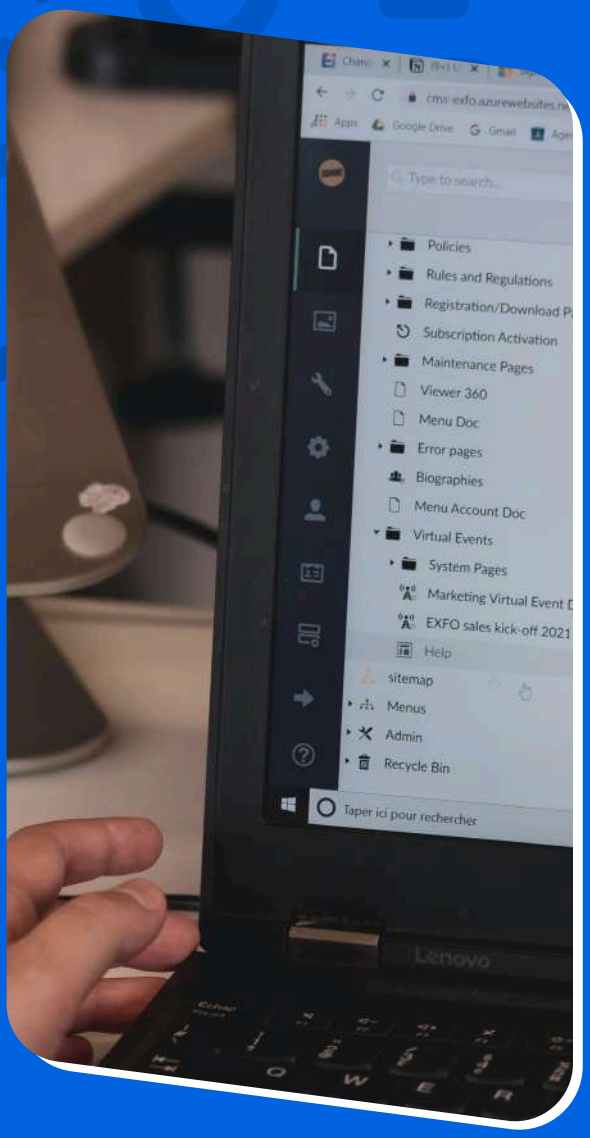
CfDS
CENTER FOR DIGITAL SOCIETY
UNIVERSITAS
GADJAH MADA



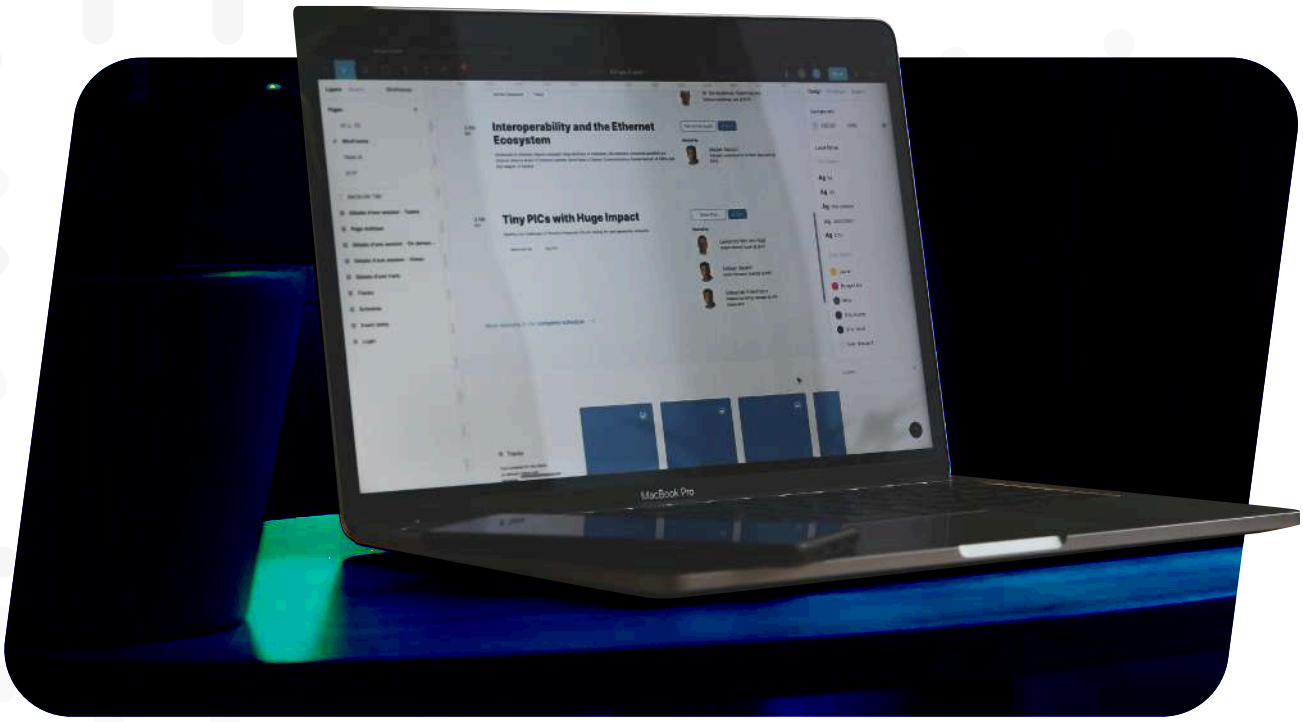
Tantangan Implementasi dan Penguatan Kerjasama Lintas Sektor Pelindungan Data Pribadi

