Veelgestelde vragen over de DPIA van Zoom

Voor wie is de DPIA toespasbaar?
Iedere instelling moet zelf bepalen in hoeverre de resultaten toepasbaar zijn op de eigen organisatie. De opgeleverde DPIA's kunnen dus door iedereen worden gebruikt, ook door organisaties buiten onderwijs en onderzoek, maar moeten altijd worden geïnterpreteerd op de eigen situatie en omgeving.

Waarom is er een DPIA naar Zoom uitgevoerd?
Zoom is een applicatie die veel door de SURF leden wordt gebruikt. De licenties worden niet enkel, maar wel grotendeels in het wetenschappelijk onderwijs gebruikt. De leden hebben aan SURF gevraagd om te zorgen voor goede gebruikscondities voor deze dienst. Uit de DPIA die het Rijk had laten uitvoeren op Zoom (afgerond in mei 2021) bleek dat er 9 hoge risico's bestonden bij het gebruik van Zoom. Daaropvolgend is SURF met Zoom in gesprek gegaan en zijn er passende afspraken voor verbeteringen gemaakt.

Wat was de scope van de DPIA?
De Data Protection Impact Assessment (DPIA) onderzoekt de verwerking van data via de betaalde diensten van Zoom voor onderwijs en enterprise klanten op vijf platformen:

- Geïnstalleerd als app op Android- en iOS-devices;
- Geïnstalleerd als Zoom-client voor meetings op Windows 10 en macOS, en;
- Gebruik via de Zoom-plug-in voor de browser Chrome.

Aanvullend, deze DPIA analyseert het gebruik van de Microsoft Outlook-plug-in en het gebruik van cookies en vergelijkbare technologie op het publiek toegankelijke en de afgeschermde Zoom-website.

Wat zijn de uitkomsten van de DPIA?

- Zoom biedt end-to-end-encryption voor alle meetings, chats en uitgewisselde bestanden. Dit is de belangrijkste risico-mitigerende maatregel genoemd door de EDPB voor doorgifte van gegevens naar een land buiten de EU zonder adequaat gegevensbeschermingsniveau.
- Om ook de risico's voor de metadata te verlagen, heeft Zoom ingestemd om alle gegevensverwerkingen vanaf eind 2022 exclusief in de EU te verwerken door een Europese Cloud in te richten en support data exclusief in Europa te laten verwerken. Wanneer ondersteuning buiten werktijden noodzakelijk is, kan de gebruiker expliciet toestemming geven per ticket voor verwerking buiten de EER.
- Uitzondering is de beperkte doorgifte van pseudonieme persoonsgegevens naar het centrale Zoom Trust & Safety team in de VS. Hiervoor heeft Zoom beloofd om een veilige oplossing te implementeren: een beveiligde verbinding waarbij de gegevens in de EU blijven, of het inrichten van een Europees Trust en Safety team. Hiermee zal er vanaf eind 2022 geen structurele verwerking meer in de VS plaatsvinden, enkel nog incidentele verwerkingen die geoorloofd zijn.
  Er zijn nog wel vorderingen op grond van de US Cloud Act mogelijk, maar die kans is klein. Dit is vergelijkbaar met de huidige Amerikaanse providers die al diensten leveren vanuit de EU aan het onderwijs en aan de overheid (zoals Microsoft en Google). Hier blijkt uit de diverse risico analyses dat de kans op vorderingen verwaarloosbaar is voor gegevens van zakelijke klanten.

