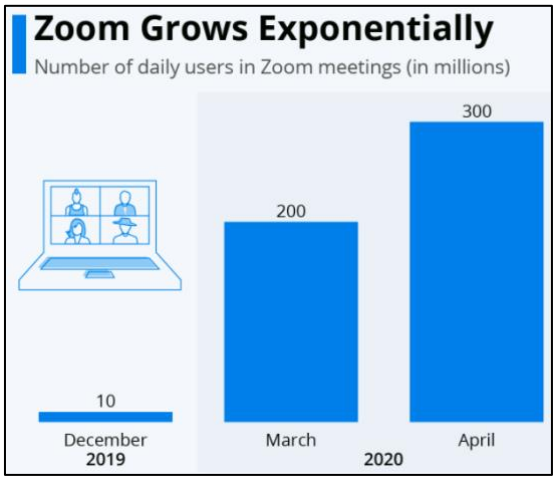
InZOOMen op privacy



Tabel van *Statista.com*

Zoom is één van de populairste videoapplicaties op dit moment.[i] Wereldwijd heeft Zoom dagelijks bijna 300 miljoen deelnemers aan vergaderingen.[ii]

Vanuit **Legal2Practice** en onze rol als externe FG, merken we dat de onrust over het gebruik van Zoom toeneemt. Er zijn veel vragen over de veiligheid van deze dienst voor videobellen vanuit organisaties.

Houdt een populaire app als Zoom zich wel aan de algemeen geldende Europese privacywetgeving en aan welke veiligheidsmaatregelen voldoen ze nou echt? Wij vinden het belangrijk dat u en de partijen waar u mee samenwerkt, in het dagelijks gebruik zorgvuldig met persoonsgegevens kunnen blijven omgaan. Met onze **Legal2Practice**-privacybril kijken wij daarom naar Zoom, de AVG en alle berichtgeving daaromheen om u objectief van feitelijke informatie te kunnen voorzien.

InZOOMen op privacy

Sinds het merendeel van werkend Nederland massaal vanuit huis werkt, is het zoeken naar creatieve oplossingen. Videobellen is een vervangend communicatiemiddel geworden voor veel organisaties. Zo wordt er door middel van videobellen op afstand lesgegeven, door bedrijven vergaderd, een vrijmibo met collega's gehouden, maar wordt videobellen ook in toenemende mate gebruikt voor het bespreken van (bedrijfs)vertrouwelijke informatie.

Met dit factsheet geven wij een overzicht van wat er goed of minder goed is aan Zoom en hoe je Zoom veilig kunt gebruiken.[iii]

Wat speelt er rondom Zoom?

In de media wordt het beeld geschetst dat Zoom niet zo veilig is, als zij zichzelf voordoet.[iv] De Amerikaanse videoconferencing tool Zoom is in de media onder vuur te komen liggen nadat gebruikers van de tool verschillende problemen hadden gemeld.[v] Zo zouden gegevens van IPhone-gebruikers van Zoom worden gedeeld met Facebook.[vi] Een gebruiker in Californië heeft Zoom om deze reden aangeklaagd.[vii] Ook zou Zoom e-mailadressen en foto's van ten minste duizend van haar gebruikers naar andere gebruikers hebben gelekt.[viii] Bovendien zouden vreemden de mogelijkheid hebben om een videogesprek met gebruikers te starten. Zoom voegde namelijk automatisch alle mensen die zich hebben aangemeld met een e-mailadres dat hetzelfde domein deelt, toe aan de lijst met contacten van een gebruiker. Zoom is dan in de veronderstelling dat deze mensen allemaal bij hetzelfde bedrijf zouden werken.[ix] Dit is bijvoorbeeld gebeurd bij mensen die een e-mailadres hebben dat eindigt op @xs4all.nl.[x] Tenslotte zouden de wachtwoorden van gebruikers van Zoom niet passend beveiligd zijn, waardoor voor een kwaadwillende de mogelijkheid bestaat om de wachtwoorden van gebruikers Zoom te achterhalen.[xi]

Met betrekking tot de beveiliging beweert Zoom gebruik te maken van "end-to-end encryptie (E2E)".[xii] Hierbij worden berichten versleuteld en zijn deze alleen voor zender en ontvanger te begrijpen. De centrale server stuurt de versleutelde berichten door en heeft zelf geen inzicht in de versleutelde data. E2E-encryptie is de veiligste manier van versleuteling.[xiii] Onderzoeksite *The Intercept* heeft echter onthuld dat Zoom geen gebruik maakt van volwaardige E2E-encryptie, althans niet gelijk aan wat de algemene opinie over deze vorm van versleuteling is. Volgens *The Intercept* gebruikt Zoom een lichtere beveiligingsvariant.[xiv] Volgens een woordvoerder van Zoom "is het op dit moment niet mogelijk om E2E-encryptie in te schakelen voor Zoom-videovergaderingen. Zoom-videogesprekken maken gebruik van een combinatie van TCP en UDP. TCP-verbindingen worden gemaakt met behulp van TLS en UDP-verbindingen worden versleuteld met AES door middel van een key die via een TLS-verbinding wordt gecommuniceerd."[xv]

