Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA Den Haag

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk
www.linkedin.com/company/ministerie-van-bzk

Kenmerk
2023-0000159485

Uw kenmerk
2023Z01674

Datum	21 maart 2023
Betreft	Beantwoording Kamervragen (2023Z01674) en maatregelen inzake het weren van apps op mobiele devices van rijksambtenaren

Op 2 februari 2023 zijn er schriftelijke vragen gesteld, met kenmerk 2023Z01674, door het lid Dekker-Abdulaziz (D66) over de mogelijkheid om de Chinese applicatie TikTok te weren op mobiele devices van medewerkers van de Rijksoverheid. In het debat *Inzet algoritmes en data-ethiek binnen de Rijksoverheid* op 15 februari jl. heb ik toegezegd nader onderzoek te doen. Er is in dat debat ook door enkele partijen gevraagd of Nederland niet net als de Verenigde Staten een verbod voor gebruik door ambtenaren moet instellen vanwege het potentieel hoge veiligheidsrisico. Sinds het debat hebben de Europese Commissie, Raad van de Europese Unie, en het Europees Parlement het gebruik van TikTok opgeschort. In deze brief zal ik ingaan op het uitgevoerde onderzoek, en aangeven welk beleid ik hierop ga volgen. Ook zijn de antwoorden op de schriftelijke vragen bijgevoegd, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties.

Onderzoek veiligheidsrisico's
Op basis van de vragen van de Kamer is aan de AIVD gevraagd een advies te geven. De conclusie daarvan is dat het gebruik en de aanwezigheid van mobiele telefoons en de daarop geïnstalleerde applicaties te allen tijde een inherent spionagerisico vormen. Het is daarom raadzaam altijd een grondige afweging plaats te laten vinden tussen de noodzaak van het installeren van een bepaalde applicatie enerzijds en het daarbij behorende risico anderzijds. Gebruik van apps van bedrijven uit landen met een offensief cyberprogramma door ambtenaren in dienst van de rijksoverheid[1] verhoogt dit risico. Voorbeelden van landen met een dergelijk offensief cyberprogramma zijn Rusland, China, Iran en Noord-Korea. Het overgaan op apparaten die door de werkgever beheerd worden is een meer structurele oplossing voor dit risico. De beschouwing van de AIVD, die de basis was voor verder interdepartementaal onderzoek, is ter informatie toegevoegd als bijlage bij deze brief.

[1] Dit zijn alle ambtenaren in dienst bij de departementen en daaronder vallende agentschappen en andere uitvoeringsorganisaties.

In algemene zin hebben applicaties vaak toegang tot alle gegevens van de mobiele telefoon. Apps vragen hier veelal via de gebruikersvoorwaarden vooraf toestemming voor. De gebruiker kan ook zelf informatie toevoegen. Er kan daarbij gedacht worden aan persoonsgegevens van de gebruiker zoals contactgegevens, bestanden zoals foto's, of contacten van de gebruiker. Maar ook aan gegevens over het specifieke apparaat en de netwerken die gebruikt worden. In specifieke gevallen worden toetsaanslagen van gebruikers onderschept.

Er is in mijn onderzoek ook nauw contact geweest met een aantal partnerlanden in de EU en de Europese Commissie, over hun inschattingen en hun beleidskeuzes voor wat betreft apps op mobiele apparaten in gebruik door hun overheidsambtenaren. Hieruit komt het beeld naar voren dat landen verschillende keuzes maken, maar dat veel landen maatregelen hebben genomen ter beveiliging van telefoons van hun ambtenaren. Enkele landen hebben gekozen voor een specifiek verbod op TikTok, een aantal landen ontraadt of verbiedt in meer generieke zin het gebruik van apps van bedrijven uit bepaalde landen vanwege de inherente risico's. Een aantal landen heeft aangegeven dat zij ervoor gekozen hebben hun mobiele apparaten zo in te richten, dat enkel vooraf toegestane apps geïnstalleerd en gebruikt kunnen worden. We volgen ook de ontwikkelingen buiten de Europese Unie. Daarbij hebben we kennis genomen van het verbod dat het Verenigd Koninkrijk als voorzorgsmaatregel heeft ingesteld voor TikTok op overheidsapparatuur, toewerkend naar een versterking van het beleid rondom apps van derde partijen. Ook worden de maatregelen en stappen die de Verenigde Staten zetten gevolgd, waar bijgevoegde vragen ook al aan refereren.

Beleid voor de rijksoverheid
In het licht van de hierboven genoemde risico's en de beschouwing van de AIVD acht ik het nodig om aanvullende stappen op het gebied van veiligheid van mobiele apparaten bij de Rijksoverheid te zetten. De eerste stap is het per direct aan ambtenaren in dienst van de Rijksoverheid ontraden om apps geïnstalleerd te hebben en te gebruiken op hun mobiele werkapparatuur van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen. Om ambtenaren in dienst van de rijksoverheid hierover goed te informeren zal op korte termijn communicatie worden ontwikkeld.

