

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

638

Vragen van het lid **Van Raan** (PvdD) aan de Minister voor Rechtsbescherming en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht dat het Chinese TikTok bij het gebruik van de in-app browser alle toetsaanslagen vastlegt en daarmee wachtwoorden en creditcardgegevens kan verzamelen* (ingezonden 8 september 2022).

Antwoord van Minister **Weerwind** (Rechtsbescherming), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 8 november 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 101.

Vraag 1

Kent u het blog «iOS Privacy: Announcing InAppBrowser.com – see what JavaScript commands get injected through an in-app browser» van Felix Krause?¹

Antwoord 1

Ja, daarmee ben ik bekend.

Vraag 2

Klopt het dat TikTok bij het gebruik van de in-app browser alle toetsaanslagen vastlegt? Klopt het dat daarmee bijvoorbeeld ook wachtwoorden en creditcardgegevens kunnen worden verzameld?

Antwoord 2

Volgens het aangehaalde onderzoek van Felix Krause laat de app van TikTok het toe dat toetsaanslagen, waaronder ook wachtwoorden en creditcardgegevens, in de in-app-browser worden vastgelegd. TikTok zegt volgens het betreffende blog van deze mogelijkheid geen gebruik te maken, en de gegevens slechts te verwerken voor probleemoplossing en prestatiebewaking van de ervaring – zoals het controleren hoe snel een pagina wordt geladen of controleren of deze crasht.

Het onderzoek van Krause geeft geen uitsluitel of toetsaanslagen ook daadwerkelijk worden vastgelegd en worden gebruikt voor andere doeleinden

¹ Blog Felix Krause, 18 augustus 2022, «iOS Privacy: Announcing InAppBrowser.com – see what JavaScript commands get injected through an in-app browser», <https://krausefx.com/blog/announcing-inappbrowsercom-see-what-javascript-commands-get-executed-in-an-in-app-browser>.

dan voor probleemoplossing en prestatiebewaking. Of het klopt dat bijvoorbeeld ook wachtwoorden en creditcardgegevens kunnen worden verzameld, is mij niet bekend. Als dat wel gebeurt, is dat natuurlijk uiterst zorgelijk. Binnenkort spreekt de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties in het kader van een serie gesprekken die zij voert met verschillende grote techbedrijven met TikTok. Het blijft aan de onafhankelijke toezichthouder om de rechtmatigheid van gegevensverwerkingen te onderzoeken en daar op te handhaven. Bij de verwerking van persoonsgegevens dient het uitgangspunt van data-minimalisatie (zo min mogelijk gebruik maken van persoonsgegevens) te worden toegepast.

Vraag 3

Klopt het dat de enige garantie dat dit nu niet gebeurt is dat TikTok zelf beweert dat ze deze functie niet gebruiken? Is er een manier om die uitspraak van TikTok te verifiëren?

Antwoord 3

Het uitgangspunt van de Algemene verordening gegevensverwerking (AVG) is dat de verwerkingsverantwoordelijke zelf, in dit geval TikTok, dient te waarborgen dat verplichtingen uit de AVG worden nageleefd. Daartoe behoort dat gebruikers controle over hun persoonsgegevens dienen te hebben en dat de verwerking van persoonsgegevens rechtmatig, behoorlijk en transparant is. Concreet betekent dit dat betrokkenen op de hoogte dienen te worden gesteld op het moment dat hun persoonsgegevens worden verzameld, en onder meer welke gegevens worden verzameld, voor welk doel en met wie deze worden gedeeld. Tevens dienen ze te worden gewezen op hun rechten, zoals het recht op inzage.

