



JUSTICES: Journal of Law

Journal website: <https://justices.pdfaii.org>

ISSN : 2964-5107 (online)
<https://doi.org/10.58355/justices.v4i3.203>

Vol. 4 No. 3 (2025)
pp. 154-168

Research Article

Analisis Yuridis Penerapan Prinsip Minimalisasi Data Dalam Mobile Banking Menurut Undang-Undang Pelindungan Data Pribadi dan EU GDPR 2018

Nyimas Safira Septiana, Sinta Dewi, Laina Rafianti

Fakultas Hukum, Universitas Padjajaran Bandung, Indonesia

E-mail: nyimas21001@mail.unpad.ac.id



Copyright © 2025 by Authors, Published by JUSTICES: Journal of Law. This is an open access article under the CC BY License <https://creativecommons.org/licenses/by/4.0/>

Received : June 26, 2025
Accepted : July 27, 2025

Revised : July 21, 2025
'Available online : August 06, 2025

How to Cite: Nyimas Safira Septiana, Sinta Dewi, & Laina Rafianti. (2025). Juridical Analysis of the Application of Data Minimization Principles in Mobile Banking According to the Personal Data Protection Law and EU GDPR 2018. *JUSTICES: Journal of Law*, 4(3), 154-168. <https://doi.org/10.58355/justices.v4i3.203>

Juridical Analysis of the Application of Data Minimization Principles in Mobile Banking According to the Personal Data Protection Law and EU GDPR 2018

Abstract. Digital transformation in the banking sector has led to the emergence of mobile banking services such as BRImo, owned by PT. Bank Rakyat Indonesia (Persero) Tbk., which offers customers easy financial transactions. However, behind this innovation, complex issues have arisen regarding compliance with the data minimization principle as stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and the 2018 General Data Protection Regulation (GDPR). This research focuses on the compliance of the personal data processing consent mechanism in the BRImo application with the data minimization principle, as well as the legal consequences of non-compliance with this principle. The research was conducted using a normative juridical approach through a review of relevant laws, doctrines, and legal literature, as well as a sociological juridical approach. The results

show that BRImo's non-compliance with the data minimization principle is reflected in the practice of bundled consent without granular options, minimal transparency regarding data purposes and retention, and limited user control to revoke or modify consent. This shifts data consent from a substantial function to a mere administrative formality, ultimately leading to potential criminal and administrative sanctions and reputational risks for service providers. Corrective measures require the implementation of granular consent, interactive privacy dashboards, strict data retention policies, the appointment of a Data Protection Officer (DPO), and internal education to ensure lawful, fair, and proportionate data processing.

Keywords: protection, personal data, data minimization.

Abstrak. Transformasi digital di sektor perbankan mendorong lahirnya layanan mobile banking seperti BRImo milik PT. Bank Rakyat Indonesia (Persero) Tbk yang menawarkan kemudahan transaksi keuangan bagi nasabah. Namun, di balik inovasi tersebut, timbul persoalan pelik mengenai kepatuhan terhadap prinsip minimalisasi data sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan General Data Protection Regulation (GDPR) 2018. Rumusan masalah penelitian ini berfokus pada kesesuaian mekanisme persetujuan pemrosesan data pribadi dalam aplikasi BRImo dengan prinsip minimalisasi data, serta akibat hukum dari ketidaktaatan terhadap prinsip tersebut. Penelitian dilakukan dengan pendekatan yuridis normatif melalui telaah peraturan perundang-undangan, doktrin, dan literatur hukum terkait, serta pendekatan yuridis sosiologis. Hasil penelitian menunjukkan ketidakpatuhan BRImo terhadap prinsip minimalisasi data tercermin dari praktik bundled consent tanpa pilihan granular, minimnya transparansi terkait tujuan dan retensi data, serta terbatasnya kontrol pengguna untuk mencabut atau mengubah persetujuan. Kondisi ini menggeser persetujuan data dari fungsi substansial menjadi sekadar formalitas administratif, yang pada akhirnya berpotensi menimbulkan sanksi pidana, administratif, dan risiko reputasi bagi penyelenggara layanan. Sebagai langkah korektif, diperlukan penerapan granular consent, dashboard privasi interaktif, kebijakan retensi data yang ketat, penunjukan Data Protection Officer (DPO), dan edukasi internal untuk menjamin pemrosesan data yang lawful, fair, dan proportionate.

Kata Kunci: pelindungan, data pribadi, minimalisasi data.

PENDAHULUAN

Dalam beberapa dekade terakhir, industri perbankan mengalami transformasi. Proses manual yang dahulu mendominasi telah bergeser menjadi layanan digital berkat kemajuan teknologi informasi, memungkinkan bank menyediakan layanan yang lebih cepat, efisien, dan terintegrasi. Perubahan ini juga memunculkan tantangan baru, terutama bagi bank konvensional yang harus bersaing dengan *fintech* dan menyesuaikan diri dengan perilaku konsumen yang semakin digital.¹ Salah satu inovasi utama dalam perbankan digital adalah mobile banking, seperti aplikasi BRImo milik PT Bank Rakyat Indonesia (Persero) Tbk. Aplikasi ini mempermudah nasabah melakukan berbagai transaksi, mulai dari pengecekan saldo hingga pembayaran online. Survei Populix 2022 menunjukkan aplikasi seperti BCA Mobile, Brimo, Livin' Mandiri, dan BNI Mobile banyak dipilih karena kepraktisan, efisiensi

¹ Ferozi Ramdana Irsyad, Filja Azkiah Siregar, Jonatan Marbun, Hasyim Hasyim, "Menghadapi Era Baru: Strategi Perbankan Dalam Menghadapi Perubahan Pasar Dan Teknologi di Indonesia", *Transformasi: Journal of Economics and Business Management*, Vol. 3, No. 2 (2024).

