AANGETEKEND EN PER E-MAIL VERZONDEN

Zoom Video Communications Netherlands

T.a.v. de directie

Locatellikade 1

1076 AZ Amsterdam

Zoom Video Communications Inc.

55 Almaden Boulevard, 6th Floor

San Jose, CA 95113, USA

info@zoom.us

Datum: 14 juli 2020

Kenmerk: SOMI / Zoom

Uw ref.:

Geachte heer, mevrouw,

Namens Stichting Onderzoek Marktinformatie (hierna: "SOMI") en de 350 deelnemers die ons daar specifiek toe gemachtigd hebben, dien ik met deze brief een klacht in over uw organisatie (Zoom Video Communications Inc. en ZVC Netherlands B.V., hierna: "Zoom"). De klacht ziet op de wijze waarop Zoom is omgegaan met persoonsgegevens van haar gebruikers. Meer dan 10.000 (voornamelijk Nederlandse) gebruikers hebben zich sinds 10 april jl. online bij SOMI aangemeld om deel te nemen aan verschillende onderdelen van deze actie en daarover geïnformeerd te blijven.

Voordat ik deze klacht formuleer en nader toelicht, geef ik hieronder eerst meer informatie over SOMI en over de geconstateerde praktijken van Zoom.

SOMI

1. SOMI is een kenniscentrum en belangenbehartiger. Met haar belangenbehartiging levert SOMI een bijdrage aan online veiligheid, digitale autonomie en privacy bescherming.

2. Inmiddels hebben ruim 10.000 personen zich ingetekend bij SOMI om hun belangen te laten behartigen (hierna: "deelnemers"), waarvan 350 personen SOMI hebben gemachtigd om in deze hun belangen te behartigen. Deze personen zijn als gebruiker van Zoom slachtoffer geworden van privacy schendingen door Zoom als gevolg van de volgende praktijken.

Praktijken van Zoom

3. Zoom is onvoldoende transparant over de wijze waarop zij omgaat met persoonsgegevens en over welke partijen daar toegang toe hebben. In 2019 is Zoom al gewaarschuwd voor problemen met de beveiliging[1], maar in 2020 zijn er nog steeds ernstige gebreken in de beveiliging ontdekt alsook onrechtmatige verwerking

[1] https://www.forbes.com/sites/zakdoffman/2019/07/09/warning-as-millions-of-zoom-users-risk-webcam-hijack-change-your-settings-now/#2452543642d9.

van persoonsgegevens. Door privacy experts worden vraagtekens geplaatst over de accuraatheid van de informatie die Zoom zelf publiceert. In de VS en in Europa hebben overheden, bedrijven en scholen hun werknemers en ambtenaren al verboden om nog langer gebruik te maken van Zoom.[2][3][4] Meer specifiek zijn de volgende praktijken aan het licht gekomen.

Delen van persoonsgegevens

4. Eén van de voornaamste ongeoorloofde praktijken van Zoom betreft het delen van gegevens van gebruikers. Zoom deelde gegevens van gebruikers met derden, waaronder Google, Facebook en LinkedIn, terwijl daar geen toestemming voor was gegeven door gebruikers en terwijl gebruikers hiervan ook niet op de hoogte werden gesteld. [5][6]

5. De software van Zoom bijvoorbeeld, heeft Facebook ingelicht zodra gebruikers Zoom openden. De software van Zoom deelt informatie over het apparaat van de gebruiker. Ook wordt er een 'identiteit' van de gebruiker gedeeld met Facebook, die dat weer kan gebruiken voor het gericht sturen van advertenties. Zoom lijkt deze praktijken te hebben erkend. Eind maart 2020 heeft Zoom besloten te stoppen met de gegevensuitwisseling met Facebook.[7]

6. Zoom deelde ook gegevens van gebruikers met de werkgever van de gebruikers. Zo werden werkgevers door Zoom ingelicht als een werknemer tijdens een Zoom gesprek niet het venster van Zoom op de voorgrond had staan (hetgeen zou suggereren dat de werknemer met andere zaken dan met werk bezig zou zijn). Ook bestond er voor de werkgever de mogelijkheid om gesprekken van werknemers op te nemen en op te slaan.[8]

Geen werkelijke eind-tot-eind versleuteling

7. Zoom biedt haar diensten aan alsof er gebruik wordt gemaakt van eind-tot-eind versleuteling, terwijl er in de praktijk geen sprake is van werkelijke eind-tot-eind versleuteling. [9][10]