Zoom maakt voor de beveiliging van videobellen gebruik van TLS, dezelfde encryptie die webservers gebruiken om HTTPS-websites te beveiligen. Dit betekent dat de service van Zoom zelf toegang heeft tot de onversleutelde video- en audio-inhoud van Zoom-bijeenkomsten. Als u een bijeenkomst via Zoom organiseert, blijft de video- en audio-inhoud versleuteld voor derden die proberen mee te kijken via Wi-Fi, maar niet voor Zoom zelf. Zolang Zoom geen gebruik maakt van volwaardige E2E-encryptie, heeft Zoom dus technisch gezien de mogelijkheid om met privé- of vertrouwelijke bijeenkomsten mee te kijken.[xvi]

De Amerikaanse justitie heeft aangegeven dat ze een onderzoek gaan instellen naar Zoom. De openbaar aanklager in New York is

bezorgd dat de bestaande veiligheidspraktijken van Zoom niet voldoende zijn om zich aan te passen aan de recente en plotselinge schommeling in zowel het volume als de gevoeligheid van persoonsgegevens die door Zoom circuleren. De organisatie moet duidelijkheid verschaffen over hoe zij de diverse 'privacy problemen' gaat aanpakken.[xvii]

Welke veiligheidsmaatregelen neemt Zoom met betrekking tot het beschermen van de privacy van haar gebruikers?

Zoom heeft in een blogpost van 1 april jl. haar excuses aangeboden voor de problemen bij het beschermen van de privacy en veiligheid van haar gebruikers.[xviii] Desondanks verklaart Zoom dat zij voldoet aan alle eisen van de AVG.[xix] In een blog die Zoom op haar website heeft gepubliceerd geeft zij aan al diverse maatregelen te hebben genomen om een aantal tekortkomingen op te lossen en ondertussen te werken aan de rest van de problemen.[xx] Een van de oplossingen is het bieden van ondersteuning aan gebruikers om wegwijs te worden met de applicatie en het toelichten van de verschillende accountfuncties ervan. Op deze manier hoopt Zoom gebruikers vertrouwd te maken met het gebruik van het platform. Verder heeft Zoom inmiddels de optie om in te loggen via Facebook verwijderd uit de iOS-app, om zo tegen te gaan dat onnodige gebruikersinformatie wordt verzameld.[xxi]

Zoom geeft in haar Privacy Policy aan dat zij privacy een extreem belangrijk onderwerp vindt en dit erg serieus neemt.[xxii] Om duidelijker, explicieter en transparanter te zijn over welke gegevens verzameld en hoe deze gebruikt worden, is deze Privacy Policy op 29 maart bijgewerkt.[xxiii] Daarnaast gebruikt Zoom een DPA (Data Processing Agreement) voor haar gebruikers.[xxiv]

Als extra beveiligingsmaatregel biedt Zoom meerdere authenticatie mogelijkheden aan zoals SAML, Google of Facebook OAuth en/of het gebruik van wachtwoorden.[xxv] Daarnaast maakt het bedrijf gebruik van een netwerk dat beveiligd wordt door middel van een Advanced Encryption Standard met een 256-bit key (AES-256) en wordt data beschermd verstuurd middels gebruik van HMAC-SHA256 message authentication codes.[xxvi] Verder worden de door Zoom gebruikte data centers op meerdere manieren fysiek beveiligd.[xxvii] Tot slot stelt Zoom dat de chatfunctie E2E wordt geëncrypt.[xxviii]

Voor het beoordelen van het IT vendor risk bij het gebruik van Zoom en het bieden van passende waarborgen aan haar klanten, stelt Zoom diverse documenten en certificeringen beschikbaar[xxix]:

- AICPA SOC 2 (Type II)
- FedRAMP (Moderate)
- Privacy Shield Certified (Self Certification[xxx])
    - EU/US Privacy Shield
    - Swiss/US Privacy Shield
- TRUSTe Certified Privacy
    - Certified Privacy Practices and Statements.