Penulis

Dewa Ayu Diah Angendari
Sri Handayani Nasution

Desain dan Tata Letak

M. Fattah Fachrial Al Fayyadi



PENGANTAR

Sebagai negara dengan dengan pertumbuhan sektor ekonomi digital tercepat di Asia Tenggara (World Bank, 2021), sektor digital Indonesia masih jauh dari kata aman. Selama pandemi saja setidaknya terdapat enam kasus kebocoran data yang krusial, baik dari sektor privat maupun sektor publik atau pemerintah, termasuk di dalamnya adalah kasus kebocoran data BPJS Kesehatan (Akbar, 2021). Lansekap keamanan siber di Indonesia juga serupa. Laporan Microsoft (2020) menyebutkan Indonesia sebagai negara dengan tingkat ancaman malware tertinggi di Asia Pasifik. Laporan Indeks Ancaman Siber *(Cyber Risk Index)* oleh TrendMicro (Chandra, 2021) mengklasifikasikan Indonesia sebagai negara dengan peningkatan ancaman *(elevated risk).*

Berbagai tantangan tersebut serta didorong dengan pertumbuhan pengguna internet di Indonesia tentunya menuntut adanya intervensi dari para aktor terkait. Salah satunya adalah keberadaan regulasi mengenai pelindungan data pribadi yang dapat menjadi langkah krusial untuk meningkatkan kondisi perlindungan data di Indonesia. Saat ini, Indonesia memiliki 30 peraturan sektoral terkait pelindungan data pribadi (Kominfo, n.d.; Riyadi, 2021). Peraturan yang tersebar ini menjadi hambatan dalam implementasi karena diperlukannya sinkronisasi dalam hal definisi dan tata kelola antar sektor.

Menangani hal ini, pemerintah melalui Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo) telah membuat formulasi draft Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP). Sejak tahun 2020, diskusi mengenai RUU PDP sudah dilaksanakan di level legislatif. Sayangnya, pengesahan RUU PDP ini masih terhalang oleh beberapa hal, seperti aspek kompleksitas implementasi bagi badan pub lik maupun badan usaha, kesiapan sumber daya manusia, isu keamanan siber, hingga keberadaan independensi Otoritas Pelindungan Data (ODP) di Indonesia.

Melihat urgensi ini, Center for Digital Society (CfDS) sebelumnya telah mengeluarkan sebuah *commentaries* yang merangkum rekomendasi pertimbangan RUU PDP dari kacamata hak asasi manusia dan ekonomi digital.[1] Poin utama yang kami angkat adalah:

- Pentingnya penerapan prinsip extra protection terhadap hak kelompok rentan dan minoritas.
- Peninjauan atas sanksi dan ganti rugi dalam RUU PDP.
- Keberadaan badan otoritas pelindungan data pribadi.
- Kebutuhan akan edukasi masyarakat yang berkelanjutan.

[1] Putri, T.E. & Karim, P. (2021). Pelindungan Data Pribadi dan Hak Masyarakat di Ranah Digital. *Commentaries.* Center for Digital Society.

