



BADAN SIBER DAN SANDI NEGARA

Jalan Harsono R.M. No.70, Ragunan, Jakarta 12550
Telepon (021) 7805814, Faksimile (021) 78844104,
Website: <http://www.bssn.go.id>, E-mail: humas@bssn.go.id

TELAAH STAF TERKAIT PEMANFAATAN APLIKASI ZOOM SEBAGAI MEDIA ONLINE MEETING YANG BANYAK DIGUNAKAN SAAT INI

A. LATAR BELAKANG

Munculnya pandemi corona virus Covid-19 menyebabkan penyesuaian kegiatan yang cukup signifikan di berbagai sektor dan bidang pekerjaan. Salah satu kebijakan pemerintah untuk menekan jumlah penyebaran virus corona adalah himbauan agar tidak keluar dari rumah dan para pekerja termasuk ASN diminta untuk bekerja dari rumah atau biasa disebut *work from home* (WFH). Agar pekerjaan yang bersifat multi personil seperti rapat-rapat internal maupun eksternal tetap dapat dilaksanakan, sebuah organisasi membutuhkan pemanfaatan teknologi *online meeting*. Teknologi ini memungkinkan rapat-rapat yang biasa dilakukan secara tatap muka langsung dapat dilakukan dari mana saja dan kapan saja. Fitur utama yang diharapkan dari sebuah teknologi *online meeting* secara umum adalah *video & voice conference*, *text messaging*, *direct share file*, serta *shared screen* antar pengguna. Aplikasi-aplikasi seperti *Zoom*, *Google Hangouts*, *Skype*, dan aplikasi *online meeting* lain mendadak menjadi sangat digemari sejak adanya himbauan WFH ini.

Salah satu aplikasi yang paling banyak digunakan saat ini untuk memfasilitasi WFH di Indonesia bahkan dunia adalah Zoom. Zoom merupakan aplikasi yang sangat diminati karena sangat *reliable*, mudah digunakan, dengan fitur *video & audio conference*, *collaboration*, *chat*, *webinar*, *shared screen*, *shared file* dengan konsep *room system* dan dapat diakses dari desktop maupun smartphone (Zoom Video Communications, Inc., 2020). Zoom tercatat sebagai *leader application* kategori *meeting solution* pada *Gartner 2019 Magic Quadrant* (Zoom Video Communications, Inc, 2019). Zoom mengakui adanya lonjakan jumlah pengguna sejak adanya fenomena pandemi Covid-19 dan WFH di seluruh dunia (Clifford, 2020). Tercatat jumlah pengguna aktif Zoom pada Februari 2020 mencapai 81.900 dan terus meningkat sampai sekarang (Smith, 2020). Statistik peningkatan permintaan ini dapat dilihat pula Zoom android yang sudah diunduh lebih dari

sembilan puluh ribu kali sampai bulan Maret 2020 (Google, n.d.). Zoom menawarkan layanan versi berbayar dan gratis. Untuk versi gratis Zoom memberikan kuota satu kali meeting selama 40 menit dengan jumlah peserta meeting sampai dengan 100 partisipan. Selain itu Zoom juga menawarkan fitur pengamanan berupa SSL/TLS encryption untuk jaminan keamanan dan privacy melalui jaringan internet, serta *end to end encryption* dengan algoritma AES 256 untuk mengamankan konten pada layer aplikasi. Tentu hal ini menjadi daya tarik bagi pengguna yang melaksanakan WFH dan saat ini sedang sangat membutuhkan aplikasi *multi-purpose* seperti Zoom.