Wat Zoom gaat doen voor nog veiliger gebruik

Zoom geeft zelf aan er nog niet te zijn en de komende tijd zich te richten op de problemen die er nog liggen.[xxxi] Zo zijn ze voornemens externe experts en gebruikers in te zetten om een uitgebreide beoordeling uit te voeren om op deze manier de veiligheid van de gebruikers te garanderen en te begrijpen. Ten tweede wordt er een CISO-raad opgericht om samen met CISO's best practices uit te wisselen op het gebied van privacy en veiligheid. Zelf gaat Zoom CEO Eric S. Yuan iedere woensdag een webinar hosten om de updates omtrent privacy en veiligheid die de app neemt, te delen.[xxxii] Deze snelle stap naar voren in het bieden van transparantie aan gebruikers, komt terug in de gepubliceerde

blogs van Zoom en het inmiddels opgestelde 90-dagenplan om proactief de beveiliging en privacy van de app te monitoren en te versterken.[xxxiii]

Als onderdeel van het 90-dagenplan heeft Zoom inmiddels een update uitgebracht; Zoom versie 5.0..[xxxiv] Met de update zijn vooral verbeteringen in de beveiliging doorgevoerd. Allereerst wordt de versleuteling van de app verbeterd. Zoom zal voortaan gebruik maken van AES 256-bit GCM-encryptie. Deze encryptiestandaard moet een verbeterde beveiliging bieden van de data uit meetings en Zoom resistenter maken tegen aanvallen.[xxxv]

Daarnaast kunnen beheerders van groepsgesprekken instellen welke datacenters voor de videogesprekken worden gebruikt. Zo hebben zij de keuze om dataservers in bepaalde regio's wel of niet te gebruiken.[xxxvi] Het is echter niet mogelijk om de standaardregio waar de beheerder zich bevindt aan te passen, maar je kan er als Europese beheerder dus wel voor kiezen om in te stellen dat videogesprekken enkel via Europese servers lopen. Opmerking verdient ook nog dat gebruikers van de gratis versie niet kunnen kiezen voor een bepaalde dataserver. Gratis gebruikers in Europa zijn dus gebonden aan de Europese servers. Op deze Europese servers is de AVG van toepassing.[xxxvii]

Bovendien biedt de nieuwe update de mogelijkheid voor beheerders van groepsgesprekken om gebruikers te rapporteren bij Zoom vanwege misbruik. Zo kunnen onbekenden die in een vergadering komen en zich misdragen, gerapporteerd worden.[xxxviii]

Verder staat voortaan bij ieder groepsgesprek een wachtwoord ingesteld en worden potentiële deelnemers eerst in een virtuele wachtruimte geplaatst. Gebruikers kunnen dus niet zomaar meer je video-vergadering binnenkomen.[xxxix]

We raden gebruikers van Zoom dan ook aan om de applicatie zo snel mogelijk te updaten naar Zoom 5.0.[xl]

Hoe kan ik ondertussen Zoom toch veilig gebruiken?

Natuurlijk hoeft u niet direct te stoppen met het gebruik van Zoom op basis van berichten in de media. Van belang is om eerst in kaart te brengen waarvoor uw organisatie Zoom wil inzetten en wat daarvan de eventuele risico´s zijn. Het per direct overstappen op andere tools is namelijk ook geen garantie dat dit beter of veiliger is. Verder kan dit op de korte termijn de nodige praktische problemen gaan opleveren doordat je medewerkers moet informeren, waarschuwen, (opnieuw) trainen etc. Zoom kan dus nog steeds gebruikt worden als applicatie voor videobellen. Naast het uitvoeren van een (snelle) risico inventarisatie is het verstandig om sowieso rekening te houden met een aantal randvoorwaarden/tips:

- Gebruik alleen betaalde licenties van Zoom
- Maak medewerkers ervan bewust dat er geen gevoelige berichten en/of opnames gedeeld worden bij het gebruik van Zoom
- Stel een wachtwoord in voor de vergadering[xli]
- Zorg dat two factor authentication (2FA) is ingeschakeld voor zoveel mogelijk accounts
- Gebruik een veilige verbinding door middel van een VPN
- Zet de in-meeting chat uit zodat er geen documenten gedeeld kunnen worden die mogelijk een virus bevatten
- Zet participant tracking uit
- Zorg dat na beëindiging van de vergadering de data bij Zoom worden verwijderd

- Update de Zoom-applicatie regelmatig zodat eventuele aanpassingen worden bijgewerkt[xlii]
- Plak een sticker op de camera wanneer deze niet wordt gebruikt[xliii]
- Zet notificaties van andere apps uit[xliv]
- Gebruik in plaats van jouw persoonlijke Zoom Meeting ID een unieke Meeting ID
- Zet de optie “waiting room” aan en “join before host” uit wanneer er ook externen deelnemen
- Lock de meeting zodra deze is gestart, zodat nieuwe deelnemers geen toegang hebben
- Zet de optie om berichten op te slaan of de meeting op te nemen uit[xlv]
- Sluit een verwerkersovereenkomst af met Zoom[xlvi]