8. Eind-tot-eind versleuteling is een sterke vorm van versleuteling waarin een bericht - of in dit geval een videogesprek - van het beginpunt tot het eindpunt versleuteld is. Het is dus direct versleuteld vanaf de apparaten van de Zoom-gebruikers die met elkaar videobellen. Zoom zou het videogesprek niet kunnen inzien.[11]

9. Dit blijkt echter niet juist omdat er geen werkelijke eind-tot-eind versleuteling is gebruikt. De versleuteling bestaat immers niet vanaf het ene gebruikersapparaat tot het andere gebruikersapparaat, maar enkel tussen de servers van Zoom (waardoor het geen werkelijke eind-tot-eind versleuteling is). Hierdoor is het mogelijk dat de communicatie tussen gebruikers wordt ontcijferd door Zoom en dus is in te zien.

10. Op 1 april 2020 zou Zoom excuses hebben aangeboden voor het ten onrechte suggereren dat er gebruikt werd gemaakt van eind-tot-eind versleuteling.[12] Zoom zelf vermeldt hier over:

> *"We want to start by apologizing for the confusion we have caused by incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption. (…) We recognize that there is a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it."*[13]

---

[2] https://www.nu.nl/tech/6042871/schoolorganisaties-in-vs-verbieden-gebruik-videobelapp-zoom.html.
[3] https://www.nu.nl/tech/6043495/duits-ministerie-van-buitenlandse-zaken-beperkt-gebruik-van-zoom.html.
[4] https://www.nu.nl/tech/6045301/ministerie-van-defensie-verbiedt-medewerkers-gebruik-van-videobelapp-zoom.html.
[5] https://privacynieuws.nl/index.php?option=com_content&view=article&id=21562:videobel-app-zoom-deelt-op-ios-ongemerkt-gegevens-met-facebook,-ook-als-je-geen-lid-bent&catid=32:sociale-netwerken&acm=911_538.
[6] https://www.businessinsider.com/zoom-sued-allegedly-sharing-data-with-facebook-2020-3?international=true&r=US&IR=T.
[7] https://www.vpngids.nl/veilig-internet/zakelijk/veilig-videobellen-online-vergaderen/.
[8] https://www.vpngids.nl/veilig-internet/zakelijk/veilig-videobellen-online-vergaderen/.
[9] https://protonmail.com/blog/zoom-privacy-issues/.
[10] https://tweakers.net/nieuws/165340/zoom-liet-e-mailadressen-uitlekken.html.
[11] https://www.nu.nl/tech-achtergrond/6041812/onveilige-wachtwoorden-en-zwakke-encryptie-wat-speelt-er-rond-zoom.html.
[12] https://www.bbc.com/news/technology-52152025.
[13] https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/.

Andere gevallen aangaande de privacy en veilig gebruik

11. Zoom koppelde geautomatiseerd namen en e-mailadressen van gebruikers aan LinkedIn-profielen.[14] Zoom liet e-mailadressen van gebruikers uitlekken naar andere gebruikers.[15] Ook wachtwoorden van gebruikers kwamen 'op straat te liggen'.[16]

12. Sommige gesprekken waren toegankelijk voor vreemden, die vervolgens een gesprek binnen gingen om daar aanstotend materiaal te delen. Dit wordt 'Zoom-bombing' genoemd. Zoom heeft daarom achteraf de functie 'wachtkamer' ingevoerd zodat de gespreksleider een aspirant deelnemer naar eigen inzicht kan toelaten tot het gesprek.[17]

13. Er zijn ook berichten dat gesprekken werden doorgeleid via een server in China, terwijl alle deelnemers in de gesprekken zich buiten China bevonden.[18]

14. Gesprekken via Zoom zouden zonder toestemming onbeveiligd zijn opgeslagen en voor iedereen op internet toegankelijk zijn.[19]

Klacht

15. Deze praktijken geven SOMI en haar deelnemers aanleiding om een klacht in te dienen. De klacht is dat Zoom op verschillende manieren de privacy van gebruikers heeft geschonden. Zoom heeft gehandeld in strijd met verschillende artikelen uit de Algemene verordening gegevensbescherming (AVG). Deze artikelen worden hieronder genoemd, alsook de wijze waarop die door Zoom zijn geschonden. Daarbij worden de hierboven al genoemde praktijken nader aangekaart in relatie tot de toepasselijke artikelen van de AVG.

