Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtsbestel

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Onze referentie
7513754

Uw referentie
2026Z07921

Datum 3 juni 2026
Betreft Antwoorden Kamervragen over het bericht 'gegevens 200.000 leden Basic-Fit gelekt, ook bij Booking klantgegevens gestolen

In antwoord op uw brief van 15 april 2026, deel ik u mede dat de vragen van het lid El Boujdaini (D66) over het bericht ‘gegevens 200.000 leden Basic-Fit gelekt, ook bij Booking klantgegevens gestolen, worden beantwoord zoals aangegeven in de bijlage bij deze brief.

De Staatssecretaris van Justitie en Veiligheid,

Claudia van Bruggen

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtsbestel

Datum
3 juni 2026

Onze referentie
7513754

Vragen van het lid El Boujdaini (D66) aan de minister van Justitie en Veiligheid en de staatssecretaris van Economische Zaken en Klimaat over het bericht 'Gegevens 200.000 leden Basic-Fit gelekt, ook bij Booking klantgegevens gestolen'. (Ingezonden op 15 april 2026, 2026Z07921)

Vraag 1
Bent u bekend met het bericht van de NOS over hacks bij Basic-Fit en Booking.com waarbij klantgegevens zijn buitgemaakt? [1]

Antwoord 1
Ja.

Vraag 2
Hoe beoordeelt u deze incidenten als indicatie van structurele tekortkomingen in de beveiliging van persoonsgegevens bij grote, digitaal opererende bedrijven?

Antwoord 2
De berichten over grootschalige datalekken zijn zorgwekkend, vooral gezien de mogelijk schadelijke gevolgen voor getroffen betrokkenen. Het is belangrijk dat getroffen burgers, wanneer het waarschijnlijk een hoog risico betreft, goed worden geïnformeerd zodat zij weten waar zij aan toe zijn en daartoe gepaste stappen kunnen ondernemen. Ik wil voorzichtig zijn met het spreken van ‘structurele tekortkomingen’. Elk incident is anders en kan een eigen oorzaak hebben, en het is niet uitgesloten dat er sprake kan zijn van een zeer geavanceerde cyberaanval waartegen zelfs goed beveiligde bedrijven kwetsbaar zijn.

Vraag 3
Heeft u voldoende structureel inzicht in de aard, omvang en frequentie van datalekken en cyberaanvallen in Nederland? Zo ja, hoe wordt dit overzicht benut voor beleid en toezicht? Zo nee, welke maatregelen neemt u om dit inzicht te verbeteren?

Antwoord 3
Organisaties die persoonsgegevens verwerken zijn verplicht om alle datalekken te documenteren, bijvoorbeeld in een register. Naast het lek zelf moeten ook de feiten en de gevolgen van het datalek en de genomen corrigerende maatregelen worden geregistreerd. Het doel van een dergelijk register is bewustwording en te leren van eerdere datalekken, alsook het nemen van effectieve maatregelen om de kans op

nieuwe, soortgelijke datalekken te verminderen. Ook stelt het de toezichthouder in staat te controleren of de meldplicht wordt nageleefd. Daarnaast houdt de Autoriteit Persoonsgegevens (AP) de bij haar gemelde datalekken bij. Niet alle datalekken worden gemeld of zijn meldplichtig: een melding bij de AP is alleen verplicht als de inschatting is gemaakt dat het waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van betrokkenen, zoals de bescherming van hun persoonsgegevens en persoonlijke levenssfeer. De AP rapporteert jaarlijks over de meldplicht datalekken. Het kabinet beschikt niet over een register van alle datalekken, maar ziet vooralsnog niet dat sprake is van een tekort aan inzicht en van de noodzaak tot het treffen van maatregelen om dat te verbeteren.

Vraag 4
Deelt u de opvatting dat herhaalde datalekken kunnen wijzen op onvoldoende structurele naleving van de Algemene verordening gegevensbescherming? Zo ja, welke systeemfouten signaleert u hierbij? Zo nee, waarom niet?

Antwoord 4
Een datalek hoeft niet te duiden op onvoldoende structurele naleving van de AVG; ook goed beveiligde organisaties, overheden en bedrijven kunnen worden getroffen. Daarbij betekent een datalek op zich niet dat er ook sprake is van een overtreding van de AVG. Het gaat er verder vooral om hoe bedrijven handelen nadat een datalek is geconstateerd. Dat handelen kan bestaan uit het nemen van (extra) beveiligingsmaatregelen, het naleven van de meldingsplicht en transparante communicatie richting de getroffen betrokkenen. Organisaties die persoonsgegevens verwerken zijn – als verwerkingsverantwoordelijke – gehouden om gedegen risico-analyses te maken en een daaraan gekoppelde passende interne beveiligingscultuur en snel en adequaat te handelen in geval van een incident.