In 2017 heeft het NCSC een factsheet gemaakt die nu nog steeds actueel is en gebruikt kan worden om de juiste app te kiezen.[xlvii] Deze biedt een overzicht van de risico‘s die bepaalde tools met zich meebrengen en biedt nuttige tips. Belangrijk is verder om te onthouden dat er altijd privacy- en beveiligingsrisico’s hangen aan het gebruik van tools zoals Zoom en het daarom belangrijk is het risico en het doel van het gebruik goed tegen elkaar af te wegen.[xlviii]

Zoom en de AVG

Valt het gebruik van applicaties zoals Zoom onder de DPIA plicht van artikel 35 AVG? Artikel 35 lid 1 van de AVG stelt dat een DPIA nodig is in het geval dat een verwerking kan worden aangemerkt als een verwerking die in alle waarschijnlijkheid een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.[xlix] Daarnaast heeft de AP een lijst gepubliceerd met daarop een aantal onderwerpen waarbij een DPIA sowieso verplicht is. De vraag is nu of we het gebruik van Zoom kunnen kwalificeren als een verwerking die een hoog risico met zich meebrengt of onder een van de door de AP gekozen onderwerpen valt.

Als vuistregel voor een hoog risico hebben de Europese toezichthouders negen criteria opgesteld waarbij er spraken is van een hoog risico als een verwerking aan twee of meer van die criteria voldoet.[l] Het gaat om:
1) Beoordelen van mensen op basis van persoonskenmerken
2) Geautomatiseerde beslissingen
3) Stelselmatige en grootschalige monitoring
4) Gevoelige gegevens
5) Grootschalige gegevensverwerking
6) Gekoppelde databases
7) Gegevens over kwetsbare personen
8) Gebruik van nieuwe technologieën
9) Blokkering van een recht, dienst of contract.

Belangrijk voor de vraag of het gebruik van Zoom voor jouw organisatie een groot risico meebrengt is afhankelijk van de vraag voor welke doeleinden Zoom wordt ingezet. Als een huisarts een digitaal spreekuur via Zoom wil organiseren zal er een DPIA uitgevoerd moeten worden. Niet alleen omdat dit voldoet aan twee van de bovenstaande negen punten maar ook omdat de AP een DPIA verplicht bij de verwerking van gezondheidsgegevens. Op het moment dat Zoom gebruikt gaat worden voor reguliere teammeetings waar geen gevoelige, bijzondere of vertrouwelijke persoonsgegevens of zaken worden besproken, is het aannemelijk dat er geen sprake is van een hoog risico dan wel een van de zeventien onderwerpen van de AP en is er ook geen verplichting tot het uitvoeren van een DPIA.

Echter, bij twijfel over de aard van de risico´s is het aan te raden om altijd een DPIA uit te voeren om te kunnen beoordelen of er inderdaad sprake is van een hoog risico. Door dit te doen en de resultaten vast te leggen, kun je desgevraagd aantonen wat de reden is om de verwerking uiteindelijk toch niet als

een hoog risico te beschouwen. Dit tegen de achtergrond van de verplichting van artikel 5 lid 2 AVG om aantoonbaar aan de AVG te voldoen.

Naast de verplichting om al dan niet een DPIA uit te voeren bij het gebruik van Zoom stelt de AVG ook nog een andere eis die zakelijke gebruikers in het achterhoofd moeten houden. Aangezien het gebruik van Zoom leidt tot de verwerking van persoonsgegevens raden wij aan om een verwerkersovereenkomst af te sluiten met Zoom. Hierin wordt onder andere overeengekomen dat Zoom alleen persoonsgegevens mag verwerken krachtens een vooraf vastgelegd doel, de vooraf vastgestelde technische en organisatorische maatregelen neemt of heeft genomen en Zoom aansprakelijk kan worden gehouden voor schending van gemaakt afspraken. Zoom biedt zelf een 'pre-signed Data Processing Addendum' aan die hiervoor gebruikt kan worden.[li]

Er vallen ons wel een aantal zaken op uit de Data Processing Agreement (DPA) van Zoom. Allereerst beperkt Zoom zich in artikel 2 tot het zijn van enkel (sub-)processor; zij zullen nooit optreden als controller (verwerkingsverantwoordelijke). Hieruit volgt dat Zoom, krachtens artikel 3.2, enkel persoonsgegevens verwerkt voor de doelen die overeengekomen zijn in de DPA. Een uitzondering hierop zijn de gevallen waarin (Amerikaanse) wetgeving dicteert dat Zoom bepaalde verwerkingen van data uitvoert. In artikel 4.2 stelt Zoom vast dat zij hun medewerkers, voor het geval zij (kunnen) beschikken over persoonsgegevens, een 'Confidentiality Agreement' hebben laten ondertekenen.