waktu, serta kemudahan integrasi dengan toko daring dan e-wallet. Alasan dominannya adalah untuk mendukung transaksi yang cepat dan aman di tengah gaya hidup yang serba digital.²

Seiring meningkatnya penggunaan layanan berbasis elektronik, isu pelindungan data pribadi menjadi semakin penting.³ Risiko kebocoran dan penyalahgunaan data menuntut penerapan prinsip pelindungan data yang ketat, salah satunya prinsip minimalisasi data. Prinsip ini mengharuskan pengumpulan data hanya sebatas informasi yang benar-benar diperlukan, sehingga meminimalkan risiko penyalahgunaan.⁴ Dalam praktiknya, implementasi prinsip ini di Indonesia masih memiliki banyak tantangan. Sebagai contoh, aplikasi BRI Mo meminta akses ke fitur seperti kamera, mikrofon, lokasi, dan media penyimpanan. Walaupun beberapa di antaranya relevan, seperti kamera untuk verifikasi identitas, akses ke fitur lain menimbulkan pertanyaan tentang kesesuaian dengan tujuan perbankan. Ketidaksesuaian ini meningkatkan risiko data digunakan untuk kepentingan komersial lain oleh pihak internal, seperti anak perusahaan.

Sebagai perbandingan, Bank Mandiri secara eksplisit menerapkan prinsip minimalisasi data dengan hanya mengumpulkan data yang relevan, memberikan akses bagi nasabah untuk mengubah atau menghapus data, serta menerapkan teknologi seperti *Data Loss Prevention* (DLP) untuk mencegah kebocoran data. Pendekatan ini bukan hanya melindungi privasi nasabah tetapi juga membangun kepercayaan publik terhadap bank. Prinsip minimalisasi data juga menjadi bagian fundamental dalam regulasi global, seperti *General Data Protection Regulation* (GDPR) Uni Eropa. GDPR menegaskan bahwa data yang dikumpulkan harus “adequate, relevant, and limited to what is necessary.” Regulasi ini juga menuntut transparansi, sehingga pengguna berhak tahu bagaimana data mereka dikumpulkan dan digunakan. Di Indonesia, pelindungan data pribadi telah diatur melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU ini memuat prinsip minimalisasi data dalam Pasal 16 Ayat (2) huruf a yang mengatur bahwa pengumpulan data harus terbatas pada informasi yang diperlukan untuk tujuan tertentu. Namun, pengaturannya belum detail dan masih membuka ruang interpretasi, sehingga penerapannya belum optimal.

Ketidaksesuaian praktik di lapangan dapat dilihat dari beberapa hal. Pertama, pengumpulan data yang berlebihan dan tidak relevan, seperti permintaan akses lokasi dan mikrofon oleh aplikasi perbankan, padahal tidak diperlukan untuk layanan dasar. Kedua, kurangnya transparansi tentang bagaimana data akan digunakan, meskipun UU PDP telah memberi hak bagi pengguna untuk mengetahuinya. Ketiga, tidak adanya kebijakan retensi data yang jelas, sehingga data berpotensi disimpan melebihi kebutuhan. Keempat, keterbatasan kontrol bagi pengguna untuk menolak atau

² Darmayanti Lubis, “Pengaruh Persepsi Kegunaan, Kemudahan dan Keamanan Terhadap Kepuasan Nasabah Menggunakan Mobile Banking”, *JEKSya Jurnal Ekonomi dan Keuangan Syariah*, Vol. 2, No. 2 (2023): 445.

³ Kadek Rima Anggen Suari, I Made Sarjana, “Menjaga Privasi di Era Digital: Pelindungan Data Pribadi di Indonesia” *Jurnal Analisis Hukum (JAH)*, Vol. 6, No. 1 (2023): 132-146

⁴ Naylawati Bahtiar, “Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah”, *Development Policy and Management Review (DPMR)*, Vol. 2, No. 1 (2022): 94.

mencabut persetujuan secara proporsional, yang dalam GDPR menjadi hak penting bagi subjek data. Praktik ini juga menimbulkan risiko penyalahgunaan data, baik oleh pihak internal maupun pihak ketiga. Tanpa penerapan prinsip minimalisasi data yang tegas, data pribadi dapat digunakan untuk tujuan komersial seperti pemasaran agresif atau disimpan dalam jangka panjang tanpa kejelasan.

UU PDP sebenarnya telah mengadopsi prinsip-prinsip yang selaras dengan GDPR, seperti transparansi, pembatasan tujuan, dan minimalisasi data. Namun, pelaksanaannya perlu diperkuat melalui regulasi turunan, pedoman teknis, dan pembentukan lembaga pengawas independen yang secara aktif mengawasi praktik pemrosesan data. Oleh karena itu, penting dilakukan kajian tentang penerapan prinsip minimalisasi data dalam layanan perbankan digital seperti BRI^{mo}.

Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, terdapat dua isu utama yang menjadi fokus penelitian ini. Pertama, bagaimana implementasi prinsip minimalisasi data dalam proses pemberian persetujuan pemrosesan data pada layanan BRI Mobile Banking. Kedua, perlu dianalisis akibat hukum yang timbul apabila layanan BRI Mobile Banking tidak mematuhi prinsip minimalisasi data sebagaimana diatur dalam UU No. 27 Tahun 2022.

Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini ialah pendekatan yuridis normatif, yang menelaah bahan pustaka seperti peraturan perundang-undangan, doktrin, dan putusan pengadilan untuk membangun argumentasi hukum, serta yuridis sosiologis melalui pengamatan langsung terhadap implementasi hukum di masyarakat. Penelitian bersifat deskriptif analitis untuk menggambarkan secara sistematis penerapan prinsip minimalisasi data dalam pemberian persetujuan pemrosesan data pribadi pada Program BRI Mobile Banking, dengan mengkaji Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi dan GDPR 2018.