Pada akhir bulan Maret 2020 muncul isu terkait keamanan dari Zoom terhadap data dan privasi penggunanya. BBC News memberitakan bahwa Zoom tidak benar-benar menerapkan *end to end encryption* seperti yang dipromosikan. Disampaikan bahwa Zoom mengumpulkan data pengguna untuk analisis layanan sekaligus memanfaatkannya untuk keperluan bisnis. Isu *privacy* yang menjadi perhatian adalah monitoring aktivitas partisipan meeting oleh *host meeting* sendiri, serta Administrator layana Zoom yang dapat melihat detail aktivitas pengguna termasuk hasil *record meeting*, sistem operasi, alamat IP, data lokasi dan informasi perangkat yang digunakan oleh pengguna. Media online lain dari Eropa KSTP (Jokich, 2020), juga turut memberitakan bahwa FBI memperingatkan para pengguna Zoom terkait adanya laporan-laporan “*zoom-bombing*”. *Zoom-bombing* merupakan istilah yang muncul karena ada banyaknya laporan dari pengguna Zoom yang merasa terganggu saat *online meeting* dilaksanakan. Hal ini terjadi karena masuknya partisipan *online meeting* yang tidak diundang atau tidak berkepentingan lalu mengganggu jalannya *meeting* dengan berbagai cara seperti berteriak tiba-tiba, menampilkan tayangan berbau pornografi dan SARA, sampai ke ancaman-ancaman bahkan ujaran kebencian (Wakefield, 2020).

Seiring maraknya penggunaan aplikasi Zoom di tengah pandemi Covid-19 dan fenomena WFH, isu *security* dan *privacy* pengguna menjadi perhatian bagi para pemerhati keamanan informasi di seluruh dunia. Kredibilitas Zoom sebagai sebuah perusahaan penyedia layanan *online meeting* dipertanyakan. Zoom memiliki *policy* tersendiri yang seharusnya menerapkan *privacy practice* yang selaras dengan berbagai peraturan *personal data protection* yang ada di dunia seperti EU GDPR. *Policy* pemanfaatan data yang diterapkan oleh Zoom pastinya sudah diketahui dan disampaikan kepada para penggunanya dengan persetujuan *acceptance agreement* saat melakukan instalasi. Tetapi mungkin banyak orang

yang tidak memperhatikan *license agreement* tersebut saat mulai menginstall Zoom.

B. Analisis Fitur Security Zoom

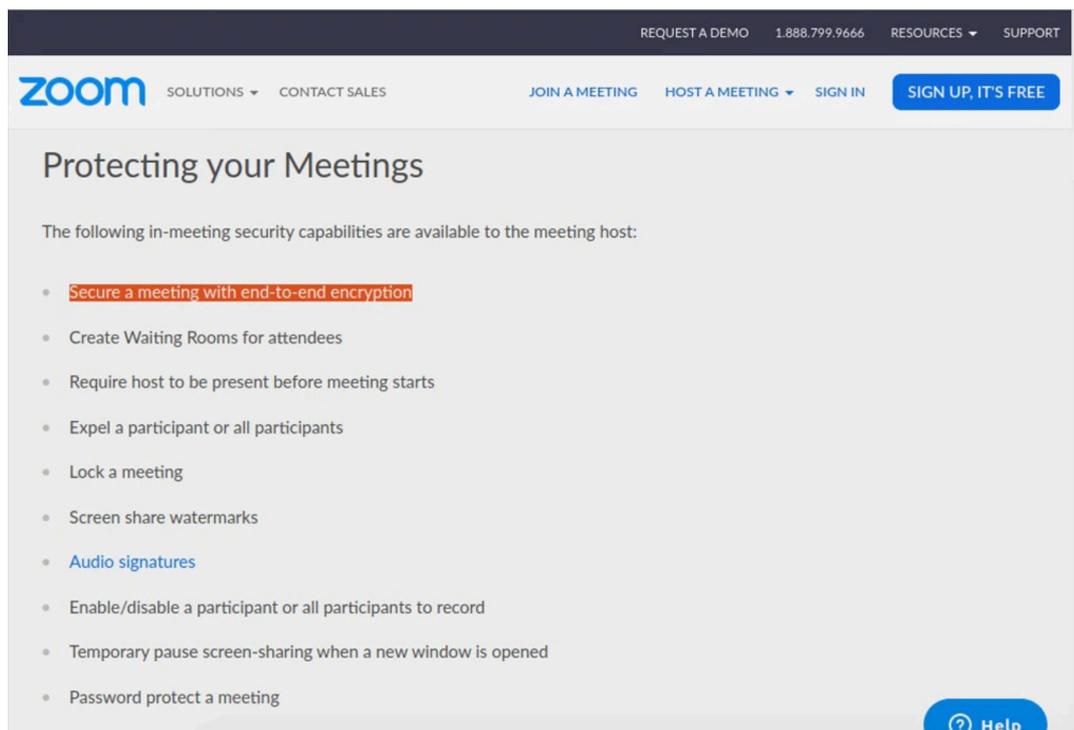
Layanan komunikasi yang diklaim oleh Zoom adalah “*end to end encryption*”. Tetapi Micah Lee dan Yael Grauer menuliskan dalam sebuah *First Look Media* (Lee & Grauer, 2020), Zoom memiliki pendefinisian tersendiri terhadap konsep “*end to end encryption*”. Implementasi nyata “*end to end encryption*” yang diakui oleh pengguna komunikasi internet adalah komunikasi yang private dan terlindungi, serta menjunjung tinggi privasi pengguna dari pihak lain yang tidak berkepentingan. Istilah “*end to end encryption*” yang digunakan oleh Zoom dianggap sebagai sebuah bahasa marketing untuk meningkatkan penjualan.