Artikel 5 heeft betrekking op het gebruik van subverwerkers door Zoom. Zoom geeft in dit artikel aan dat zij gebruik mogen maken van alle partijen die zij in een speciale subverwerkers lijst op hun site noemen.[lii] Deze lijst kan geüpdatet worden waarbij de klant enkel op de hoogte wordt gesteld van potentieel nieuwe subverwerkers als de klant dit aangeeft. Op het moment dat een klant niet akkoord gaat met een nieuwe subverwerker of het door Zoom aangedragen alternatief, dan heeft Zoom de mogelijkheid om de DPA te beëindigen.

Met betrekking tot de veiligheid en bescherming van persoonsgegevens stelt artikel 6 dat, rekening houdend onder meer met de kosten van implementatie en de omvang en het doel van de verwerking, Zoom passende technische en organisatorische veiligheidsmaatregelen neemt. Een lijst van wat dit onder meer inhoudt is te vinden in 'Exhibit B' van de DPA. Wij raden aan om deze lijst met de CISO of IT safety expert van de eigen organisatie te bespreken. Voor overdracht van persoonsgegevens naar landen buiten de EU hanteert Zoom krachtens artikel 7 'EU Standard Contractual Clauses' en/of het Privacy Shield Framework.

De rechten van data subjecten zien we terug in artikel 8, waarbij Zoom als verwerker zijn medewerking verleent in het geval van een Data Subject Request en zij zullen de klant op de hoogte stellen van verzoeken die zij van gebruikers binnenkrijgen. In artikel 9 zien we, naast een aanvulling op Zoom's verplichting van artikel 8 om documentatie bij te houden om aan te kunnen tonen dat ze voldoen aan hetgeen is overeengekomen in de DPA, de mogelijkheid om als klant rapporten en certificaten op te vragen die compliance met data security standaarden laat zien. Daarnaast gaan artikel 9 leden 5 tot en met 7 in op het geval van een datalek. In dat geval zal Zoom dit melden zonder onnodige vertraging maar niet meer dan 72 uur na bevestiging van die datalek. In eerste oogopslag lijkt dit ruimer dan de termijn die de AP stelt, namelijk niet meer dan 72 uur na ontdekking van een datalek. Verder stelt Zoom, afhankelijk van de verwerking, zijn medewerking te verlenen aan klanten bij het voldoen aan diens

verplichtingen onder specifieke privacywetgeving. Het bovenstaande gaat niet op in het geval dat het datalek het gevolg is van acties of omissies van de klant.

VERGELIJKINGEN

Zoom biedt een aantal verschillende versies aan, te weten: 'Basic', 'Pro', 'Business' en 'Enterprise'. Hieronder zullen kort de belangrijkste verschillen besproken worden:

	Basic	Pro	Business	Enterprise
Number of participants	Max. 100	Includes 100 participants	Includes 300 participants	Includes 500 participants
Time limit per meeting	Max. 40 minutes	Max. 24 hours	Max. 24 hours	Max. 24 hours
Support	Online Support	Online Support	Dedicated phone support	Dedicated customer succes manager
Security	- SSL encryption - AES 256-bits encryption	- See Basic, including: - User Management - Admin feature controls	- See Pro, including: - Admin dashboard - Option for on-premise - Single sign-on	- See Business
Price	Free	€13.99/mo/host	€18.99/mo/host minimum 10 host	€18.99/mo/host minimum 50 host

Daarnaast biedt Zoom ook oplossingen voor de volgende specifieke bedrijfstakken:

- Zorginstellingen
- Overheidsinstellingen
- Financiële instellingen
- Onderwijsinstellingen.

Zorginstellingen
Bij de toepassing voor zorginstellingen is er gekeken naar Amerikaanse en Canadese regelgeving omtrent privacy en gezondheidsgegevens. De wetten waar Zoom aan refereert zijn 'the Health Insurance Portability and Accountabiliyu Act' (HIPAA) uit de VS, de Canadese 'Personal Information Protection and Electronic Documents Act' (PIPEDA) en 'the Personal Health Information Protection Act' (PHIPA) specifiek voor Ontario. In een tweetal documenten gaat Zoom in op de door het bedrijf genomen maatregelen en in hoeverre die aansluiten bij de desbetreffende wetgeving.[liii] Zoom beschikt niet over HIPAA dan wel PIPEDA of PHIPA certificering, omdat er op dit moment geen partijen zijn die een bedrijf als Zoom certificeren. Aan de hand van eerdergenoemde vergelijking veronderstelt Zoom zelf dat hun applicatie ook bruikbaar is voor zorginstellingen.