PEMBAHASAN

Penerapan Mekanisme Persetujuan Pemrosesan Data Pribadi di Layanan BRI Mobile Banking

1. Praktik Persyaratan Permintaan Persetujuan pada Layanan BRI Mobile Banking

Di era digital, layanan BRI^{mo} menjadi salah satu inovasi penting dari Bank Rakyat Indonesia untuk mendukung kemudahan transaksi finansial nasabah. Agar dapat mengakses aplikasi ini, pengguna diwajibkan melalui tahap registrasi dengan mengisi data pribadi seperti nama lengkap, NIK, email, dan nomor telepon aktif. Selanjutnya, pengguna diminta mengunggah foto KTP dan swafoto untuk verifikasi identitas berbasis teknologi pengenalan wajah, sejalan dengan prinsip *Know Your Customer* (KYC) yang diwajibkan regulator perbankan nasional.⁵ Sebelum menikmati layanan seperti pengecekan saldo dan transfer, pengguna harus menyetujui dua

⁵ "Pemberitahuan Privasi PT Bank Rakyat Indonesia (Persero) Tbk" <https://bri.co.id/privacy>

dokumen penting, yakni syarat dan ketentuan serta pemberitahuan privasi. Dokumen ini menjelaskan penggunaan data untuk layanan, keamanan transaksi, hingga pemenuhan kewajiban hukum, serta kemungkinan pembagian data ke pihak ketiga. Namun, informasi tersebut kerap disusun dalam bahasa hukum yang sulit dipahami oleh masyarakat awam, sehingga jarang dibaca secara teliti sebelum pengguna menyetujui.⁶

Selain data identitas dan transaksi, aplikasi BRI Mo juga meminta akses ke fitur perangkat seperti kamera, mikrofon, lokasi GPS, dan media penyimpanan. Persetujuan ini diberikan secara menyeluruh atau *bundled consent* pengguna hanya bisa melanjutkan layanan jika menyetujui seluruh permintaan akses tersebut, tanpa opsi memilih akses tertentu.⁷ Model persetujuan ini berpotensi menyalahi prinsip transparansi dan persetujuan yang bebas dan sadar, sebagaimana diatur dalam Pasal 20 ayat (2) huruf c UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang mewajibkan persetujuan bersifat spesifik, eksplisit, dan berdasar informasi memadai.⁸

Permintaan akses terhadap fitur seperti galeri atau mikrofon juga menimbulkan pertanyaan relevansi, sebab tidak seluruhnya berkaitan langsung dengan layanan inti perbankan. Hal ini bertentangan dengan prinsip minimalisasi data dalam Pasal 16 ayat (2) huruf a UU PDP, serta Pasal 5(1)(c) GDPR yang menegaskan data yang diproses harus terbatas, relevan, dan sesuai kebutuhan. Selain itu, BRI Mo belum menyediakan penjelasan terbuka tentang tujuan dan penggunaan data tambahan tersebut, yang memperlemah aspek transparansi sebagaimana diwajibkan oleh Pasal 20 ayat (1) UU PDP dan Pasal 12 GDPR.

Di sisi lain, pengguna juga dihadapkan pada situasi di mana persetujuan menjadi syarat mutlak untuk mengakses layanan, yang menyalahi konsep *freely given consent* (Pasal 7(4) GDPR). Selain itu, meski permintaan unggahan foto KTP dapat dibenarkan untuk kepentingan KYC dan sesuai POJK No. 12/POJK.01/2017, tidak tersedia penjelasan terbuka mengenai masa penyimpanan data serta mekanisme penghapusannya, padahal UU PDP dan GDPR menuntut batasan waktu penyimpanan yang jelas.⁹

Aspek kontrol pengguna juga belum optimal. Pengguna tidak diberikan sarana mudah untuk mencabut persetujuan atau mengubah akses data, padahal Pasal 5 UU PDP menjamin hak koreksi, penghapusan, dan penarikan persetujuan. GDPR pun mengatur hak pengguna untuk menarik persetujuan kapan saja tanpa konsekuensi negatif (Pasal 7(3) GDPR). Terakhir, dari sudut pandang akuntabilitas, pengendali data seperti BRI berkewajiban membuktikan bahwa persetujuan diperoleh secara sah dan sadar (Pasal 25 UU PDP dan Pasal 5(2) GDPR). Namun, minimnya pelaporan terbuka mengenai audit internal, penilaian risiko perlindungan data (*Data Protection*

⁶ "Pemberitahuan Privasi PT Bank Rakyat Indonesia (Persero) Tbk" <https://bri.co.id/privacy>

⁷ Bojana Kostic and Emmanuel Vargas Penagos, "The freely given consent and the "bundling" provision under the GDPR" *Afl.* 4 augustus 2017

⁸ "Pemberitahuan Privasi PT Bank Rakyat Indonesia (Persero) Tbk" <https://bri.co.id/privacy>

⁹ Elizabeth Schweyen, "Making Sense of Consent Under The GDPR", 7 Maret 2018, <https://blog.returnpath.com/making-sense-consent-gdpr/> diakses pada tanggal 21 April 2025 (Lihat juga Pasal 5 ayat (1) General Data Protection Regulation).

Impact Assessment/DPIA), atau pengawasan menunjukkan penerapan akuntabilitas belum maksimal.

Keseluruhan praktik ini memperlihatkan bahwa meskipun terdapat langkah-langkah untuk memenuhi kewajiban hukum, model persetujuan pada BRI Mo cenderung bersifat administratif dan belum sepenuhnya menempatkan hak privasi pengguna sebagai prioritas utama. Oleh karena itu, penting untuk mengevaluasi kembali desain persetujuan agar selaras dengan prinsip minimalisasi data, transparansi, dan penguatan kontrol pengguna sebagaimana diamanatkan oleh UU PDP dan GDPR.