Gambar 1 Informasi Pengaktifan “*End to End Encryption*” pada Zoom Meeting

Zoom *white paper* (Zoom Video Communications, Inc., 2019) mensyaratkan “*pre-meeting security capabilities*” yang harus dipenuhi untuk membuat sebuah *online meeting* dalam kondisi “*end to end encrypted meeting*”. Host yang membuat *meeting room* harus meng-*enable* kan terlebih dahulu pengaturan “*Require Encryption for 3rd Party Endpoints*” sebelum *meeting* dimulai. Apabila pengaturan tersebut sudah dilakukan maka seluruh partisipan akan dapat mengidentifikasinya melalui *icon* gembok yang berwarna hijau dan bertuliskan “*Zoom is using an end to end encrypted connection*”. Hal tersebut telah diklarifikasi kepada pihak Zoom dan diketahui “*end to end encryption*” tidak berlaku untuk *video meeting*. Fitur

Zoom *video meeting* menggunakan kombinasi TCP dan UDP. Koneksi TCP dibentuk melalui TLS connection antara web browser dengan Zoom server, kemudian koneksi UDP dienkripsi dengan AES 128 yang memanfaatkan kunci hasil *key negotiation* pada koneksi TLS. Dalam Komunikasi VoIP biasa disebut sebagai “*media encryption*” atau portokol *Secure Real-time Transport Protocol* (SRTP). Dari skema tersebut dapat dilihat bahwa enkripsi yang digunakan oleh Zoom *video meeting* adalah koneksi TLS. Koneksi TLS secara umum banyak dijumpai seperti halnya komunikasi HTTPs pada sebuah websites atau biasa disebut “*transport encryption*”. Komunikasi TLS ini berbeda dengan konsep “*end to end encryption*” yang seharusnya, yaitu enkripsi antar *end user*. Penerapan koneksi TLS antara client dan server masih memungkinkan penyedia layanan membuka konten yang dilewatkan melalui server. Jadi pemanfaatan *video meeting* melalui Zoom dapat dikatakan aman dari percobaan intersepsi di tengah jaringan, tetapi tidak dapat menjamin kerahasiaan data pengguna ketika konten *meeting* melalui server Zoom. Zoom selaku penyedia layanan dapat secara bebas melakukan pembacaan data yang melewati server mereka.



Gambar 2 Informasi Fitur End to End Encryption Zoom pada Website

Apabila Zoom benar-benar menerapkan konsep “*end to end encryption*”, seharusnya Zoom selaku penyedia tidak dapat membuka konten yang ditransmisikan melalui servernya tanpa sebuah kunci. Konten yang ditransmisikan hanya dapat dibuka oleh partisipan yang saling berbagi kunci satu sama lain dalam