Selain diperlukannya pertimbangan dan diskusi atas beberapa substansi terkait RUU PDP, CfDS juga melihat pentingnya antisipasi atas implementasi RUU PDP dan kerjasama lintas sektor sebagai penguatan pelindungan data pribadi di Indonesia. Untuk itu, CfDS berkolaborasi dengan Meta, mengadakan 2 (dua) rangkaian diskusi terbuka yang diselenggarakan pada tanggal 11 dan 18 November 2021. Kedua diskusi ini masing-masing menyoroti tantangan implementasi jika nantinya RUU PDP disahkan dan peran masing-masing sektor terkait dalam pelindungan data pribadi pengguna internet di Indonesia. Sama seperti rangkaian diskusi sebelumnya, CfDS kembali mengundang perwakilan dari Kementerian Komunikasi dan Informatika Republik Indonesia, Komisi I DPR RI, platform media sosial, akademisi, maupun praktisi.

Dari kedua diskusi tersebut, CfDS mengangkat beberapa usulan, yakni:

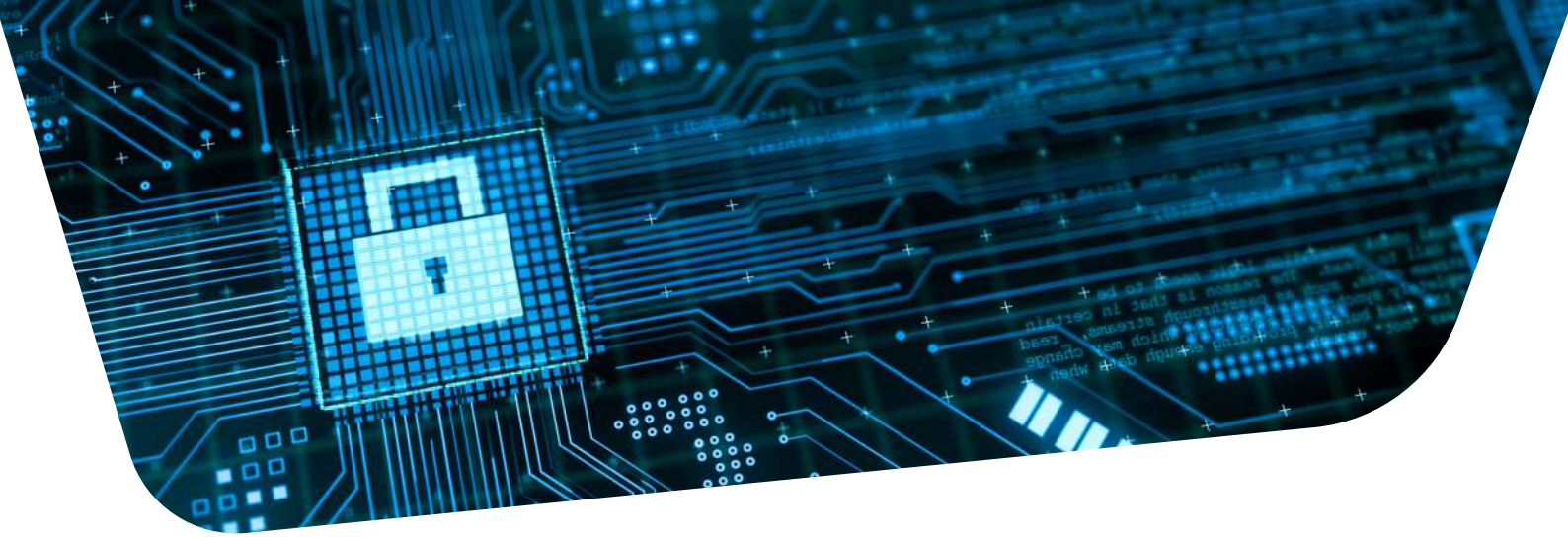
1. Peninjauan kemungkinan penerapan RUU PDP oleh badan publik dan badan usaha.
2. Keterkaitan RUU PDP dengan isu keamanan siber.
3. Perbandingan keberadaan badan otoritas pelindungan data pribadi.
4. Peran sektor terkait dalam pelindungan data.