2. Analisis Kesesuaian Keterkaitan antara prosedur BRI Mobile Banking dengan Prinsip Minimalisasi Data dalam UU No. 27 Tahun 2022 dan GDPR

Dalam hukum positif Indonesia, prinsip minimalisasi data tercantum dalam Pasal 16 ayat (2) huruf a UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang mewajibkan pemrosesan data dilakukan terbatas dan relevan dengan tujuan yang telah diinformasikan kepada subjek data. Artinya, data yang dikumpulkan tidak boleh melampaui kebutuhan sebenarnya. Namun, praktik BRI Mo yang meminta akses ke lokasi, galeri, dan mikrofon tanpa penjelasan fungsi konkrit menunjukkan adanya potensi ketidaksesuaian dengan prinsip ini. Di tingkat internasional, GDPR dalam Pasal 5(1)(c) juga mengatur bahwa data pribadi harus “adequate, relevant and limited to what is necessary,” dengan redaksi lebih tegas yang menekankan pentingnya pembatasan proporsional antara tujuan dan volume data. Dalam BRI Mo, permintaan data yang bersifat menyeluruh tanpa pemisahan antara data esensial dan tambahan menunjukkan belum diterapkannya prinsip pembatasan ini.

Idealnya, pengguna seharusnya dapat menyetujui pengumpulan data wajib terlebih dahulu, lalu memilih secara sukarela untuk data tambahan. Prinsip *Data Protection by Design and by Default* sebagaimana diatur Pasal 25 GDPR juga mewajibkan desain sistem yang memprioritaskan perlindungan data sejak awal, yang belum tampak dalam prosedur BRI Mo. Sebagai pembanding, Bank Mandiri melalui laporan ESG menyatakan hanya mengumpulkan data sesuai kebutuhan transaksi, menyediakan opsi penghapusan, dan menggunakan teknologi DLP.¹⁰

Dari aspek retensi data, GDPR (Pasal 5(1)(e)) dan UU PDP (Pasal 16 ayat (2) huruf d) mengharuskan adanya batas waktu penyimpanan. Namun, BRI Mo tidak secara jelas menyampaikan masa simpan data KTP atau mekanisme penghapusannya. Transparansi internal juga belum tampak; padahal Pasal 25 UU PDP mengharuskan pengendali data membuktikan kepatuhan, misalnya melalui audit atau DPIA. Selain itu, BRI Mo belum secara tegas menjamin bahwa data hanya dipakai untuk tujuan awal sebagaimana diatur dalam prinsip *purpose limitation* (Pasal 5(1)(b) GDPR). Tidak adanya mekanisme kontrol terhadap perubahan tujuan pemrosesan memperbesar risiko pelanggaran dan menurunkan kepercayaan pengguna. Dengan demikian, penerapan prosedur BRI Mo belum sepenuhnya sesuai prinsip minimalisasi data dalam UU PDP dan GDPR. Penyesuaian kebijakan dibutuhkan tidak hanya sebagai

¹⁰ <https://www.bankmandiri.co.id/esg-customer-rights>

kewajiban hukum, tetapi juga demi memperkuat kepercayaan nasabah terhadap pelindungan data pribadi mereka.

3. Penilaian Terhadap Mekanisme Persetujuan Berdasarkan Standar Pelindungan Data Pribadi

Mekanisme persetujuan dalam layanan BRI Mo belum sepenuhnya sesuai dengan standar pelindungan data pribadi baik menurut hukum nasional maupun internasional. GDPR Pasal 4(11) mendefinisikan persetujuan sebagai pernyataan kehendak yang diberikan secara bebas, spesifik, berdasarkan informasi, dan tegas. Dalam praktik BRI Mo, elemen *freely given* dan *specific consent* belum terpenuhi, karena pengguna diminta menyetujui seluruh syarat dan kebijakan privasi sekaligus tanpa opsi untuk memilih data mana saja yang boleh diproses.¹¹ Hal ini bertentangan dengan prinsip *granular consent*, yang menuntut agar persetujuan dapat dipilah berdasarkan tujuan atau jenis pemrosesan. Selain itu, BRI Mo belum menyediakan mekanisme bagi pengguna untuk menarik atau mengubah persetujuan yang telah diberikan.¹² Padahal, Pasal 7(3) GDPR mewajibkan pengendali data menyediakan cara yang mudah bagi pengguna untuk mencabut persetujuan kapan saja. Ketiadaan fitur ini mengurangi kontrol pengguna atas data pribadinya, bertentangan dengan prinsip *right to informational self-determination*.

Di sisi teknis, BRI Mo juga tidak menunjukkan transparansi terkait bagaimana persetujuan disimpan dan diverifikasi. Standar GDPR Pasal 7(1) mengharuskan pengendali data menyimpan bukti sah bahwa persetujuan diberikan secara aktif. Belum diketahui apakah BRI Mo memiliki catatan digital yang mendukung validitas persetujuan tersebut. Penerapan prinsip *privacy by design and by default* sebagaimana diatur dalam Pasal 25 GDPR juga tampak belum diterapkan. Sistem BRI Mo cenderung langsung meminta akses ke berbagai fitur perangkat tanpa pilihan untuk menolak data non-esensial. Secara normatif, UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi juga mengatur perlunya pemrosesan yang spesifik dan terbatas, namun implementasi teknis di BRI Mo belum mencerminkan hal tersebut.