sebuah *online meeting*. Kemudian melalui Zoom *white paper* tersebut, diketahui konsep “*end to end encryption*” secara nyata hanya diterapkan pada fitur *meeting text chat*. Paper tersebut menyebutkan bahwa hanya pengirim dan penerima message yang berhak saja yang dapat membaca pesan yang ditransmisikan. Untuk enkripsi *text chat* ini, Zoom mengimplementasikan *hybrid cryptosystem* yaitu gabungan antara kriptografi asimetrik dan simetrik. Sistem asimetrik kunci public dan private dimanfaatkan untuk mengamankan *session key* dari sistem kriptografi simetrik AES-256. *Session key* ini dibangkitkan dari parameter hardware UID pengguna dan disimpan dalam penyimpanan local pada perangkat pengguna, sehingga Zoom sendiri tidak dapat melakukan dekripsi data *text chat* yang ditransmisikan karena tidak memiliki *session key* tersebut.

Hasil analisis yang dilakukan terhadap permasalahan *Zoom-Bombing* adalah karena kurang *aware*-nya pengguna terhadap konfigurasi *room meeting* yang dibuat. Sebuah *room meeting* dapat dibuat dengan beberapa mode pengamanan seperti diproteksi dengan password, *lock-meeting*, dan perijinan khusus untuk pengguna. Setelah *room-meeting* dibuat, Zoom akan membuat sebuah URL atau *invitation link* yang di dalamnya dapat mengandung password untuk mempermudah partisipan lain masuk ke dalam *room-meeting*. *Invitation link* ini biasanya didistribusikan melalui berbagai media, termasuk media social. *Invitation link* yang tidak termaintain dengan baik dan didistribusikan secara sembarangan melalui berbagai media ini yang biasanya dimanfaatkan oleh pihak yang tidak berkepentingan untuk ikut masuk ke dalam sebuah *meeting-room*. Setelah pihak yang tidak berkepentingan tersebut berhasil masuk ke dalam *meeting-room* yang ditemukan, kemudian *zoom-bombing* biasanya akan terjadi. Untuk meminimalisir adanya *zoom-bombing*, host dari *meeting room* dapat lebih *aware* terhadap konfigurasi *meeting* yang dibuat. Selain itu seluruh partisipan juga harus lebih berhati-hati dalam mendistribusikan URL *invitation meeting* yang ditujukan kepada dirinya.

C. Benturan Kepentingan Bisnis dan Klaim Kepentingan Perolehan Data Pengguna Zoom

Dari berbagai sumber disebutkan bahwa Zoom bisa jadi sudah menyalahi aturan dengan menyampaikan informasi yang tidak sebenarnya terkait fitur “*end to end encryption*”. Zoom dinilai dapat merugikan pengguna yang sudah dijanjikan fitur keamanan sedemikian rupa tetapi kenyataannya tidak terimplementasi dengan

benar. Zoom juga dinilai dapat merugikan penyedia layanan serupa lainnya, karena membuat pelanggan beralih ke Zoom dengan cara yang dianggap tidak jujur. Dari sisi kepentingan bisnis Zoom akan banyak berbenturan dengan aturan *Federal Trade Commission* (FTC) untuk perdagangan global (Lee & Grauer, 2020). Salah satu asosiasi yang sudah mengangkat isu tentang ketidaksesuaian fitur security Zoom adalah AccesNow. AccesNow meminta Zoom untuk membuat dan mempublikasikan laporan *Transparency Report* seperti halnya dilakukan oleh penyedia lain (Accessnow.org, 2019). *Transparency Report* dapat menjadi pedoman bagi para pengguna untuk memperlihatkan akuntabilitas sebuah perusahaan penyedia komunikasi melindungi dan mempergunakan data para penggunanya.

Zoom yang tidak terbuka menimbulkan berbagai macam persepsi publik terkait pemanfaatan data pengguna yang dikumpulkan. Digunakan untuk apa dan siapa saja pemanfaatnya. Berbagai persepsi tersebut muncul karena Zoom saat ini sangat banyak digunakan oleh berbagai perusahaan, organisasi, dan pemerintah negara hampir di seluruh dunia. Tentu saja data yang dikumpulkan menjadi sangat berharga, apalagi jika data tersebut sampai disalahgunakan oleh Zoom selaku penyedia layanan.