Vraag 5
Acht u de toezicht- en handhavingscapaciteit van de Autoriteit Persoonsgegevens toereikend om structurele naleving af te dwingen? Zo ja, waarom? Zo nee, welke versterkingen zijn nodig?

Antwoord 5
Het kabinet is van mening dat de AP over voldoende middelen beschikt om de (toezicht- en handhavings)taken die voortvloeien uit de AVG en de UAVG uit te voeren. De AP mag zelf bepalen hoe zij de middelen die zij voor AVG-toezicht ontvangt, verdeelt over de afzonderlijke AVG-toezichtstaken. Zoals genoemd in de beleidsreactie op de evaluatie van de AP[1] wil het kabinet samen met de AP stappen zetten om te komen tot een meer objectieve basis die ondersteunend is bij de besluitvorming over een passende hoogte van het budget van de AP. Een landenvergelijkend onderzoek kan daarbij een nuttig instrument zijn.

Vraag 6
Ziet u aanleiding om te komen tot strengere, afdwingbare beveiligingsnormen voor bedrijven die op grote schaal persoonsgegevens verwerken? Zo nee, waarom niet?

[1] https://www.rijksoverheid.nl/documenten/kamerstukken/2025/07/11/tk-reactie-op-evaluatie-autoriteit-persoonsgegevens

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtsbestel

Datum
3 juni 2026

Onze referentie
7513754

Antwoord 6
De AVG biedt in principe voldoende normen voor het nemen van passende beveiligingsmaatregelen voor alle organisaties en bedrijven die (op grote schaal) persoonsgegevens verwerken. Passende beveiligingsmaatregelen houden concreet onder meer in dat organisaties en bedrijven bij risicovolle en/of grootschalige gegevensverwerkingen vooraf een Data Protection Impact Assessment (DPIA) dienen uit te voeren. Dit is een instrument om voorafgaand aan de verwerking de privacyrisico's in kaart te brengen om daarmee de impact op de rechten van betrokkenen te beoordelen en gerichte maatregelen te nemen om deze risico's te verkleinen. Daarnaast zijn organisaties en bedrijven in het geval van grootschalige gegevensverwerking vaak verplicht om een functionaris voor gegevensbescherming (FG) aan te stellen. De FG is een onafhankelijke toezichthouder binnen een organisatie of bedrijf die toeziet op de naleving van de AVG en adviseert over het zorgvuldig verwerken van persoonsgegevens. De verwerkingsverantwoordelijke heeft voor het treffen van passende beveiligingsmaatregelen een verantwoordingsplicht. Gelet hierop zie ik geen noodzaak voor extra (strenge) maatregelen. Wel geldt straks voor organisaties en bedrijven die opereren in voor de samenleving cruciale sectoren, waaronder onder andere de transport- en energiesector, het bankwezen en de digitale infrastructuur, de Cyberbeveiligingswet. Deze wet is op 15 april jl. door uw Kamer aangenomen en treedt later dit jaar in werking. De Cyberbeveiligingswet is de doorvertaling van de Europese NIS2- en CER-richtlijn die lidstaten weerbaarder moeten maken tegen gevaren van buitenaf, waaronder cyberdreigingen. De wet verplicht onder andere tot het uitvoeren van een risicoanalyse en het op basis daarvan treffen van passende en evenredige maatregelen voor het betreffende netwerk- en informatiesysteem. Ook hebben organisaties en bedrijven op grond van deze wet een zorg-, meld- en registratieplicht.

Vraag 7
In het kader van dataminimalisatie: ziet u kansen dat de ontwikkeling van de EDI-wallet in Nederland kan bijdragen aan het verkleinen van het risico op datalekken bij organisaties, doordat consumenten hun persoonsgegevens minder vaak rechtstreeks hoeven te delen met verschillende partijen?

Antwoord 7
Ja. De Europese Digitale Identiteit (EDI) stelt burgers in staat binnen de hele Europese Unie digitaal te legitimeren of in te loggen op websites. Het veilig delen van persoonsgegevens behoort daar ook toe, waarbij enkel de gegevens worden gebruikt die strikt noodzakelijk zijn.

Vraag 8
Kunt u de vragen afzonderlijk beantwoorden?

Antwoord 8
De vragen zijn afzonderlijk beantwoord.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtsbestel

Datum
3 juni 2026

Onze referentie
7513754

[1] NOS, 13 april 2026 (Gegevens 200.000 leden Basic-Fit gelekt, ook bij Booking klantgegevens gestolen).