Kelemahan lain adalah informasi kebijakan privasi disajikan dalam bentuk teks panjang yang sulit dipahami, sehingga melanggar semangat *meaningful consent*.¹³ Dalam perspektif hukum kontrak, ini mendekati bentuk kontrak baku yang berpotensi memberatkan satu pihak dan berisiko tidak memenuhi asas keadilan serta itikad baik. BRI Mo juga tampak belum memiliki dokumentasi publik seperti audit atau laporan tahunan mengenai pelindungan data. Padahal, Pasal 25 UU PDP menuntut akuntabilitas dan transparansi pengendali data. Ketiadaan informasi ini membuat mekanisme persetujuan lebih bersifat administratif ketimbang substansial. Untuk memenuhi standar GDPR dan UU PDP, BRI Mo perlu mengembangkan fitur

¹¹ Elizabeth Schweyen, "Making Sense of Consent Under The GDPR", 7 Maret 2018, <https://blog.returnpath.com/making-sense-consent-gdpr/> diakses pada tanggal 21 April 2025 (Lihat juga Pasal 5 ayat (1) General Data Protection Regulation).

¹² Ilias Gultom, Auditya Firza Saputra, Muhammad Faiz Aziz, "Pelindungan data pribadi di Indonesia Menyikapi Liberalisasi Ekonomi Digital" *Indonesia for Global Justice* Juni 2021

¹³ Tiana Dermendjieva, "PIPEDA's Guidelines for Obtaining Meaningful Consent" GDPR Local <https://gdprlocal.com/pipedas-guidelines-for-obtaining-meaningful-consent/>

dashboard persetujuan, memisahkan data esensial dan tambahan, serta menyusun laporan pelindungan data secara rutin. Hanya melalui langkah konkret tersebut, persetujuan dapat benar-benar melindungi pengguna dan bukan sekadar syarat formal.

Implikasi Yuridis Ketidakpatuhan BRI Mobile Banking terhadap Prinsip Minimalisasi Data dalam Undang-Undang Pelindungan Data Pribadi

1. Penerapan Prinsip Minimalisasi Data pada Permintaan Persetujuan BRI Mobile Banking Berdasarkan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi

Pelindungan data pribadi dalam layanan BRI Mo diatur melalui UU PDP, serta regulasi sektoral dari OJK dan BI. UU PDP mewajibkan pengendali data, termasuk BRI, untuk memproses data secara sah, adil, transparan, dan mematuhi prinsip minimalisasi data. Artinya, BRI hanya diperbolehkan mengumpulkan data pribadi yang relevan dan benar-benar diperlukan sesuai tujuan layanan. Pengendali data juga wajib memperoleh persetujuan yang sah dari nasabah, sekaligus menjamin hak nasabah untuk mengakses, memperbarui, atau mencabut persetujuan atas pemrosesan data.¹⁴ Sebagai bentuk tanggung jawab, BRI harus melaksanakan kebijakan internal dan pengamanan ketat, seperti enkripsi data, autentikasi ganda, audit berkala, serta prosedur tanggap insiden bila terjadi kebocoran data. Langkah ini bukan hanya kewajiban hukum, tetapi juga penting untuk menjaga kepercayaan publik dan kestabilan sektor perbankan digital.¹⁵

UU ITE memperkuat posisi hukum data elektronik dan mengharuskan penyelenggara sistem elektronik menjaga keamanan informasi. Sementara itu, Peraturan Bank Indonesia (PBI) menekankan penerapan manajemen risiko teknologi informasi, pengawasan internal, dan audit untuk memastikan kepatuhan terhadap pelindungan data. Kerangka hukum ini menempatkan tanggung jawab langsung pada bank atas pelanggaran yang merugikan nasabah, sehingga tidak hanya mencegah penyalahgunaan data tetapi juga mendukung akuntabilitas layanan perbankan digital.¹⁶

Dalam praktik pembukaan rekening digital, calon nasabah BRI cukup mengisi data diri melalui aplikasi, mengunggah foto KTP, dan melakukan swafoto untuk verifikasi identitas biometrik. Proses ini memanfaatkan teknologi pencocokan data dengan database Dukcapil agar lebih cepat, akurat, dan aman.¹⁷ Meski secara teknis efisien, muncul persoalan mendasar terkait pemenuhan prinsip minimalisasi data dan sahnya persetujuan. Proses ini sering kali tidak diikuti dengan penjelasan

¹⁴ Sutra Disemadi, H. "Pelindungan Nasabah Dalam Penerapan Electronic Banking Sebagai Bagian Aktifitas Bisnis Perbankan Di Indonesia. Jurnal Perspektif Administrasi Dan Bisnis" Vol. 2 No. 1 (2021), 27-40. <https://doi.org/10.38062/jpab.v2i1.16>

¹⁵ Sutra Disemadi, H. *Pelindungan Nasabah Dalam Penerapan Electronic Banking Sebagai Bagian Aktifitas Bisnis Perbankan Di Indonesia...*,

¹⁶ Riza Diandra Tanjung, Nurhilmiah, "Aspek Pelindungan Hukum Atas Data Pribadi Nasabah pada Penyelenggaraan Layanan Mobile Banking pada PT. Bank Rakyat Indonesia Cabang Stabat" *Dinasti Review* Vol. 4, No. 5, Juli (2024), 3.

¹⁷ ida. (2023, April 18). Peran verifikasi identitas Biometrik Untuk pendaftaran rekening online. HOME. <https://vida.id/id/blog/the-role-of-biometric-identity-verification-for-online-account-registration>

memadai kepada pengguna tentang bagaimana data biometrik akan digunakan, disimpan, atau dihapus. Padahal, UU PDP mensyaratkan persetujuan yang eksplisit, bebas, dan berdasarkan informasi yang lengkap. Praktik ini melanggar asas transparansi dan membuka risiko pemrosesan data berlebihan.¹⁸

Selain itu, calon nasabah diminta menyetujui beberapa klausul wajib: persetujuan pemrosesan data oleh pihak ketiga, pernyataan calon nasabah, dan syarat ketentuan. Ketiganya harus disetujui sekaligus agar proses pendaftaran berjalan. Tidak adanya pilihan menolak sebagian persetujuan menempatkan nasabah dalam posisi lemah, kehilangan kendali atas data pribadinya, dan menjadikan persetujuan tidak bebas (*bundled consent*). *Bundled consent* bertentangan dengan Pasal 20 ayat (2) huruf c UU PDP, yang menegaskan persetujuan harus eksplisit, spesifik, dan berbasis informasi lengkap. Prinsip *granular consent* yang berlaku dalam GDPR (Pasal 7(4)) juga mengharuskan pemisahan persetujuan sesuai jenis pemrosesan. Jika nasabah tidak dapat menggunakan layanan inti tanpa menyetujui pemrosesan data tambahan (misalnya untuk pemasaran atau kerja sama), maka persetujuan menjadi tidak sah karena tidak diberikan secara sukarela.