Wanneer betrokkenen inzicht willen in welke gegevens van hen door TikTok worden verwerkt, dan is TikTok op hun verzoek verplicht inzage te geven in hun persoonsgegevens. Mocht een verzoek om inzage niet het gewenste resultaat hebben, dan kunnen betrokkenen daarover een klacht indienen. In eerste instantie is het raadzaam om deze klacht bij de Functionaris Gegevensbescherming (FG) van TikTok neer te leggen. Als dat niet het gewenste effect sorteert, dan kan een klacht worden ingediend bij de toezichthouder die toeziet op de naleving van de AVG, de Autoriteit Persoonsgegevens (AP). Zoals hierboven beschreven, kan de vraag welke gegevens daadwerkelijk door TikTok worden gebruikt, beantwoord worden wanneer gebruikers zelf een verzoek doen tot de inzage van de verwerking van hun persoonsgegevens of wanneer de AP onderzoek doet (bijv. n.a.v. een klacht over beperkte inzage). Dit neemt niet weg dat het kabinet van alle bedrijven in Nederland, dus ook TikTok, verwacht dat zij zich aan de geldende wet- en regelgeving houden en daarmee dus ook aan de AVG.

Vraag 4

Bent u bereid om, op de kortst mogelijke termijn, TikTok om opheldering te vragen?

Antwoord 4

Het houden van toezicht op en het handhaven van de rechtmatigheid van gegevensverwerkingen in de private sector is geen taak van het kabinet, maar van de toezichthouder. Deze is onafhankelijk en heeft een ruim mandaat en uitgebreide bevoegdheden om te onderzoeken of partijen voldoen aan hun verplichtingen uit de AVG. De onafhankelijkheid brengt mee dat het aan de toezichthouder dient wordt gelaten om te bepalen in welke gevallen een onderzoek noodzakelijk en wenselijk is.

Dat neemt niet weg dat de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, zoals hierboven aangegeven, binnenkort een gesprek heeft met TikTok. De hierboven genoemde uitgangspunten zullen bij TikTok onder de aandacht worden gebracht, mede naar aanleiding van de berichtgeving hierover.

Vraag 5

Deelt u de mening dat deze functie – ook wanneer TikTok hem niet zou gebruiken – absoluut onacceptabel is en TikTok op de kortst mogelijke termijn geblokkeerd moet worden, in ieder geval tot deze functionaliteit geschrapt is?

Antwoord 5

Ik deel de mening dat het gezien de veiligheidsrisico's absoluut onacceptabel zou zijn wanneer TikTok gegevens ten aanzien van toetsenbord invoer op onrechtmatige wijze zou verwerken. Daarvan kan bijvoorbeeld sprake zijn als voor een volgens de AVG voor gegevensverwerking vereiste verwerkingsgrondslag, bijvoorbeeld toestemming van de betrokkene, ontbreekt. Ook moet worden voldaan aan de beginselen van behoorlijke gegevensverwerking, waaronder het beginsel van dataminimalisatie. Dit beginsel houdt in dat slechts de gegevens mogen worden verwerkt die noodzakelijk zijn voor het doeleinde waarvoor de verwerking van persoonsgegevens plaatsvindt. Het is aan de onafhankelijke toezichthouder om toe te zien op de rechtmatigheid van gegevensverwerking en deze te handhaven.

Vraag 6

Op welke manier maakt de overheid (in de breedste zin van het woord) gebruik van TikTok? Welke (gevoelige) overheidsinformatie kan door TikTok op deze manier verzameld zijn?

Antwoord 6

De Baseline Informatiebeveiliging Overheden (BIO) en van toepassing zijnde privacywetgeving regelt dat iedere organisatie zelf verantwoordelijk is voor het beoordelen van privacy- en veiligheidsrisico's voor het in gebruik nemen van ICT-producten en diensten, zoals TikTok. Er is geen centraal overzicht beschikbaar van het gebruik van TikTok door de overheid. De BIO schrijft ook voor hoe met (gevoelige) overheidsinformatie moet worden omgegaan. In generieke zin moet worden geborgd dat dergelijke informatie niet door niet-geautoriseerde partijen en personen kan worden ingezien. Daarnaast adviseert de Dienst Publiek en Communicatie (DPC) van het Ministerie van Algemene Zaken (AZ) de inzet van TikTok voor de rijksoverheid op te schorten tot TikTok haar gegevensbeschermingsbeleid heeft aangepast.