Usulan Rekomendasi

01 Penerapan oleh Badan Publik dan Badan Usaha

Sebagai sebuah regulasi payung yang bertujuan mengharmonisasikan berbagai regulasi sektoral yang telah ada sebelumnya, penting untuk memastikan bahwa RUU ini nantinya dapat diimplementasikan oleh badan publik maupun privat yang menjadi subjek dari peraturan tersebut. RUU PDP perlu mempertimbangkan variasi kemampuan dan tingkat adaptasi berbagai badan usaha yang beroperasi di Indonesia, terutama badan usaha dengan skala kecil dan menengah. Perumusan kebijakan tidak hanya melihat *"how things should be"* melainkan juga mengenai *"what should we do"* (Goodin, R.E., et.al., 2011).

Dalam konteks RUU PDP, regulator perlu mempertimbangkan kemampuan sumber daya yang dimiliki oleh pihak yang akan diatur dalam RUU tersebut. Sebagai contoh, pelaku industri level domestik dengan skala kecil dan menengah dalam bentuk perorangan tentu memiliki kemampuan teknis, keuangan, dan sumber daya yang berbeda dengan organisasi multinasional. RUU PDP diharapkan dapat menjadi motor akselerasi ekonomi digital Indonesia dan bukan sebaliknya. Oleh karena itu, RUU PDP perlu melakukan pendefinisian skala usaha dan tahapan adopsi beban kewajiban yang dapat dievaluasi secara berkala.



02 Keterkaitan dengan Keamanan Siber

Di bawah peraturan mengenai perlindungan data pribadi, kehadiran *Data Protection Officer (DPO)* adalah hal yang wajib. Beberapa negara terdekat yang dapat menjadi acuan dalam pengaturan DPO adalah Filipina dan Thailand. Keduanya memiliki peraturan perlindungan data pribadi yang terkonsolidasi dan memuat elemen-elemen *European Union General Data Protection Regulations* atau EU GDPR (ABLI, 2020). Thailand malah disebut sebagai satu-satunya negara di Asia yang secara eksplisit 'berbasis GDPR' (Privacy Laws & Business, 2019). Di bawah ketiga peraturan ini, penunjukan DPO adalah hal yang wajib diselenggarakan oleh organisasi, baik swasta maupun publik.

Berdasarkan GDPR dan peraturan di Thailand, beberapa tugas dan aspek yang harus dipenuhi DPO adalah menginformasikan, melakukan fungsi sebagai penasehat, melakukan pengamatan mengenai kepatuhan organisasi terhadap peraturan yang berlaku, dan sebagai kontak rujukan baik oleh *data controller* atau *data processor* (Data Guidance, 2020). Lebih lanjut lagi, peraturan di Filipina secara eksplisit menekankan bahwa DPO harus memiliki pemahaman mendalam mengenai operasionalisasi peraturan undang-undang yang berlaku dan juga GDPR, dan memiliki kemampuan dan pemahaman mengenai teknologi.

RUU PDP juga mewajibkan keberadaan DPO dalam organisasi pengelola dan pemroses data. Keberadaan DPO akan menimbulkan permintaan pasar atas kemampuan teknis yang berkaitan dengan profesi tersebut. Padahal, data menunjukkan bahwa Indonesia masih kekurangan sumber daya manusia (SDM) yang memiliki kemampuan teknis dalam bidang keamanan siber. Implikasi lain dari adanya kebutuhan akan DPO adalah standardisasi sertifikasi yang dapat diakui di seluruh Indonesia. Proses standardisasi sertifikasi dan pemenuhan kebutuhan SDM ini tentunya akan memakan waktu yang dikhawatirkan justru menghambat proses implementasi RUU PDP. Oleh karena itu, pemerintah juga perlu melakukan pendefinisian skala badan usaha dan persyaratan mengenai penunjukan DPO, mengingat banyaknya badan usaha dengan skala Usaha Mikro Kecil Menengah (UMKM), yang juga merupakan tulang punggung perekonomian di Indonesia.

03 Perbandingan Keberadaan Badan Otoritas Pelindungan Data Pribadi

Perdebatan mengenai independensi badan otoritas pelindungan data pribadi masih belum mendapatkan titik temu. Pemerintah menganggap kehadiran badan otoritas tidak harus independen dan dapat berada di bawah kementerian terkait. Dalam skenario ini, aspek transparansi dan objektivitas dapat diraih dengan bergantung kepada mekanisme *check and balance* antar lembaga pemerintah seperti yang sudah berlangsung selama ini. Misalnya, pada hakikatnya, Kominfo akan terus diawasi oleh DPR. Di sisi lain, keberadaan badan otoritas di bawah naungan pemerintah dikhawatirkan melemahkan independensi, transparansi, dan akuntabilitas badan itu sendiri. Kominfo sebagai lembaga publik juga memiliki tanggung jawab atas dan terikat oleh RUU PDP. Tentunya terdapat risiko penilaian yang non-objektif dari badan otoritas non-independen.