Onderwijsinstellingen
Net als bij de analyse over zorginstellingen is er ook voor onderwijsinstellingen een vergelijking gemaakt door Zoom met Amerikaanse wetgeving. Zoom vergelijkt zijn eigen veiligheidsmaatregelen met die door de Amerikaanse overheid in 'the Federal Education Rights and Privacy Act' (FERPA) zijn vastgesteld.[liv] Echter, wederom is er geen specifiek FERPA certificaat beschikbaar omdat er op dit moment geen partijen zijn die een

bedrijf als Zoom certificeren; dit moet door de onderwijsinstelling zelf bepaald worden.

Overheidsinstellingen
Zoom gaat niet in op specifieke wetgeving voor overheidsinstellingen zoals bijvoorbeeld 'the Privacy Act of 1974' uit Amerika.[lv] Wel worden de FERPA en HIPPA genoemd als regelgeving waar Zoom aan voldoet.[lvi]

Financiële instellingen
Overeenkomstig met het kopje over overheidsinstellingen wordt er ook hier niet ingegaan op specifieke wetgeving zoals 'the Right to Financial Privacy Act' (RFPA) uit Amerika.[lvii] Wederom wordt er verwezen naar compliance met FERPA en HIPPA.[lviii]

Welke alternatieven zijn er voor Zoom?

Vanzelfsprekend is Zoom niet de enige tool die online videobellen faciliteert. Er zijn talloze alternatieven beschikbaar die gebruikt kunnen worden en wellicht beter aansluiten bij uw situatie.

De Autoriteit Persoonsgegevens (AP) heeft een 'Keuzehulp privacy videobellen' opgesteld, waarbij dertien veelgebruikte videobel-apps met elkaar zijn vergeleken.[lix] De AP heeft alleen gekeken naar wat de bedrijven zelf zeggen over wat de videobel-apps met persoonsgegevens doen, bijvoorbeeld in hun privacyverklaring.[lx]

Volgens Bits of Freedom is Jitsi Meet[lxi] de beste app om te gebruiken als je met meerdere mensen wilt videobellen. Uit hun onderzoek blijkt namelijk dat Jitsi het beste omgaat met de privacy van haar gebruikers.[lxii] Jitsi is een open source tool die het verkeer tussen Jitsi en de gebruiker versleuteld, wat het gebruik van de applicatie veiliger maakt.[lxiii] Ook in de keuzehulp van de AP scoort Jitsi hoog, vooral op de beveiliging van de communicatie. Jitsi maakt gebruik van E2E-encryptie en iedereen kan de broncode controleren (open source). Tenslotte verzamelt Jitsi geen gegevens van haar gebruikers.[lxiv] Jitsi is namelijk een non-profit organisatie en verzamelt geen gegevens om geld mee te verdienen.[lxv]

Uit de keuzehulp van de AP blijkt voorts dat de apps Signal[lxvi] en Nextcloud Talk[lxvii] geen gegevens van gebruikers verzamelen, een open source broncode hebben en E2E-encryptie bieden.[lxviii] De kanttekening hierbij is dat je bij Signal maar met maximaal twee personen kan videobellen en dat Nextcloud Talk alleen tegen betaling beschikbaar is.[lxix]

Een mogelijk ander betaald alternatief is Wire. Deze applicatie is open source en biedt end-to-end encryptie. Wire geeft zelf aan conform de AVG te handelen.[lxx] Een gratis alternatief dat versleutelde videobijeenkomsten aanbiedt is Wickr. Zij geven aan geen gegevens van gebruikers te bewaren.[lxxi]

In haar keuzehulp heeft de AP alleen achter de videobel-app Zoom een sterretje heeft geplaatst met de opmerking: "Wees voorzichtig als u Zoom gebruikt. Deze app is nog volop in ontwikkeling."[lxxii]

Tot slot

We zullen u op de hoogte houden van de laatste ontwikkelingen met betrekking tot het veilig gebruik van Zoom. Het belang van de bescherming van de privacy en het bieden van veiligheid kan verschillen per video-vergadering. Bedenk dus vooraf voor welk doel u Zoom wilt gebruiken en of de versie van Zoom die u daarbij wilt gebruiken, hiervoor passend is of dat u mogelijke restrisico's bewust wilt accepteren. Zoals aangegeven, zal Zoom de komende tijd komen met de nodige verbeteringen op het gebied van beveiliging en privacy. Belangrijk is dan ook om deze ontwikkelingen te blijven volgen om te kunnen beoordelen of het gebruik van Zoom binnen de eigen organisatie kan worden voortgezet of dat dit gebruik dient te worden uitgesteld. Wij zullen deze factsheet steeds bijwerken aan de hand van de laatste ontwikkelingen. Voor een

inhoudelijk advies over het gebruik van Zoom binnen de context van uw organisatie, kunt u uiteraard contact met ons opnemen.