- Zoom heeft verklaard dat zij, op basis van historische data, de kans vrijwel nihil acht dat zij een vordering krijgt voor het verstrekken van metadata van het onderwijs of overheidsorganisaties aan de (Amerikaanse) overheid.
- Zoom heeft in een verbeterplan beloofd voor het einde van dit jaar alle mitigerende maatregelen op orde te hebben. SURF en Zoom hebben schriftelijk vastgelegd dat Zoom aan SURF tweemaandelijks rapporteert over de voortgang.
- Zoom treedt alleen nog op als verwerker voor alle persoonsgegevens, tenzij ze via de overeenkomst gemachtigd zijn om sommige persoonsgegevens 'verder' te verwerken als zelfstandige verantwoordelijke. Er zijn met SURF strikte doelbindingsafspraken gemaakt, zowel over de 'verwerkers' doelen, als over de 'verantwoordelijke' doelen.
- Zoom heeft de bewaartermijnen ingekort en de noodzaak uitgelegd.
- Zoom heeft grote vooruitgang geboekt in de transparantie over de verwerking van persoonsgegevens (met name in de meta-data).
- Zoom biedt vanaf eind 2022 een inzageportaal voor admins en gebruikers. Daarnaast wordt een verwijdermogelijkheid ontwikkeld voor individuele gebruiksgegevens.

Wanneer kunnen onderwijsinstellingen veilig gebruik maken van Zoom?
Wij zijn van mening dat Zoom veilig gebruikt kan worden. Iedere instelling moet deze afweging echter zelf maken en draagt hiervoor zelf de verantwoordelijkheid. Op basis van de informatie die uit de DPIA volgt kan iedere instelling deze afweging weloverwogen maken.

Wat moet ik zelf doen voordat mijn onderwijsinstelling Zoom kan gebruiken?
In de DPIA zijn maatregelen beschreven om de risico's te mitigeren. We hebben deze maatregelen met een stappenplan voor implementatie opgenomen in een cookbook voor admins, hosts en users.

Is het noodzakelijk dat ik alle technische handelingen uitvoer die in de handleiding zijn opgenomen?
Ja, alleen dan heb je Zoom zo privacyvriendelijk mogelijk ingesteld voor je gebruikers en zijn de rechten van betrokkenen het best gewaarborgd.

Kan ik de handleiding delen met mijn leverancier die onze omgeving beheert?
Ja, de handleiding is bedoeld om Zoom zo in te stellen dat de risico's zoveel mogelijk zijn gemitigeerd. Als je het beheer van de Zoom omgeving hebt uitbesteed dan zal degene die de controle over jouw omgeving heeft (de admin) de instellingen moeten toepassen.

Zijn de onderhandelingen nu klaar of gaan jullie nog verder in gesprek met Zoom?
Zoom heeft naast de maatregelen die zij al genomen heeft beloftes gedaan voor het nemen van verdere maatregelen. Eind 2022 zullen alle maatregelen zijn doorgevoerd. We blijven daarom met Zoom in gesprek om de voortgang te waarborgen.

Wat waren de belangrijkste problemen die er eerder waren bij het gebruik van Zoom?
- Zoom zag zichzelf niet als verwerker voor de persoonsgegevens van de education- en enterprise-klanten.
- Er miste transparantie over welke persoonsgegevens Zoom verwerkte.
- Betrokkenen konden hun rechten onvoldoende uitoefenen.
- Zoom verzamelde te veel gegevens.
- Zoom bewaarde gegevens te lang.

Hoe zijn die problemen nu opgelost?
Zie voor een uitgebreide beschrijving de uitkomsten van de DPIA.

Door tot op directieniveau in gesprek te gaan met Zoom heeft zij zich aan de afspraken gecommitteerd en zowel technische, organisatorische als juridische maatregelen genomen om de risico's te mitigeren, waaronder:

- er is een uitgebreide nieuwe verwerkersovereenkomst afgesloten;
- Zoom geeft inzicht in welke persoonsgegevens zij verwerken;
- Zoom heeft hun handmatige opvolging van data subject requests aangepast tot zij hier aan het einde van het jaar een tool voor hebben ontwikkeld, de data verzameling is geminimaliseerd en Zoom bewaart gegevens alleen nog zolang als nodig;
- om ook de risico's voor de metadata te verlagen heeft Zoom ingestemd om alle gegevensverwerkingen vanaf eind 2022 exclusief in de EU te verwerken door een Europese Cloud in te richten en support data exclusief door een Europese derde partij te laten verwerken. Wanneer service buiten werktijden noodzakelijk is zal de gebruiker expliciet toestemming moeten geven voor verwerking buiten de EER.