Implikasi dari lembaga yang non-independen juga sampai kepada isu tata kelola data lintas batas negara. Negara dengan hukum pelindungan data pribadi dan lembaga otoritas yang independen bisa saja ragu atau menolak untuk melakukan perpindahan data dan data *sharing* dengan negara yang tidak memiliki peraturan pelindungan data yang setara (ABLI, 2020), termasuk dalam aspek lembaga otoritas yang independen. Negara-negara ini memiliki proses penilaian kelayakan perlindungan data pribadi di suatu negara, negara Uni Eropa misalnya dengan *adequacy decision* sedangkan negara-negara lain seperti Singapura, Filipina, Thailand, dan Malaysia misalnya dengan memiliki *whitelist* (ABLI, 2020).

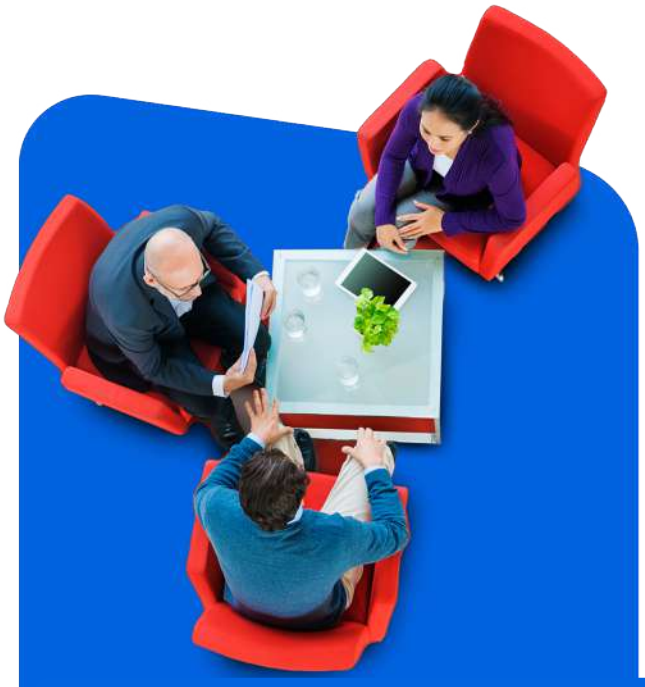
Dengan konsiderasi ini, lembaga otoritas yang independen menjadi lebih ideal dalam proses implementasi RUU PDP di Indonesia. Selain independen, beberapa praktik terbaik dalam lembaga otoritas pelindungan data adalah sebagai berikut:

- Memiliki prinsip yang konstruktif, artinya lembaga otoritas menampung masukan dan saran mengenai implementasi hukum dari berbagai pihak;
- Memiliki fungsi konsultatif, artinya lembaga otoritas memberikan pedoman serta penafsiran yang jelas, praktikal, dan mudah dipahami kepada badan publik atau swasta mengenai implementasi UU PDP yang sudah disahkan;
- Memiliki fungsi klarifikasi, artinya lembaga otoritas memberikan pedoman dan konsultasi mengenai hal-hal prosedural dari UU PDP yang sudah disahkan;
- Menggunakan alat-alat hukum dengan inovatif, seperti menerapkan mekanisme *regulatory sandbox* guna menampung input dari pihak-pihak yang relevan;

04 Kolaborasi Lintas Sektor

RUU PDP dapat menjadi pintu masuk pelindungan data pribadi pengguna internet yang lebih baik di Indonesia. Namun, RUU PDP bukan satu-satunya intervensi yang dapat dilakukan untuk menjamin data pengguna. Diperlukan kerjasama lintas sektor terkait, mulai dari regulator, perusahaan penyedia sistem elektronik, organisasi masyarakat, akademisi, media, hingga masyarakat itu sendiri sebagai aktor utama di ranah digital.