Gezonde groet,

Legal2Practice B.V.
+31 (0) 26 848 3118
info@legal2practice.nl

Geraadpleegde bronnen:

[i] M. Hijink & S. Bronzwaer, 'Is Zoom wel veilig? En vijf andere vragen over videobellen', *Nrc.nl* 1 april 2020; 'Onveilige wachtwoorden en zwakke encryptie: wat speelt er rond Zoom?', *Nu.nl* 1 april 2020.

[ii] 'Zoom groeit met de helft in een maand: nu 300 miljoen dagelijkse gebruikers', *Nu.nl* 23 april 2020; M. Hijink, '300 miljoen gebruikers, maar zo had Zoom het nooit bedoeld', *Nrc.nl* 24 april 2020.

[iii] NB. Deze factsheet is een tweede versie en zal verder worden uitgebreid naar aanleiding van recente ontwikkelingen.

[iv] 'Onveilige wachtwoorden en zwakke encryptie: wat speelt er rond Zoom?', *Nu.nl* 1 april 2020; M. Hijink & S. Bronzwaer, 'Is Zoom wel veilig? En vijf andere vragen over videobellen', *Nrc.nl* 1 april 2020.

[v] 'Baas populaire app Zoom biedt excuses aan voor privacyproblemen', *Nrc.nl* 3 april 2020.

[vi] J. Cox, 'Zoom iOS app sends data to Facebook even if you don't have a Facebook account', *Vice.com* 26 maart 2020.

[vii] I. A. Hamilton, 'Zoom is being sued for allegedly handing over data to Facebook', *Businessinsider.com* 31 maart 2020.

[viii] J. Cox, 'Zoom is leaking peoples'email adresses and photos to strangers', *Vice.com* 1 april 2020; T. Hofmans, 'Zoom liet e-mailadressen en Windows-wachtwoorden uitlekken in aantal incidenten', *Tweakers.net* 1 april 2020.

[ix] 'Onveilige wachtwoorden en zwakke encryptie: wat speelt er rond zoom?', *Nu.nl* 1 april 2020; J. Cox, 'Zoom is leaking peoples'email adresses and photos to strangers', *Vice.com* 1 april 2020.

[x] XS4ALL, @xs4all *Twitter.com* 29 maart 2020 12:57.

[xi] 'Onveilige wachtwoorden en zwakke encryptie: wat speelt er rond zoom?', *Nu.nl* 1 april 2020.

[xii] 'Security Guide Zoom Video Communications, Inc.', *Zoom.us* juni 2019.

[xiii] M. Hijink & S. Bronzwaer, 'Is Zoom wel veilig? En vijf andere vragen over videobellen', *NRC.nl* 1 april 2020.

[xiv] M. Lee & Y. Grauer, 'Zoom meetings aren't end-to-end encrypted, despite misleading marketing', *Theintercept.com* 31 maart 2020.

[xv] Idem.

[xvi] Idem; 'Onveilige wachtwoorden en zwakke encryptie: wat speelt er rond zoom?', *Nu.nl* 1 april 2020.

[xvii] D. Hakim & N. Singer, 'New York attorney general looks into Zoom's privacy practices', *Nytimes.com* 30 maart 2020.

[xviii] E. S. Yuan, 'A message to our users', *Blog.zoom.us* 1 april 2020.

[xix] 'Official statement: EU GDPR Compliane', *Support.zoom.us.*

[xx] E. S. Yuan, 'A message to our users', *Blog.zoom.us* 1 april 2020.

[xxi] E. S. Yuan, 'Zoom's use of Facebook's SDK in iOS client', *Blog.zoom.us* 27 maart 2020.

[xxii] 'Privacy Policy', *Zoom.us* 29 maart 2020.

[xxiii] A. Bawa, 'Zoom's Privacy Policy', *Blog.zoom.us* 29 maart 2020.

[xxiv] 'Global Data Processing Addendum', *Zoom.us* december 2019.

[xxv] 'Security at Zoom', *Zoom.us.*

[xxvi] 'HIPAA Compliance Guide', *Zoom.us* juli 2017.

[xxvii] 'Zoom and PIPEDA/PHIPA Compliance', *Zoom.us* September 2018.

[xxviii] 'Security at Zoom', *Zoom.us.*

[xxix] Idem.

[xxx] 'A step-by-step guide to self-certification on the privacy shield website', *Privacyshield.gov.*

[xxxi] E. S. Yuan, 'A message to our users', *Blog.zoom.us* 1 april 2020.