Lebih lanjut, UU PDP mewajibkan transparansi mengenai siapa saja pihak ketiga yang menerima data dan untuk tujuan apa. Praktik BRI yang tidak menyajikan penjelasan rinci terkait hal ini melemahkan keabsahan persetujuan dan melanggar hak data *autonomy* nasabah. Permintaan akses aplikasi BRI^{mo} ke berbagai fitur perangkat juga perlu dinilai berdasar prinsip minimalisasi data. UU PDP Pasal 16 ayat (2) huruf a menyatakan data hanya boleh dikumpulkan secara terbatas dan relevan. Ketentuan ini sejalan dengan Pasal 5(1)(c) GDPR, yang menyebut data harus "*adequate, relevant, and limited to what is necessary*".

- a. Akses Kamera: relevan dan sah karena digunakan untuk verifikasi identitas melalui swafoto dan pemindaian KTP.
- b. Akses Mikrofon: justifikasinya tidak jelas, sehingga melanggar prinsip minimalisasi jika pengguna tidak diberi informasi tentang fungsinya.
- c. Akses Galeri: meskipun mungkin digunakan untuk unggah dokumen tambahan, tanpa penjelasan eksplisit tujuan dan cara pemrosesan, maka permintaan ini tidak memenuhi syarat transparansi dan proporsionalitas.

Permintaan akses tanpa pemisahan kebutuhan utama dan tambahan menyebabkan persetujuan menjadi tidak bebas. Apalagi, persetujuan diberikan satu paket tanpa pilihan untuk menolak sebagian. Ini melanggar prinsip persetujuan yang sah sebagaimana diatur UU PDP dan GDPR. Pengumpulan data tanpa kejelasan tujuan juga menyalahi Pasal 3 huruf f UU PDP tentang prinsip minimalisasi data. Permintaan akses mikrofon dan galeri tanpa penjelasan menimbulkan *excessive processing*, yang membuka peluang risiko penyalahgunaan data. Dalam konteks hukum Indonesia, hal ini juga dapat dianggap melanggar hak privasi yang dijamin Pasal 28G UUD 1945.

Selain legalitas, prinsip proporsionalitas juga terlanggar. UU PDP dan GDPR menegaskan bahwa setiap data yang diproses harus punya dasar hukum, tujuan sah,

¹⁸ Tereza Pertot, "Personal data supplying: the issue of bundled consent" *Università degli Studi di Trieste* Vol. 3 (2023)

dan disertai persetujuan yang jelas. Tanpa informasi rinci, pemrosesan data cenderung tidak proporsional dan rawan disalahgunakan. Ketiadaan *dashboard* persetujuan atau opsi *granular consent* juga melemahkan hak kendali pengguna. Nasabah idealnya dapat menarik atau mengubah persetujuan kapan saja, sesuai Pasal 7(3) GDPR. Ketiadaan fitur ini menjadikan kontrol data sepihak pada bank, bukan pada pemilik data.

Praktik *bundled consent* juga menimbulkan ketimpangan relasi antara pengguna dan pengendali data. Bank sebagai pihak dominan memaksa pengguna menerima semua ketentuan. Padahal, UU PDP mengatur persetujuan harus diberikan dengan bebas, bukan dipaksakan sebagai syarat akses layanan inti.¹⁹ Selain itu, tidak ada keterbukaan apakah BRI menyimpan bukti persetujuan secara aktif (misalnya log digital). Padahal, Pasal 7(1) GDPR mewajibkan pengendali data membuktikan bahwa persetujuan telah diberikan secara sah. Ketiadaan bukti ini melemahkan akuntabilitas dan transparansi. Pada akhirnya, meskipun penggunaan biometrik seperti kamera sah untuk verifikasi, permintaan akses lain (mikrofon, galeri) yang tak dijelaskan melanggar prinsip legalitas dan proporsionalitas. Bank seharusnya menjelaskan kepada pengguna bagaimana, untuk apa, dan berapa lama data disimpan, sesuai prinsip transparansi.

Kesimpulannya, model persetujuan BRI Mo yang mengharuskan nasabah menyetujui seluruh syarat sekaligus, tanpa ruang menolak sebagian, melanggar ketentuan UU PDP dan GDPR. Upaya perbaikan dapat dilakukan melalui pengembangan sistem *granular consent*, *dashboard* transparan, serta audit dan laporan berkala mengenai pengelolaan data pribadi. Hanya dengan penerapan prinsip minimalisasi data yang nyata, kepercayaan publik terhadap layanan digital bank dapat terjaga.

Akibat Hukum yang Timbul dari Ketidaktaatan Layanan BRI Mobile Banking Terhadap Asas Minimalisasi Data Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi dirancang untuk memperkuat hak warga negara atas data pribadinya. Regulasi ini memiliki beberapa tujuan pokok:²⁰ pertama, menjamin hak individu mengendalikan data pribadinya; kedua, mencegah penyalahgunaan informasi oleh pihak ketiga; ketiga, menjaga keamanan data pribadi dari kebocoran atau ancaman siber; dan keempat, membangun kepercayaan masyarakat terhadap layanan digital dan lembaga pengelola data.

¹⁹ J. Ahmed et al., "GDPR Compliant Consent Driven Data Protection in Online Social Networks: A Blockchain-Based Approach," 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 2020, 307–312, <https://doi.org/10.1109/ICICT50521.2020.00054>.