Dari sisi regulator, dibutuhkan komunikasi yang lebih transparan dan akuntabel untuk memperlihatkan dinamika serta kemajuan diskusi RUU ini. Setelah disahkan, pemerintah juga perlu mengeluarkan berbagai aturan teknis turunan untuk menjamin kepatuhan seluruh entitas yang diatur dalam RUU ini. Selain itu, diperlukan mekanisme evaluasi untuk memastikan RUU PDP mencapai tujuan aslinya yakni melindungi hak digital warga dan mendorong percepatan ekonomi digital Indonesia.



Selanjutnya, badan usaha, baik publik dan privat, dapat secara paralel menyediakan infrastruktur yang mendukung keamanan data pengguna, SDM yang tidak hanya paham mengenai aspek teknis dan etis, rancangan platform yang menjadikan privasi sebagai tanggung jawab dan tujuan bersama. Kemudian, akademisi dan organisasi masyarakat sipil dapat berkolaborasi untuk menyediakan lebih banyak edukasi yang menyasar level kognisi hingga perilaku pengguna. Kolaborasi ini harus dilakukan secara bersama-sama untuk menghasilkan dampak yang lebih besar. Pengguna sebagai aktor utama juga harus dibekali kemampuan untuk memahami pentingnya data pribadi dan berbagai tindakan yang dapat dilakukan untuk menjaga datanya. Terlebih, RUU PDP sama halnya seperti GDPR juga menjadikan *consent* atau persetujuan pengguna sebagai salah satu basis hukum pengumpulan dan pemrosesan data. Tanpa pemahaman data yang baik, keberadaan persetujuan pengguna ini justru berpotensi menjadi titik lemah dari RUU ini.

PENUTUP

Jika disahkan, RUU PDP dapat menjadi titik awal peningkatan pelindungan data dan tata kelola data pribadi di Indonesia. Namun, keberadaan RUU PDP perlu disertai dengan kejelasan teknis implementasinya. RUU PDP akan berlaku bagi lembaga publik dan sektor swasta dan diharapkan mampu menjawab tantangan digital hingga beberapa waktu ke depan *(future proof).* Beberapa tantangan implementasi yang mungkin muncul diantaranya permasalahan pembagian beban dan kewajiban untuk tingkatan badan usaha, keterkaitan dengan keamanan siber, independensi badan otoritas data pribadi. Selain tantangan implementasi, diperlukan juga kerjasama lintas sektor untuk memastikan privasi dan keamanan data pribadi pengguna. Keberadaan regulasi tanpa disertai infrastruktur dan SDM pengelola yang memadai dari penyedia sistem elektronik dan kemampuan navigasi dari pengguna tentunya tidak akan berjalan dengan efektif. Terakhir, pemerintah harus memastikan prinsip *trust,* kredibilitas, dan transparansi dari proses formulasi RUU PDP hingga implementasinya.

Referensi

Asian Business Law Institute. (2020). Transferring Personal Data in Asia: a Path to Legal Certainty and Regional Convergence.

Akbar, C. (September 3rd, 2021). 6 Kasus Kebocoran Data Pribadi di Indonesia. https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia

Chandra, G. N. (September 3rd, 2021). Indonesia at Highest Risk Level of Cyber Threat: TrendMicro. https://jakartaglobe.id/tech/indonesia-at-highest-risk-level-of-cyber-threat-trendmicro

Data Guidance. (n.d.). Comparing Privacy Laws: GDPR v. Thai Personal Data Protection Act.

Goodin, R. E., & Ratner, S. R. (2011). Democratizing international law. Global Policy, 2(3), 241-247.

Ministry of Communication and Informatics. (n.d) Existing Regulations Regarding Personal Data Protection in Indonesia [infographic].

Microsoft Indonesia. (June 20th, 2020). Malware encounter rate in Indonesia highest across Asia Pacific: Microsoft Security Endpoint Threat Report 2019. https://news.microsoft.com/id-id/2020/06/26/16846/

Privacy Law & Business. (2019). Data Protection & Privacy Information Worldwide. International Report (161).

Riyadi, G. A. (2021). Data Privacy in the Indonesia Personal Data Protection Legislation. Center for Indonesian Policy Studies Policy Brief Series.

World Bank. (2021). Report: Beyond Unicorns: Harnessing Digital Technologies for Inclusion in Indonesia, p.2.