[xxxii] Idem.

[xxxiii] E. S. Yuan, 'A message to our users', *Blog.zoom.us* 1 april 2020.
[xxxiv] O. Gal, 'It's Here! 5 Things to Know About Zoom 5.0', *Blog.zoom.us* 27 april 2020.
[xxxv] C. Rodriguez, 'Zoom Hits Milestone on 90-Day Security Plan, Releases Zoom 5.0', *Blog.zoom.us* 22 april 2020.
[xxxvi] B. Ittelson, 'Coming April 18: Control Your Zoom Data Routing', *Blog.zoom.us* 13 april 2020.
[xxxvii] F. Poort, 'Zoom laat betalende gebruikers regio van server kiezen', *Bright.nl* 14 april 2020.
[xxxviii] O. Gal, 'It's Here! 5 Things to Know About Zoom 5.0', *Blog.zoom.us* 27 april 2020.
[xxxix] B. Vroegop, 'Zoom rolt grote update uit: problemen beveiliging aangepakt', *Bright.nl* 23 april 2020.
[xl] 'Download Center', *Zoom.us*
[xli] IBD, 'Vragen over videoconferencingtools', *Informatiebeveiligingsdienst.nl* 25 maart 2020.
[xlii] 'Hoe veilig is zoom en hoe zit het met privacy?', *Iculture.nl* april 2020.
[xliii] N. Van der Louw, 'Hoe gebruik je Zoom op een zo privacyvriendelijk mogelijke manier?', *Ddma.nl* 2 april 2020.
[xliv] Idem.
[xlv] Idem.
[xlvi] Idem.
[xlvii] Nationaal Cyber Security Centrum, 'Kies een berichtenapp oor uw organisatie', *Ncsc.nl* 31 augustus 2017.
[xlviii] L. Oliver, 'What You Should Know About Online Tools During the COVID-19 Crisis', *Eff.org* 19 maart 2020.
[xlix] Artikel 35 EU-AVG, Gegevensbeschermingseffectbeoordeling.
[l] Autoriteit Persoonsgegevens, 'Vraag over DPIA - Wat zijn de criteria van de Europese privacytoezichthouders?', Autoriteitpersoonsgegevens.nl
[li] 'Data Processing Addendum', S*upport.zoom.us.*
[lii] 'Subprocessors', *Zoom.us* 31 december 2019
[liii] 'HIPAA Compliance Guide', *Zoom.us* april 2020; 'Zoom and PIPEDA/PHIPA Compliance', *Zoom.us* september 2018
[liv] 'Zoom and FERPA Compliance', *Zoom.us* februari 2018
[lv] Privacy Act of 1974, The United States Department of Justice.
[lvi] 'Zoom for Government', *Zoom.us*.
[lvii] Right to Financial Privacy Act, The United States Department of Justice.
[lviii] 'Zoom for Financial Services', *Zoom.us.*
[lix] Autoriteit Persoonsgegevens, 'Keuzehulp privacy videobellen', *Autoriteitpersoonsgegevens.nl* versie 15 april 2020.
[lx] Autoriteit Persoonsgegevens, 'Keuzehulp privacy bij videobel-apps', *Autoriteitpersoonsgegevens.nl* nieuwsbericht 15 april 2020.
[lxi] Jitsi, *Meet.jit.si*
[lxii] E. Crabbendam, 'Wegwijs in de tools om te videobellen', *Bitsoffreedom.nl* 7 april 2020; E. Austin, 'Tool nodig om te videobellen? Probeer Jitsi.', *Bitsoffreedom.nl* 26 maart 2020.
[lxiii] 'Privacy', *Community.jitsi.org*.
[lxiv] Autoriteit Persoonsgegevens, 'Keuzehulp privacy videobellen', *Autoriteitpersoonsgegevens.nl* versie 15 april 2020.
[lxv] V. van Amerongen, 'Gratis videobellen via internet', *Consumentenbond.nl* 8 april 2020.
[lxvi] Signal, *Signal.org.*
[lxvii] Nextcloud Talk, *Nextcloud.com.*
[lxviii] Autoriteit Persoonsgegevens, 'Keuzehulp privacy videobellen', *Autoriteitpersoonsgegevens.nl* versie 15 april 2020.
[lxix] V. van Amerongen, 'Gratis videobellen via internet', *Consumentenbond.nl* 8 april 2020.
[lxx] 'Security at Zoom', *Zoom.us.*
[lxxi] 'Privacy', *Wickr.com.*
[lxxii] Autoriteit Persoonsgegevens, 'Keuzehulp privacy videobellen', *Autoriteitpersoonsgegevens.nl* versie 15 april 2020.