Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Prinses Irenestraat 6
2595 BD DEN HAAG

Directoraat-generaal
Economie en Digitalisering

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6011 (algemeen)
www.rijksoverheid.nl/ezk

Ons kenmerk
DGED / 105381312

Uw kenmerk
2026Z03910

Datum 9 april 2026
Betreft Beantwoording over het bericht *'Odido-datalek erger dan gemeld, ook burgerservicenummers gelekt'*

Geachte Voorzitter,

Hierbij zend ik u de antwoorden op de vragen van het lid El Boujdaini (D66) over over het bericht *'Odido-datalek erger dan gemeld, ook burgerservicenummers gelekt'* (kenmerk: 2026Z03910; ingezonden: 27 februari 2026).

W.J.M. Aerdts
Staatssecretaris van Economische Zaken,
Digitale Economie en Soevereiniteit

Claudia van Bruggen
Staatssecretaris van Justitie en Veiligheid,

Directoraat-generaal
Economie en Digitalisering

2026Z03910

Ons kenmerk
DGED / 105381312

1
Bent u bekend met het bericht van RTL waarin wordt gemeld dat bij telecomprovider Odido een grootschalig datalek heeft plaatsgevonden en dat hierbij, anders dan eerder door het bedrijf gecommuniceerd, ook burgerservicenummers (BSN) zijn gelekt?

Antwoord
Ja

2
Hoe beoordeelt u de ernst van het incident, in het bijzonder het lekken van BSN, vanuit het perspectief van de bescherming van fundamentele rechten van burgers en hoe ingrijpend beoordeelt u de impact op burgers?

Antwoord
De schaal van dit datalek, de hoeveelheid getroffen burgers en de soms gevoelige aard van de gelekte gegevens 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 beveiliging van persoonsgegevens zoals vereist in de Algemene Verordening Gegevensbescherming (AVG) pure noodzaak is en een cruciaal onderdeel van de bedrijfsprocessen moet zijn. 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 een strafrechtelijk onderzoek naar de aanval en de daders.

De gelekte gegevens waaronder ook het BSN zijn niet direct bruikbaar voor fraudeurs om zelfstandig fraude op naam van gedupeerden te plegen. Criminelen gebruiken de gegevens vooral om phishingaanvallen uit te voeren en gedupeerden te verleiden om op een link te klikken of nog meer gegevens prijs te geven.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties adviseert niet om paspoorten of identiteitskaarten te vernieuwen. Er zijn alleen paspoortnummers gelekt. Alleen met die informatie kunnen criminelen niet zelfstandig fraude plegen. Zij kunnen die informatie echter wel gebruiken voor bijvoorbeeld gerichte phishingaanvallen. Met behulp van de gestolen informatie proberen ze dan om zo betrouwbaar mogelijk te lijken en in te spelen op het gevoel van burgers met als doel om meer informatie te ontfutselen of burgers te verleiden op een link, button of QR-code te klikken.

3
In hoeverre acht u daarbij het recht op privacy en gegevensbescherming geschonden, nu (oud-)klanten van Odido buiten hun eigen schuld risico lopen op misbruik van hun persoonsgegevens?

Antwoord
In algemene zin is een datalek een inbreuk in verband met het recht op persoonsgegevens. Of, en zo ja in hoeverre, de privacy en het recht op gegevensbescherming van betrokken in deze concrete zaak zijn geschonden, is niet aan het kabinet om te beoordelen. Dit is aan de Autoriteit Persoonsgegevens (AP) en de Rijksinspectie Digitale Infrastructuur (RDI) als toezichthouders of in voorkomende gevallen aan de rechter om te beoordelen.

4
Hoe beoordeelt u het advies aan Odido om geen losgeld te betalen, gelet op de huidige situatie waarin de hackersgroep Shinyhunters is overgegaan tot publicatie van gestolen persoonsgegevens, met mogelijke ernstige gevolgen voor de (oud-)klanten van Odido?[2]

Antwoord
Het besluit van Odido om geen losgeld te betalen sluit aan bij de visie van het kabinet. Slachtoffer worden van dergelijke afperspraktijken kan veel impact hebben. De schade kan enorm oplopen en plaatst een getroffen bedrijf in een moeilijke positie, ook richting hun klanten. Zeker in dit geval waar het aantal gestolen gegevens zo omvangrijk is. De uiteindelijke afweging ligt bij de getroffen organisatie, maar het dringende advies van de overheid blijft om geen losgeld te betalen. Betaling van losgeld biedt geen garantie dat criminelen systemen herstellen, gestolen data verwijderen of ervan afzien deze openbaar te maken of door te verkopen aan andere criminelen. Daarnaast houdt het betalen van losgeld het verdienmodel van cybercriminelen in stand. De opbrengsten worden veelal ingezet voor verdere, geavanceerde cyberaanvallen, waarmee nieuwe slachtoffers worden gemaakt. Dit kan bovendien nieuwe aanvallen op Nederlandse organisaties uitlokken.

5
Kunt u aangeven welke opsporingsprioriteit wordt gegeven aan het strafrechtelijk onderzoek dat is gestart door het Openbaar Ministerie en ligt daarbij ook een rol voor de digitale recherche?

Antwoord
Het OM gaat over de opsporingsprioriteit. De politie is onder gezag van het Openbaar Ministerie een opsporingsonderzoek gestart. Een team van het Team High Tech Crime, dat gespecialiseerd is in dit soort cybercriminaliteit, doet onderzoek naar het incident.

6
Welke rol ziet u bij het ondersteunen en informeren van burgers van wie persoonsgegevens door cybercriminelen zijn gepubliceerd en acht u het huidige instrumentarium hiervoor toereikend?

Antwoord
De overheid geeft praktische tips om de digitale weerbaarheid van burgers te vergroten. Zo hebben burgers de mogelijkheid om websites zoals

veiliginternetten.nl en die van het NCSC te raadplegen waar veel informatie en adviezen worden gegeven over hoe ze zich online kunnen beschermen en over de basisprincipes van digitale weerbaarheid. Via Centraal Meldpunt Identiteitsfraude (CMI) kan er melding worden gedaan van fraude, hier is ook een specifieke pagina over de Odido hack. Daarnaast zal het kabinet met een reactie komen in lijn met de gedane toezegging door de staatsecretaris van Economische Zaken – digitale economie en soevereiniteit en de aangenomen motie van het lid Rajokowski die opriep tot een duidelijk handelingskader voor slachtoffers van datalekken.[1]

7
Ziet u aanleiding om het strafrechtelijk kader of de opsporingscapaciteit op het terrein van hacks en digitale afpersing te versterken, bijvoorbeeld door intensivering van de digitale recherche van de politie of door aanpassing van wet- en regelgeving?

Antwoord
Door het ministerie van Justitie en Veiligheid worden met de politie en het OM worden gesprekken gevoerd over wat er nodig is om de aanpak van online criminaliteit een stap verder te brengen, daarin zullen de recente incidenten zoals de hacks bij Clinical Diagnostics en Odido worden meegenomen.

In het coalitieakkoord is verder aangekondigd dat de strafmaxima voor zware cyberdelicten zullen worden verhoogd. Bij de nadere beleidsuitwerking hiervan zal ook aandacht worden besteed aan deze recente incidenten.

8
Kunt u de vragen afzonderlijk beantwoorden en dit doen voorafgaand aan de behandeling van de Cyberbeveiligingswet?

Antwoord
Dit is helaas niet gelukt.

[1] https://www.tweedekamer.nl/downloads/document?id=2026D09253