Tegelijk zal op korte termijn worden toegewerkt naar een situatie waarbij mobiele apparaten, uitgereikt aan ambtenaren in dienst van de rijksoverheid, zo zijn ingericht dat er alleen vooraf toegestane apps, software en/of functionaliteiten kunnen worden geïnstalleerd en gebruikt. Het worden dan in zijn geheel zogeheten '*managed apparaten*', waarvoor is bepaald welke apps daarop kunnen worden geïnstalleerd en gebruikt door de gebruiker. Apps van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen zullen dan niet toegestaan worden. Ik wil dit beleid zo snel als mogelijk ingericht hebben, in samenwerking met de *'shared service organisaties'* (SSO's) die deze mobiele apparaten beheren. Daarbij bezie ik ook het *bring your own device* beleid dat door onderdelen van de rijksoverheid wordt gehanteerd.
Uitzondering op de bovenstaande maatregelen geldt wanneer een dergelijke applicatie nodig is of kan zijn voor het uitoefenen van een primaire taak van een

rijksorganisatie. Hierbij kan worden gedacht aan inspectie en toezicht, opsporingsonderzoek of inlichtingenbelang. Deze uitzondering zal in samenwerking met de departementen de komende periode verder worden uitgewerkt.

Appgebruik in de samenleving
Deze brief heeft zich tot nu gericht op risico's voor de rijksoverheid. Apps worden ook door andere overheden en vooral ook door burgers, waaronder kinderen, gebruikt. Het is belangrijk om het bewustzijn over gegevensverwerking door dit soort apps te verhogen. Daarom gaat het kabinet hier de komende periode op inzetten. Voor de zomer komen wij hier bij uw Kamer op terug.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties
Digitalisering en Koninkrijksrelaties

Alexandra C. van Huffelen

Vraag 1
Deelt u de mening dat het onduidelijk is in hoeverre de gegevensbescherming van TikTok voldoet en dat de Chinese applicatie daarmee een potentieel hoog veiligheidsrisico heeft?

In de begeleidende brief bij deze antwoorden, ben ik nader ingegaan op risico's voor de Rijksoverheid, en de stappen die ik in reactie daarop ga nemen.

Als het gaat om het voldoen van TikTok aan de geldende regels, doet op dit moment de Ierse privacytoezichthouder (de zogenaamde *Data Protection Commission*), als leidende EU-privacytoezichthouder, onderzoek naar de wijze waarop TikTok persoonsgegevens verwerkt. Het onderzoek van de Ierse toezichthouder richt zich onder andere op rechtmatigheid van de overdracht door TikTok van persoonsgegevens naar derde landen waaronder China en de naleving van de vereisten van de Algemene verordening gegevensbescherming (AVG) voor deze overdrachten.

De minister voor Rechtsbescherming heeft de Autoriteit Persoonsgegevens (AP) gevraagd om bij haar Ierse collega te vragen naar de stand van zaken van dit onderzoek. Uit deze navraag blijkt dat de onderzoeksresultaten in de eerste helft van 2023 worden verwacht. Uit dit onderzoek zal blijken in hoeverre de gegevensbescherming van TikTok voldoet aan de geldende wet- en regelgeving.

Vraag 2
Hoe kijkt u naar de ontwikkeling in de Verenigde Staten waar het besloten is om publieke vertegenwoordigers te verbieden TikTok op hun mobiele werkdevice te hebben en zou u dit ook aan Nederlandse volksvertegenwoordigers adviseren? [1]

Zoals aangegeven in de begeleidende brief, is in het traject de afgelopen weken nauw contact geweest met Europese partners, en hun beleid rondom mobiele apparaten bij de overheid en TikTok. Deze contacten hebben daarmee bijgedragen aan de in de brief genoemde besluiten.

De risico's die naar voren zijn gekomen, gelden niet alleen voor de rijksoverheid, maar kunnen ook breder gelden. Ik adviseer het Nederlandse parlement dan ook om kennis te nemen van de brief, en met inachtneming van zijn eigen onafhankelijke positie, te besluiten over eventuele extra veiligheidsmaatregelen.

Vraag 3
Bent u bereid medewerkers van de Rijksoverheid en andere overheidsambtenaren te verbieden de applicatie TikTok op hun mobiele werkdevice te hebben, om op die manier potentiële risico's te verkleinen?

Voor het antwoord op deze vraag verwijs ik naar het beleid zoals geformuleerd in de begeleidende brief bij deze antwoorden.