rdi-starten-onderzoek-naar-odido

Vraag 7
Welke risico's lopen getroffen klanten en acht u de door Odido genomen maatregelen voldoende om deze risico's te beperken?

Antwoord 7
Zie het antwoord op de vraag 4. De vraag of Odido voldoende maatregelen heeft genomen om te voldoen aan de zorgplicht uit de Telecommunicatiewet en de AVG is aan de toezichthouders om te beoordelen.

Vraag 8
Welke eisen worden momenteel gesteld aan telecomproviders ten aanzien van cyberbeveiliging en gegevensbescherming en voldoen deze volgens u nog aan de huidige dreigingscontext?

Antwoord 8
Het toepasselijke normenkader stelt de strikte vereisten die noodzakelijk zijn voor een goede bescherming in een steeds veranderende dreigingscontext. Zoals aangegeven in het antwoord op vraag 3 valt Odido onder de zorgplicht van de Telecommunicatiewet. Onder de zorgplicht dienen aanbieders passende technische en organisatorische maatregelen te nemen om risico's voor de beveiliging van hun netwerken of diensten te beheersen. Dit moet zorgen voor een veiligheidsniveau dat is afgestemd op risico's die zich voordoen. De RDI ziet toe op de naleving van de vereisten van deze zorgplicht.
Daarnaast zijn telecomproviders gebonden aan de AVG, waaronder de beginselen van behoorlijke gegevensverwerking. Het beginsel van dataminimalisatie houdt bijvoorbeeld in dat organisaties alleen persoonsgegevens mogen verzamelen en verwerken die strikt noodzakelijk zijn voor een vooraf bepaald, specifiek doel. Op verwerkingsverantwoordelijken rust daarnaast de verplichting om passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen. Deze beveiligingsmaatregelen dienen een op de risico's voor de rechten en vrijheden van personen afgestemd beveiligingsniveau te waarborgen en rekening te houden met de stand van de techniek, alsook met de aard, omvang, context en doeleinden van de verwerking. Het waarborgen van passend bewustzijn van de beveiligingsrisico's bij personen die toegang hebben tot de te verwerken gegevens is daarbij van belang. Verwerkingsverantwoordelijken dienen hun beveiligingsmaatregelen doorlopend te evalueren en zo nodig aan te passen aan nieuwe risico's, waaronder nieuwe cyberdreigingen. Op grond van de AVG fungeert de Functionaris gegevensbescherming (FG) als onafhankelijk adviseur en ziet toe op de naleving van het gegevensbeschermingsrecht waaronder de te nemen maatregelen.
Het Nationaal Cyber Security Centrum staat rond actuele kwetsbaarheden en cyberdreigingen in nauw contact met partners binnen de telecomsector en werkt onder meer samen via het telecomgerichte Information Sharing and Analysis Center (ISAC).
EZK werkt samen met de telecomoperators in het Nationaal Continuïteit Overleg Telecom (NCOT) om gezamenlijk aan de continuïteit van de telecomdienstverlening te werken in het kader van de huidige dreiging.

Vraag 9
Ziet u aanleiding om aanvullende eisen of toezichtmaatregelen te treffen richting telecomproviders om grootschalige datalekken te voorkomen?

Antwoord 9
Op dit moment ziet de Staatssecretaris van Economische Zaken geen aanleiding om aanvullende eisen te stellen richting telecomproviders om grootschalige datalekken te voorkomen. Zoals uiteengezet in het antwoord op vraag 8 zijn onder de toepasselijke wet- en regelgeving, waaronder de Telecomwet en de AVG, organisaties zelf verantwoordelijk voor het nemen van passende maatregelen om, mede gelet op de huidige dreigingscontext, (grootschalige) datalekken te voorkomen. Het is aan de toezichthouders om daarop toe te zien en in dit verband de nodige toezichtmaatregelen te treffen. Dit is niet aan mij als bewindspersoon.

Vraag 10
Welke rol ziet u voor de overheid bij het ondersteunen van bedrijven en burgers bij het beperken van schade na grootschalige datalekken?