²⁰ JDIH Kota Semarang, "Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP): Menjaga Keamanan dan Privasi Data Warga Negara," Senin, 2 Desember 2024, <https://jdih.semarangkota.go.id/artikel/view/undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-pdp-menjaga-keamanan-dan-privasi-data-warga-negara>.

UU PDP berlaku bagi siapa pun, termasuk individu, badan publik, dan organisasi internasional, sepanjang aktivitas pemrosesan data pribadi dilakukan di wilayah Indonesia atau memiliki dampak hukum di Indonesia. Ini memastikan setiap pemrosesan data milik warga negara Indonesia, baik di dalam maupun luar negeri, tetap tunduk pada UU PDP. Data pribadi sendiri dibagi menjadi dua kategori utama (Pasal 4 UU PDP): data pribadi umum seperti nama, agama, atau kewarganegaraan, dan data pribadi spesifik yang lebih sensitif, seperti data kesehatan, biometrik, informasi keuangan, atau pandangan politik. Perlindungan hukum lebih ketat diberikan untuk data spesifik karena risikonya lebih besar jika disalahgunakan.²¹

Landasan utama UU PDP terletak pada penghormatan terhadap hak subjek data. Pemrosesan data oleh pengendali data maupun pihak ketiga harus selalu mempertimbangkan hak-hak individu. Pendekatan ini diwujudkan dalam delapan prinsip pemrosesan data yang diatur Pasal 16 ayat (2) UU PDP:²²

1. pengumpulan data harus terbatas, sah, transparan, dan relevan.
2. pemrosesan data harus sesuai tujuan yang jelas.
3. penghormatan terhadap hak subjek data.
4. menjaga akurasi dan kelengkapan data.
5. perlindungan keamanan data.
6. transparansi dalam aktivitas pemrosesan.
7. penghapusan data setelah masa retensi selesai; dan
8. akuntabilitas, yakni pengendali data dapat membuktikan kepatuhan.

Di antara prinsip tersebut, asas minimalisasi data sangat penting, hanya data relevan yang boleh dikumpulkan untuk tujuan sah, eksplisit, dan spesifik. Prinsip ini mencegah pengumpulan data berlebihan (*overcollection*) yang berpotensi melanggar privasi.²³ UU PDP juga memberikan hak kepada subjek data, seperti hak mengakses, memperbaiki, menghapus, atau menarik persetujuan atas data pribadinya. Meski ada pengecualian untuk kepentingan tertentu (pertahanan, penegakan hukum, administrasi kependudukan, dan sektor jasa keuangan), pengendali data tetap wajib menjaga keseimbangan antara kepentingan publik dan hak privasi individu.

Untuk memastikan kepatuhan, pengendali data diwajibkan menunjuk pejabat perlindungan data (*Data Protection Officer/DPO*). DPO bertugas memantau kepatuhan perusahaan terhadap UU PDP, melaksanakan kebijakan internal, serta memastikan adanya sistem keamanan data yang memadai. Kehadiran DPO juga mendukung akuntabilitas lembaga, menjaga kepercayaan konsumen, dan memperkuat citra korporasi. Perkembangan pesat layanan digital, termasuk BRI Mobile Banking, memudahkan transaksi nasabah, tetapi juga meningkatkan risiko pelanggaran privasi. Sebagai lembaga keuangan, BRI wajib mematuhi prinsip

²¹ Heru Tjatur, Debora Irene C., Bayu Wardhana, dan Guruh Dwi Riyanto, *Pelindungan Data Pribadi dalam Jurnalisme dan Media*, (Jakarta: Asosiasi Media Siber Indonesia, 2024), 14.

²² Heru Tjatur, Debora Irene C., Bayu Wardhana, dan Guruh Dwi Riyanto, *Pelindungan Data Pribadi dalam Jurnalisme dan Media...*, 19.

²³ Masitoh Indriani and Annida Aqila Putri, "Persetujuan Dinamis sebagai Sarana Optimalisasi Pelindungan Data Pribadi dan Hak atas Privasi," *Jurnal HAM* 14, no. 2 (Agustus 2023): 105–122, <https://doi.org/10.30641/ham.2023.14.105-122>.

minimalisasi data: hanya mengumpulkan data yang diperlukan untuk layanan perbankan. UU PDP memuat tiga aspek yang mencerminkan prinsip ini:

1. Batasan tujuan (*purpose limitation*): data hanya digunakan untuk kepentingan yang sah dan sudah diinformasikan.
2. Akurasi dan relevansi (*data accuracy and relevance*): data harus selalu mutakhir dan relevan.
3. Transparansi dan persetujuan eksplisit (*transparency and consent*): persetujuan harus jelas, tidak memaksa, dan berbasis informasi lengkap.²⁴

Dalam praktiknya, jika BRI Mobile Banking mengumpulkan data yang berlebihan atau tidak sesuai tujuan, ini melanggar UU PDP. Misalnya, pemaksaan calon nasabah untuk menyetujui penggunaan data untuk pihak ketiga tanpa pilihan menolak sebagian (*bundled consent*). Praktik ini bertentangan dengan Pasal 20 ayat (2) huruf c UU PDP, yang menuntut persetujuan eksplisit, khusus, dan berdasar informasi lengkap. Selain *bundled consent*, risiko juga muncul dari permintaan akses aplikasi ke fitur perangkat seperti kamera, mikrofon, atau galeri. Akses kamera bisa dianggap wajar untuk verifikasi identitas. Namun, permintaan akses mikrofon atau galeri tanpa kejelasan tujuan berpotensi menjadi pemrosesan data berlebihan (*excessive processing*). Ini bertentangan dengan prinsip minimalisasi data di Pasal 16 ayat (2) huruf a UU PDP dan Pasal 5(1)(c) GDPR.