Schending artikel 5 AVG – Beginselen inzake verwerking van persoonsgegevens

16. In overeenstemming met artikel 5 van de AVG moeten persoonsgegevens worden verwerkt "op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is". Deze principes van "rechtmatigheid", "behoorlijkheid" en "transparantie" zijn meermaals door Zoom geschonden, waarover hierna meer.

17. Tevens dienen persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verzameld en mogen die gegevens vervolgens niet op een met die doeleinden onverenigbare wijze worden verwerkt. Dit principe van "doelbinding" is door Zoom geschonden, ook daarover hieronder meer.

18. Verder dienen persoonsgegevens "toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt". Uit wat hieronder volgt zal blijken dat ook dit principe van de "minimale gegevensverwerking" door Zoom is geschonden.

19. Ten slotte dienen persoonsgegevens "door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier te worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging". Uit wat volgt zal blijken dat ook deze principes "integriteit" en "vertrouwelijkheid" meermaals door Zoom zijn geschonden.

Schending artikel 6 AVG – Rechtmatigheid van de verwerking

20. Tot eind maart 2020 stuurde Zoom de profielen van iOS gebruikers naar Facebook als onderdeel van de "log in with Facebook" feature in de iPhone en iPad Zoom apps. Deze verwerking gebeurde zonder medeweten

---

[14] https://www.nu.nl/tech/6042203/zoom-matchte-e-mailadres-gebruikers-automatisch-aan-linkedin-profielen.html.
[15] https://tweakers.net/nieuws/165340/zoom-liet-e-mailadressen-uitlekken.html.
[16] https://mashable.com/article/stolen-zoom-passwords-dark-web/?europe=true.
[17] https://www.businessinsider.com/zoom-setting-avoid-trolls-control-call-with-waiting-room-2020-3?r=US&IR=T#as-the-host-control-the-waiting-room-by-selecting-manage-participants-10.
[18] https://www.bbc.com/news/technology-52152025.
[19] https://www.ad.nl/tech/opgenomen-zoom-gesprekken-makkelijk-door-iedereen-online-te-vinden~a67d91b0/.

van de betrokkene en er werd geen melding van deze verwerking gemaakt in haar privacyverklaring. Deze verwerking was aldus in strijd met artikel 6 a) van de AVG. Bovendien dienen de betrokkenen goed geïnformeerd te zijn en dient de toestemming vrijwillig gegeven te zijn.

21. Naast de hierboven genoemde praktijk, was er een gebrek aan transparantie in de technische mogelijkheden van de applicatie. Die applicatie stelde de gastheer van een videogesprek in staat zaken te ondernemen die onzichtbaar blijven voor de mededeelnemers. De gastheer kan bijvoorbeeld de gesprekken opnemen, uitwerken en later met derde partijen bespreken of aan derde partijen doorgeven. Opnieuw gebeurt deze verwerking zonder toestemming van de betrokkenen.

22. Op 1 april kondigde het bedrijf aan de transparantie naar haar gebruikers toe te verhogen en daarbij de zogenaamde "attention tracking-feature" uit te schakelen. Die liet hosts (en vaak dus werkgevers) toe om zonder toestemming van de betrokkenen na te gaan in hoeverre deelnemers (en vaak dus werknemers) al dan niet actief deelnemen aan het gesprek en/of actief zijn in andere tabbladen of applicaties. Ook deze gegevens werden verwerkt zonder geïnformeerde toestemming van de betrokkenen.

23. Er heeft dus, in strijd met artikel 6 AVG, onrechtmatige verwerking van persoonsgegevens plaatsgevonden.

Schending artikel 12 AVG – Transparante informatie, communicatie en nadere regels voor de uitoefening van rechten van de betrokkene

24. Een belangrijke tekortkoming inzake transparantie naar de betrokkenen is de claim van Zoom van het bedrijf op haar website en in haar security whitepaper dat het "end-to-end encryption" gebruikt op voorwaarde dat elke deelnemer aan een gesprek inbelt vanop een computer of mobiele applicatie. Onder druk van The Intercept heeft Zoom toegegeven dat Zoom's definitie "end-to-end" en "endpoint" nogal verschilt van de gangbare definitie. Zo blijkt dat Zoom de term "end to end" versleuteling begrijpt als de verbinding die versleuteld wordt van Zoom end point naar Zoom end point. Deze praktijk werd op veel kritiek onthaald, wordt door security analisten gezien als misleidende communicatie en vormt aldus ook een schending van het transparantiebeginsel zoals voorzien in de AVG. Zoals gezegd is deze tekortkoming toegegeven door Zoom.