Zoom melalui *privacy policy* (Zoom Video Communications, Inc., 2020) yang diupdate pada tanggal 29 Maret 2020 menyampaikan beberapa poin untuk mengklarifikasi isu yang ada. Poin-poin tersebut antara lain:

1. Zoom tidak menjual data personal penggunanya.
2. Zoom tidak melakukan monitoring terhadap meeting-meeting yang dilakukan penggunanya, termasuk hasil *record meeting* yang tersimpan.
3. Record meeting yang tersimpan di dalam layanan cloud Zoom hanya sebuah opsi apabila pengguna membutuhkan. Zoom memberikan jaminan perlindungan terhadap unauthorised access dari file yang tersimpan di cloud Zoom.
4. Pengumpulan data pengguna oleh Zoom hanya digunakan untuk kepentingan layanan Zoom. Data-data yang dikumpulkan termasuk alamat IP, informasi OS dan device digunakan untuk kepentingan *improvent* layanan dan *user experience* aplikasi Zoom.
5. Zoom tidak mempergunakan data yang dikumpulkan untuk kepentingan advertising.

6. Zoom berkomitmen untuk melindungi data privacy pengguna dan tidak bertentangan dengan regulasi yang ada di dunia seperti COPPA, FEPR, CCPA, dan regulasi lainnya.

Jenis-jenis data pengguna secara detail yang dikumpulkan oleh Zoom sesuai Privacy Policy yang dibuat dan diberitahukan ke publik ada pada Lampiran A, B, C, dan D.

D. Kesimpulan dan Saran

Kesimpulan yang dapat diambil adalah sebagai berikut:

- 1) Aplikasi Zoom tidak 100% menerapkan “*End to End Encryption*” untuk layanan yang mereka berikan. “*End to End Encryption*” hanya diterapkan pada fitur *meeting text chat* memanfaatkan Hybrid Crypto System. Sedangkan pengamanan fitur *video meeting* dilakukan menggunakan TLS Connection dan *Secure Real-time Transport Protocol (SRTP)*. TLS Connection banyak diimplementasikan pada komunikasi client server seperti HTTPs dan dianggap bukan merupakan user “*End to End Encryption*” karena penyedia layanan masih dapat melakukan pembacaan data di sisi server.
- 2) Fitur Zoom untuk “*End to End Encryption*” menjadi perdebatan saat ini karena dapat merugikan pengguna dan penyedia layanan *online meeting* serupa lainnya. Zoom dianggap telah memberikan informasi yang tidak sesuai dengan implementasinya untuk menarik pelanggan.
- 3) Zoom telah memberikan klarifikasi resmi terkait jenis-jenis data pengguna yang dikumpulkan dan pemanfaatannya untuk kepentingan internal Zoom dan tidak dipublikasikan atau diperjualbelikan.

Saran yang dapat diberikan apabila pengguna terutama instansi-instansi pemerintah Indonesia masih berniat menggunakan aplikasi Zoom, maka hal-hal berikut dapat menjadi perhatian untuk diterapkan.

- 1) Tidak menggunakan aplikasi Zoom pada *meeting-meeting* yang bersifat rahasia, karena “*End to End Encryption*” tidak berlaku pada fitur *video meeting* Zoom dan pihak Zoom masih dapat melakukan pembacaan data *video* dan *audio* yang melewati server.
- 2) Pengguna yang berperan sebagai Host yang membuat sebuah *meeting room* harus meng-*enable* terlebih dahulu pengaturan “*Require Encryption for 3rd Party Endpoints*” sebelum *meeting* dimulai.

- 3) Pengguna yang berperan sebagai Host juga dapat meningkatkan keamanan *online meeting* dari ancaman *Zoom-bombing* dengan mengaktifkan proteksi *password room meeting*, *locked-meeting*, dan perijinan khusus partisipan rapat melalui email. Fitur-fitur keamanan tersebut sudah ada pada Zoom tetapi secara default tidak diaktifkan.
- 4) Pengguna yang berperan sebagai partisipan sebuah *online meeting* dapat lebih *aware* terhadap URL *invitation link* yang diberikan oleh *host meeting*. *Invitation link* ini dapat mudah didistribusikan melalui media sosial dan dapat dimanfaatkan oleh pihak yang tidak berkepentingan untuk melakukan *zoom-bombing*.