Een uitzondering hierop is de beperkte doorgifte van pseudonieme persoonsgegevens naar het centrale Zoom Trust & Safety team in de VS. Hiervoor heeft Zoom beloofd om een veilige oplossing te implementeren: een beveiligde verbinding waarbij deze gegevens in de EU blijven of het inrichten van een Europees Trust en Safety team. Hiermee zal er vanaf 2022 geen structurele verwerking meer in de VS plaatsvinden, slechts nog incidentele verwerkingen die geoorloofd zijn.

Waarom is deze DPIA over Zoom zo belangrijk voor Nederlandse onderzoeks- en onderwijsinstellingen?
Zoom is een veelgebruikte applicatie door onze leden. De licenties worden niet alleen, maar wel grotendeels in het wetenschappelijk onderwijs gebruikt. De leden vragen SURF daarom om te zorgen voor goede afspraken met leveranciers. Daarom is er, mede op verzoek van SURF, in 2020 een DPIA op Zoom uitgevoerd (afgerond in mei 2021). Hieruit bleek dat er negen hoge risico's waren bij het gebruik van Zoom. Daaropvolgend is SURF met Zoom in gesprek gegaan en zijn er passende afspraken gemaakt met Zoom voor het doorvoeren van verbeteringen.

Wat waren de belangrijkste knelpunten bij die gesprekken?
Het belangrijkste knelpunt bij dergelijke gesprekken is de impact op de techniek. Een partij als Zoom moet technische veranderingen doorvoeren in zijn software, en dat heeft een grote impact op resources. Daarom is het ook zo belangrijk dat iedereen (tot op directieniveau) betrokken is en achter de aanpassingen staat; alleen dan kunnen deze stappen worden gezet.

Waarom heeft het zo lang geduurd voordat er tot een oplossing is gekomen?
Het kost tijd om de belangen die spelen duidelijk te maken en alle mensen die nodig zijn om de maatregelen door te voeren bij elkaar te krijgen. Daarna is er nog veel overleg nodig over de te nemen maatregelen en hoe deze uitgevoerd worden. Het daadwerkelijk doorvoeren van de maatregelen kost daarna ook veel tijd.

Er wordt door een grote groep mensen bij zowel Zoom als SURF bijna fulltime aan gewerkt.

Heeft SURF nu een voorkeur voor Zoom voor videoconferencing?
De geschiktheid van een tool hangt helemaal af van het gebruik en de doelen die een organisatie heeft. Er is daardoor geen sprake van een bepaalde voorkeur voor een bepaalde tool, maar bij gebruik moet gekeken worden naar welke tool passend is.

SURF neemt hier geen positie over in. Wij maken in opdracht van de leden afspraken met leveranciers. Zoom is nu een van de geschikte partijen voor videoconferencing als het privacy en security betreft.

Hoe kan het dat sommige van de afspraken die SURF heeft gemaakt nu gelden voor heel Europa?
SURF heeft onderhandeld namens de gehele onderwijssector en de overheid. Veel van de maatregelen die Zoom neemt zijn dusdanig generiek van aard dat het voor Zoom loont om deze voor heel Europa door te voeren. Ook heeft Zoom in gezien dat zij met het nemen van privacy maatregelen een veel betere positie kan krijgen in de Europese markt. Daardoor was Zoom bereid om de vele maatregelen die ze nemen niet alleen voor SURF door te voeren maar voor heel Europa.

Hoe staat deze DPIA in relatie met de op Microsoft Teams uitgevoerde DPIA?
Beide DPIA's zijn een op zichzelf staand traject. Op beide dossiers is samengewerkt door SLM Rijk en SURF. In de uitvoering van DPIA's volgen wij standaard procedures en de geldende wet- en regelgeving. Er is geen relatie tussen beide DPIA's, omdat het om 2 verschillende applicaties gaat.