Vraag 7

Op welke wijze gaat u ervoor zorgen dat alle gegevens die op deze (onrechtmatige) manier verzameld zijn door TikTok worden verwijderd? Ziet u ook in dat u daar nauwelijks de mogelijkheid toe heeft?

Antwoord 7

Het is juist dat het niet aan het kabinet is om persoonsgegevens die op een onrechtmatige manier zijn verzameld, te laten verwijderen. De onafhankelijke toezichthouder ziet toe op het handhaven van de rechtmatigheid van gegevensverwerking onder de AVG.

Betrokkenen hebben het recht om te verzoeken om bepaalde persoonsgegevens te laten verwijderen, op grond van artikel 17 van de AVG. Als de verwerkingsverantwoordelijke daartoe in voorkomende gevallen niet overgaat, is het raadzaam om, zoals in antwoord 3 staat, een klacht eerst bij de FG van TikTok neer te leggen en als dit niet het gewenste effect heeft, bij de AP.

Vraag 8

Deelt u daarom de mening dat het toezicht op (grote) techbedrijven en hun digitale producten veel beter moet en veel meer aan de voorkant zou moeten plaatsvinden omdat de geleden schade achteraf vaak niet ongedaan te maken is? Zo nee, waarom niet? Zo ja, hoe gaat u dat realiseren?

Antwoord 8

Zoals gezegd is de verwerkingsverantwoordelijke (in casu TikTok) ervoor verantwoordelijk dat de bescherming van persoonsgegevens aan de standaarden voldoet. De AVG voorziet – naast extern toezicht – daartoe ook in intern toezicht en het kunnen afleggen van verantwoording daarover. Daarmee is de AVG er mede op gericht om, door een adequate risicobeheersing (aan de voorkant), zo veel mogelijk te voorkomen dat gegevens op een onrechtmatige manier worden verwerkt. Een verwerkingsverantwoordelijke heeft op grond van de AVG bijvoorbeeld de plicht om voorafgaand aan verwerkingen van persoonsgegevens die waarschijnlijk hoog risico zijn, een Data Protection Impact Assessment (DPIA), ofwel een gegevensbeschermingseffectenbeoordeling, uit te voeren, zodat een organisatie passende

maatregelen kan nemen. Wanneer een DPIA uitwijst dat verwerking gepaard gaat met een hoog risico dat de verwerkingsverantwoordelijke niet kan beperken door maatregelen die met het oog op de beschikbare technologie en de uitvoeringskosten redelijk zijn, dient vóór de verwerking een raadpleging van de toezichthoudende autoriteit plaats te vinden. Ook hebben organisaties, zoals (grote) technologie bedrijven – die belast zijn met de verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige en regelmatige observatie op grote schaal van betrokkenen vereisen – de verplichting om een FG aan te stellen die onder meer als taak heeft om toe te zien op de naleving van de verordening en te werken aan een cultuur van gegevensbescherming.

In het coalitieakkoord is al aangegeven dat we toezicht willen versterken. Om deze reden heeft de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties in haar werkagenda een heel aantal acties opgenomen. Een voorbeeld hiervan is de oprichting van de toezichthouder op algoritmes. Hierbij kijken we in samenwerking met betrokken departementen en toezichthouders of we toezicht meer vooraf kunnen laten plaatsvinden, bijvoorbeeld met behulp van certificering. Ook zullen zeer grote platforms zoals TikTok met inwerkingtreding van de DSA verplicht worden om risico's van hun systemen voor kinderrechten in kaart te brengen en worden bedrijven via de AI-act verplicht om risico's van AI systemen voor mensenrechten in kaart te brengen. Deze risicoanalyses bieden concrete handvatten om proactief toezicht te houden op mogelijk risico's.