E. Penutup

Demikian dokumen ini dibuat sebagai bahan pertimbangan pimpinan dalam menentukan kebijakan lebih lanjut.

Jakarta, April 2020

Mengetahui,
Kapuskajibang Tekkamsisan

Penulis

Dra. Retno Artinah S.

Ariq Bani Hardi

F. Referensi

- Smith, C. (2020, March 25). *DMR Bussiness Statistics*. Retrieved from Interesting Zoom Statistics and Facts 2020: <https://expandeddrablings.com/index.php/zoom-statistics-facts/>
- Google. (n.d.). *Zoom Cloud Meetings*. Retrieved from Google Play: <https://play.google.com/store/apps/details?id=us.zoom.videomeetings>
- Zoom Video Communications, Inc. (2020). *Zoom*. Retrieved from Zoom Solution: <https://zoom.us/>
- Zoom Video Communications, Inc. (2019). *Zoom : A Leader in the 2019 Gartner Magic Quadrant for Meeting Solutions*. Retrieved from Zoom : A Leader in Gartner Magic Quadrant: <https://zoom.us/gartner>
- Wakefield, J. (2020, March 27). *Coronavirus: Zoom is in everyone's living room - how safe is it?* Retrieved from Coronavirus: Zoom is in everyone's living room - how safe is it? - BBC News: <https://www.bbc.com/news/technology-52033217>
- Jokich, A. (2020, March 31). *FBI warning the public about 'Zoom-bombing' of video chats*. Retrieved from FBI warning the public about 'Zoom-bombing' of video chats | KSTP.com: <https://kstp.com/news/fbi-warning-the-public-about-zoom-bombing-of-video-chats-/5688940/>
- Lee, M., & Grauer, Y. (2020, March 31). *ZOOM MEETINGS AREN'T END-TO-END ENCRYPTED, DESPITE MISLEADING MARKETING*. Retrieved from Zoom Meeting don't Support End to End Encryption: <https://theintercept.com/2020/03/31/zoom-meeting-encryption/>
- Accessnow.org. (2019, October). *TRANSPARENCY REPORTING INDEX*. Retrieved from TRANSPARENCY REPORTING INDEX - AccessNow: <https://www.accessnow.org/transparency-reporting-index/>
- Zoom Video Communications, Inc. (2020, March 29). *Privacy Policy - Zoom*. Retrieved from Privacy Policy: <https://zoom.us/privacy>
- Zoom Video Communications, Inc. (2019, June). *Zoom Security Guide*. Retrieved from Security Guide - Zoom: <https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf>
- Clifford, T. (2020, February 2). *Coronavirus outbreak increases demand for Zoom Video remote work tools, says CEO*. Retrieved from cbnc news: <https://www.cnbc.com/2020/02/03/zoom-video-is-seeing-record-usage-amid-coronavirus-fears-ceo-says.html>

Lampiran A Data yang Diberikan Pengguna kepada Zoom

| Type of Data | Examples | Zoom Uses it to |
|---|---|--|
| Information that identifies you | <p>For customers: Account owner name, billing name and address, payment method</p> <p>Your name, username and email address, or phone number, when you use this information to access or use our services</p> <p>The phone number a Zoom Phone user dials</p> | <p>Create a customer account</p> <p>Provide Zoom services</p> <p>Communicate with a customer</p> <p>Respond to requests for support</p> |
| Other account data | Your phone number (if you choose to put it in), language preference, password (if SSO is not used), title, department | <p>Create a customer account</p> <p>Provide Zoom services</p> |
| Customer content: information you or others upload, provide, or create while using Zoom | Cloud recordings, chat / instant messages, files, whiteboards, and other information shared while using the service, voice mails | <p>Provide Zoom services*</p> <p>Store chat logs (for delivery and so you can review and search chat history)</p> <p>Store recordings, if explicitly requested by the host or Customer</p> |

| | | |
|--|--|---------------------------------|
| | | Store voice mail for Zoom Phone |
|--|--|---------------------------------|