25. Verschillende privacy experts, waaronder zij die verbonden zijn aan de consumenten beschermingsorganisatie Consumer Reports, ontdekten dat Zoom conform haar eigen privacy policy het recht had om de persoonsgegevens van gebruikers te delen met derde partijen en marketingbedrijven. Onder de noemer "Does Zoom sell Personal Data?" luidt de verklaring: "Depends what you mean by 'sell.'" Samengevat stelde de privacy policy dat, hoewel Zoom de persoonsgegevens van gebruikers niet verkoopt aan derde partijen in ruil voor geld, Zoom die persoonsgegevens wél deelt met derde partijen (zoals bijvoorbeeld Google, LinkedIn en Facebook) omwille van "business purposes". Hoewel Zoom sindsdien haar privacy policy heeft aangescherpt, blijft het onduidelijk in hoeverre Zoom precies de persoonsgegevens van haar gebruikers deelt met genoemde marketingbedrijven.

26. Er blijven ten slotte ook bij het gewijzigde transparantiebeleid vragentekens staan. Zo stelde Zoom bijvoorbeeld op 29 maart 2020 dat het opnames zal maken van elk videogesprek waarvan de gastheer dat wenst.[20] Dat betekent echter dat Zoom te allen tijde toegang heeft tot de inhoud van die videogesprekken. Zoom zegt nergens dat het geen andere inhoud opslaat. Zolang Zoom niet duidelijk stelt dat het daadwerkelijke end-to-end versleuteling gebruikt, heeft Zoom feitelijk toegang tot deze gegevens. Het is tot op heden onduidelijk in welke mate Zoom precies toegang heeft tot deze gegevens en hoelang het de opgeslagen gegevens precies bewaart.

27. Al deze onduidelijkheden wijzen op een gebrek aan transparantie, hetgeen strijd oplevert met artikel 12 AVG.

Schending artikel 25 AVG – Gegevensbescherming door ontwerp en door standaardinstellingen

28. Op 9 mei jl. kondigde Zoom een reeks maatregelen aan, waaronder het verplicht maken van wachtwoorden voor videogesprekken. Tot dan was de standaardoptie of 'default' om géén wachtwoord in te stellen bij het aanmaken van een nieuw videogesprek. Dit was een duidelijke schending van het "privacy by default" principe. Artikel 25 van de AVG schrijft immers voor dat de nodige technische en organisatorische maatregelen dienen te worden getroffen opdat "persoonsgegevens in beginsel niet zonder menselijke

[20] https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/.

tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt." Met deze praktijk heeft Zoom artikel 25 AVG geschonden.

Schending artikel 32 AVG – Beveiliging van de verwerking

29. In overeenstemming met artikel 32 nemen de verwerkingsverantwoordelijke en de verwerker "passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen". De beveiliging van Zoom is niet in overeenstemming met artikel 32 AVG.

30. Beveiligingsexperts hebben verschillende gebreken aan de beveiliging van Zoom ontdekt, waaronder "zero day-exploits". Zo is er:

    - een bug die het Windows wachtwoord kan stelen;
    - een bug die toelaat om via de chat functie malware te installeren;
    - een ernstig lek in de Zoom Waiting Rooms;
    - een bug die toelaat om administrator rechten te krijgen over het volledige Mac-systeem.

31. Ook lijkt Zoom hacker-achtige technieken te gebruiken om de beveiliging van Mac-systemen te omzeilen. Een andere bug maakt het dan weer mogelijk om als buitenstaander een vergadering binnen te dringen en als administrator op te treden of om de microfoon of webcam over te nemen. Ten slotte kunnen of konden ook opnames van videogesprekken op de cloudservers van Zoom gemakkelijk teruggevonden en vaak ook integraal bekeken worden.

32. Een bijkomend risico voor de betrokkenen dat veelvuldig is beschreven, is het eerder genoemde fenomeen van "Zoom-bombing". Vreemden dringen een vergadering binnen om daar dan hun boodschap van welke aard dan ook achter te laten. Het probleem heeft zo'n omvang gekregen dat verschillende nationale en internationale autoriteiten, waaronder de Autoriteit Persoonsgegevens, richtlijnen hebben uitgebracht om Zoom op een meer veilige manier te kunnen gebruiken.