Antwoord 10
De AP ziet als onafhankelijke toezichthouder toe op de naleving van de AVG en kan handhavend optreden wanneer organisaties tekortschieten. Daarnaast heeft de toezichthouder een belangrijke rol in voorlichting. Door het geven van uitleg, richtsnoeren en praktische handvatten ondersteunt de toezichthouder organisaties en burgers bij de toepassing van de AVG en het uitoefenen van hun rechten.
Ook Veiliginternetten.nl geeft adviezen in deze casus. Dit is een publiek-private website om neutrale informatie over digitale veiligheid te verstrekken aan burgers. Het Nationaal Cyber Security Centrum (NCSC) deelt via openbare kanalen diverse adviezen en richtlijnen over cybersecurity, zoals beveiligingsadviezen, dreigingsinformatie en maatregelen om digitale incidenten te voorkomen of te beperken. Het Ministerie van EZK verstrekt jaarlijks via Mijn Cyberweerbare Zaak subsidie aan kleinere mkb'ers ter versterking van hun digitale weerbaarheid.
Mensen die vermoeden dat ze slachtoffer zijn geworden van diefstal van hun gegevens kunnen op de site van de politie controleren of hun data in handen is gevallen van criminelen.

Vraag 11
Acht u de oproep van Odido aan klanten om «extra alert» te zijn voldoende, of ziet u een verantwoordelijkheid voor aanvullende beschermingsmaatregelen richting getroffen klanten?

Antwoord 11
Zoals uiteengezet in het antwoord op vraag 8, stelt het toepasselijke normenkader, in het bijzonder de AVG, de nodige strikte vereisten. De AP ziet toe op de naleving van dat kader.

Vraag 12
Bestaan er landelijke richtlijnen of protocollen voor ondersteuning van burgers die slachtoffer zijn van grootschalige datalekken waarbij identiteitsgegevens zijn buitgemaakt? Zo ja, worden deze in dit geval toegepast?

Antwoord 12
Het handelingskader voor slachtoffers van datalekken wordt vormgegeven door de AVG. De AVG verplicht verwerkingsverantwoordelijke organisaties om betrokkenen te informeren over een «hoog risico» datalek. De wijze waarop betrokkenen in lijn met de AVG dienen te worden geïnformeerd, wordt uitgewerkt in richtsnoeren van het Europees Comité voor gegevensbescherming (EDPB). Het is aan de AP om daarop toe te zien. Tevens heeft de AP op grond van de AVG de eigen wettelijke taak om voorlichting te geven aan burgers over hun rechten en handelingsmogelijkheden uit hoofde van de AVG bij datalekken. De website van de AP biedt een overzicht van mogelijkheden voor betrokkenen bij een datalek.
Daarnaast zal het kabinet met een reactie komen in lijn met de gedane toezegging door de Staatssecretaris van Digitale Economie en Soevereiniteit en de aangenomen motie van het lid Rajkowski die opriep voor een duidelijk handelingskader voor slachtoffers van datalekken en de gedane toezegging[5].

Vraag 13
Op welke wijze houdt de Autoriteit Persoonsgegevens toezicht op de opvolging van dit incident, en beschikt de toezichthouder volgens u over voldoende bevoegdheden en capaciteit om effectief toezicht te houden bij grootschalige datalekken?

[5] Tweede Kamer, vergaderjaar 2025–2026, 36 800 VII, nr. 7

Antwoord 3
De AP heeft laten weten geen informatie te verstrekken over individuele zaken. In zijn algemeenheid houdt de AP bij omvangrijke datalekken onder meer toezicht op de naleving van de meldplicht datalekken en onderzoekt daarbij ook de beveiliging ten tijde van het lek en genomen vervolgstappen. Maar ook andere aspecten die specifiek zijn voor de datalekzaak kunnen door de AP worden onderzocht. Daarbij wordt ook rekening gehouden met signalen uit openbare bronnen en signalen uit klachten die de AP heeft ontvangen.
De AP beschikt over voldoende handhavende bevoegdheden vanuit de AVG om in te grijpen wanneer een (voorgenomen) verwerking van persoonsgegevens niet rechtmatig, behoorlijk en/of transparant plaatsvindt. Bijvoorbeeld door het bevestigen van normen, het geven van waarschuwingen, stilleggen van verwerkingen of het opleggen van boetes.

Vraag 14
Welke lessen trekt u uit dit incident voor het beleid richting de markt op het gebied van de weerbaarheid van organisaties die grote hoeveelheden persoonsgegevens verwerken?

Antwoord 14
Zie het antwoord op vraag 2.