Lampiran B Data yang Dikumpulkan oleh Sistem Zoom dari Pengguna

| Type of Data | Examples | Zoom Uses it to |
|---|---|--|
| <p>Technical information about your devices, network, and internet connection</p> | <p>IP address, MAC address, other device ID (UDID), device type, operating system type and version, client version, type of camera, microphone or speakers, connection type, etc.</p> <p>The phone number of a person making a call using Zoom services (e.g. Zoom Phone)</p> | <p>Connect you to and optimize your experience using our services</p> <p>Provide customers dashboards and reports</p> <p>Respond to requests for support</p> <p>Monitor performance of our data centers and networks</p> <p>Conduct anonymized, aggregated analytics to improve Zoom’s service performance</p> |

| | | |
|---|--|--|
| <p>Approximate Location</p> | <p>To the nearest city (we do not “track” your specific location)</p> | <p>Connect you to the nearest data center</p> <p>Comply with privacy and other laws – for example, so we can provide you with the right notices for your area</p> <p>Suggest choices such as language preferences</p> <p>Monitor performance of our data centers and networks</p> <p>Respond to requests for support</p> |
| <p>Information about how you use Zoom (this is NOT information or content you share in your meetings or in chats)</p> | <p>Did you use VoIP or a phone call?</p> <p>Did you shift from the mobile client to the desktop?</p> | <p>Optimize your Zoom experience</p> <p>Respond to requests for support</p> <p>Conduct anonymized, aggregated analytics to improve Zoom’s performance.</p> |
| <p>Setting and preferences chosen by the user</p> | <p>Join with video off</p> | <p>To provide you choices for how you use Zoom</p> |

| | | |
|-----------------|--|---|
| | <p>Require meeting password</p> <p>Enable waiting room</p> <p>Do not allow screen sharing other than host</p> | |
| <p>Metadata</p> | <p>Duration of the meeting / Zoom Phone call</p> <p>Email address, name, or other information that a participant enters to identify themselves in the meeting</p> <p>Join and leave time of participants</p> <p>Name of the meeting</p> <p>Date / time that meeting was scheduled</p> <p>Chat status (unless a setting is actively chosen by user)</p> <p>Call data records for Zoom Phone</p> | <p>Provide Zoom services</p> <p>Provide customers dashboards and reports</p> <p>Respond to requests for support</p> |

Lampiran C Data yang Menjadi Pilihan Pengguna untuk Diberikan/Tidak Diberikan kepada Zoom

| Type of Data | Examples | Zoom Uses it to |
|---------------------------------|---|--|
| Information that identifies you | Your name, username, physical address, email address, phone number | Create an account when you sign up Respond to requests from you Send you marketing communications, unless you tell us not to (or if you say it's OK, i.e., opt-in) |
| Information about your job | Company, title, department | Provide tailored information Respond to requests from you |
| Payment information | Credit/debit card (goes directly to our payment processor; credit card information is not accessed or stored by Zoom) | Charge you when you sign up for a paid plan |

Lampiran D Data Lain yang Dapat Diambil oleh Zoom tentang Pengguna

| Type of Data | Examples | Zoom Uses it to |
|--|---|---|
| Data collected through the use of cookies and pixels | Data collected from tools such as Google Analytics and Google Ads | Analyze how our website is used so we can improve your experience |

| | | |
|----------------------|--|--|
| | <p>(All cookies are visible in the Cookie Preferences tool. You have control over what non-essential cookies you accept. For more information, see our Cookie Policy and the Cookie section below)</p> | <p>Allow you to do things like completing orders, sharing pages, and remembering settings.</p> <p>Evaluate the success of our Marketing campaigns</p> <p>Send you tailored Zoom advertising when you are on other sites.</p> <p>(For more information on how Zoom uses cookies, see our Cookie Policy)</p> |
| <p>Third Parties</p> | <p>Data Enrichment services</p> <p>Mailing Lists</p> <p>Public Sources</p> | <p>Send you marketing communications, unless you tell us not to (or if you say it's OK, i.e., opt-in)</p> <p>Provide tailored information based on your interests</p> |