33. Ook de versleuteling van persoonsgegevens, die specifiek vermeld wordt in artikel 32 AVG onder a, was niet in orde. Op haar website verklaart Zoom dat zij het AES-256 algoritme gebruikt om video en geluid data die verstuurd wordt tussen Zoom servers en Zoom Clients te versleutelen. Onderzoekers van Citizen Lab aan de University of Toronto ontdekten echter dat Zoom het zwakkere AES-128 algoritme gebruikt. Bovendien bleken deze sleutels, ook voor gebruikers uit de EER en de Verenigde Staten, vaak gegenereerd door Chinese servers.

34. Deze gebreken leiden tot de conclusie dat de beveiliging van Zoom in strijd is met artikel 32 AVG.

Schending artikel 33 AVG – Melding inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit

35. De voorbije maanden zijn er verschillende belangrijke gegevenslekken bekend geraakt waarbij persoonsgegevens van Zoom gebruikers vrijkwamen. Zo rapporteerde Yahoo News dat er Zoom accounts illegaal werden verhandeld (via het 'dark web').

36. Onderzoekers van IngSights ondekten dat er 2.300 Zoom login gegevens werden verkocht op een online crimineel forum. Midden april 2020 rapporteerde het Singaporese informatie veiligheidsbedrijf Cyble dat het 530.000 gegevens van Zoom gebruikers wist aan te schaffen via het Dark web voor slechts 0,2 cent per stuk. Deze veelvuldige gegevenslekken onderstrepen nogmaals het zwakke beveiligingsniveau en het gebrek aan passende technische waarborgen door Zoom.

37. Bovendien dient Zoom, conform artikel 33 van de AVG, dergelijke gegevenslekken uiterlijk binnen de 72 uur na de kennisname ervan te melden aan de Toezichthoudende Autoriteit. Het is onduidelijk in hoeverre het bedrijf deze verplichting is nagekomen. Graag ontvangen wij namens onze Deelnemers ook hier alle informatie over.

MF

Schending artikel 45 AVG – Doorgifte op basis van adequaatheidsbesluiten

38. Zoom stelt dat het aan de Amerikaanse wetgeving voldoet inzake toegang van de overheid tot opgeslagen data. Het werkterrein van Zoom is echter wereldwijd. Dat betekent dat bijvoorbeeld de Amerikaanse overheid dankzij de Cloud Act potentieel toegang heeft tot buitenlandse data. Dat betekent dat die overheid niet alleen toegang kan opeisen tot allerlei bedrijfsdata, maar zelfs confidentiële data van vreemde mogendheden. De doorgifte van gegevens van gebruikers in de EER naar de VS is geregeld onder het USEU Privacy Shield framework. Deze doorgifte is echter aan heel wat voorwaarden onderworpen. Nu blijkt dat Zoom, in tegenstelling tot wat zij aan haar gebruikers communiceert, géén daadwerkelijke end-to-end encryptie gebruikt, zwakkere AES-128 – encyptie sleutels gebuikt en daarbij gebruik maakte van Chinese servers om deze sleutels uit te geven, schendt Zoom de voorwaarden van het US-EU Privacy Shield framework. In dat geval heeft Zoom een specifieke toestemming nodig voor een dergelijke doorgifte van persoonsgegevens buiten de EER.

39. Op 13 april 2020 kondigde Zoom aan dat betaalde gebruikers van Zoom voortaan zouden kunnen kiezen via welke regio hun data omgeleid zou worden: Australië, Canada, China, Europa, India, Japan/Hong Kong, Latijns America of de Verenigde Staten. Deze keuze was voordien niet voorhanden en blijft mogelijk ook vandaag nog achterwege voor (een deel van de) niet-betalende klanten.

Conclusie klacht

40. Gelet op al het voorgaande is sprake van ernstige en grootschalige schendingen door Zoom van de privacy van gebruikers en van verschillende herhaaldelijke overtredingen van de AVG.

Afronding

41. Namens SOMI en de deelnemers verzoek ik u om deze klacht in behandeling te nemen en om mij te informeren over de ontvangst van deze klacht en over de wijze waarop Zoom deze klacht in behandeling zal nemen. Ook verneem ik graag wanneer Zoom uiterlijk inhoudelijk op deze klacht zal reageren.

Hoogachtend,

Stichting Onderzoek Marktinformatie

Mr. Drs. H.J.M.G. Franke