Apabila terjadi pelanggaran prinsip ini, UU PDP mengatur konsekuensi hukum berupa sanksi pidana dan administratif. Dari sisi pidana, Pasal 67 dan 68 menetapkan ancaman penjara atau denda bagi pihak yang terbukti memproses data secara ilegal, mengumpulkan data tanpa dasar hukum, atau menyebarkan data pribadi tanpa izin. Untuk korporasi, ada sanksi administratif (Pasal 70), seperti peringatan tertulis, penghentian sementara pemrosesan data, hingga kewajiban melaksanakan tindakan korektif. Selain hukuman formal, pelanggaran privasi dapat merusak reputasi lembaga keuangan seperti BRI. Kepercayaan publik adalah modal penting dalam industri perbankan digital. Kebocoran data atau penyalahgunaan informasi dapat memicu penurunan jumlah nasabah, rusaknya loyalitas pelanggan, dan dampak negatif bagi citra perusahaan di mata investor.

Sebagai perbandingan, GDPR di Uni Eropa juga menekankan prinsip *data minimization* dalam Pasal 5(1)(c). Pelanggaran serius dapat dikenakan denda sangat tinggi: hingga €20 juta atau 4% omzet global tahunan. GDPR juga memberi hak subjek data untuk menuntut ganti rugi dan memaksa pengendali data melakukan audit, penghentian pemrosesan, atau penghapusan data ilegal. Tujuannya sama yakni mencegah pengumpulan data yang tidak relevan dan memperkuat akuntabilitas lembaga pengelola data.²⁵ Persamaan UU PDP dan GDPR terletak pada pengakuan bahwa data pribadi adalah hak asasi individu. Meski mekanisme sanksi berbeda, keduanya menegaskan pentingnya: pengumpulan data terbatas, persetujuan

²⁴ Sinta Dewi Rosadi, "Pelindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara," in *Kebebasan Berekspresi di Indonesia: Hukum, Dinamika, Masalah Dan Tantangannya* (2016), 210.

²⁵ Masitoh Indriani and Ekawestri Prajwalita Widiati, "The Privacy Challenge in the 'Smart Era': A Study of the Implementation of e-Government in Surabaya," *ICPS 2018 Proceeding*, no. ICPS (2019): 641-644, <https://doi.org/10.5220/0007548606410644>.

transparan, dan perlindungan hak subjek data. Bagi BRI Mobile Banking, kepatuhan bukan hanya soal menghindari sanksi, tetapi juga menjaga reputasi dan kepercayaan konsumen.

Sebagai simpulan, ketidaksesuaian mekanisme persetujuan dan retensi data di BRI Mo menunjukkan perlunya reformasi prosedur, seperti penerapan dashboard transparansi dan pemisahan persetujuan (*granular consent*). Penunjukan DPO, audit berkala, serta pembatasan retensi data menjadi langkah penting untuk memastikan kepatuhan terhadap prinsip minimalisasi data. Langkah ini bukan hanya tuntutan hukum, tetapi juga upaya strategis menjaga kepercayaan publik di era layanan keuangan digital yang kian kompetitif.

PENUTUP

Berdasarkan hasil analisis, mekanisme persetujuan pemrosesan data di aplikasi BRI Mo saat ini belum sepenuhnya sesuai dengan prinsip perlindungan data pribadi dalam UU PDP dan GDPR, antara lain terlihat dari penerapan *bundled consent* yang tidak memberi opsi selektif bagi pengguna, sehingga melanggar prinsip *data minimization* dan asas *privacy by design and by default*. Kurangnya transparansi dalam penyampaian tujuan, masa retensi, dan pemusnahan data juga bertentangan dengan kewajiban memberikan informasi yang jelas sebagaimana diatur dalam Pasal 20 UU PDP dan Pasal 12 GDPR, sedangkan ketiadaan fitur pencabutan dan revisi persetujuan secara mandiri serta dokumentasi persetujuan yang memadai tidak selaras dengan prinsip *freely given and granular consent*. Permasalahan ini mengindikasikan bahwa mekanisme persetujuan BRI Mo lebih bersifat formalitas administratif ketimbang penghormatan substantif terhadap hak pengguna. Maka, disarankan agar BRI menerapkan *granular consent* yang memisahkan izin berdasarkan jenis data dengan penjelasan manfaat teknis yang mudah dipahami; menyediakan dashboard privasi interaktif untuk memudahkan pengguna memantau, mencabut, atau mengubah persetujuan; menetapkan kebijakan retensi data yang proporsional dan disosialisasikan dengan jelas; menerapkan *privacy by design* melalui proses *Data Protection Impact Assessment* (DPIA) yang diawasi oleh *Data Protection Officer* (DPO); serta memperkuat budaya perlindungan data dengan pelatihan internal dan komunikasi aktif dengan otoritas terkait. Langkah-langkah tersebut penting untuk memastikan pemrosesan data berjalan proporsional, akuntabel, dan sejalan dengan regulasi yang berlaku demi menjaga kepercayaan dan hak privasi nasabah.

DAFTAR PUSTAKA

- Ahmed, J., et al. (2020). GDPR Compliant Consent Driven Data Protection in Online Social Networks: A Blockchain-Based Approach. 2020 3rd International Conference on Information and Computer Technologies (ICICT), 307–312. <https://doi.org/10.1109/ICICT50521.2020.00054>
- Bahtiar, N. (2022). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. *Development Policy and Management Review (DPMR)*, 2(1), 94.

- Disemadi, H. S. (2021). Pelindungan Nasabah Dalam Penerapan Electronic Banking Sebagai Bagian Aktifitas Bisnis Perbankan Di Indonesia. *Jurnal Perspektif Administrasi Dan Bisnis*, 2(1), 27–40. <https://doi.org/10.38062/jpab.v2i1.16>
- Gultom, L., Saputra, A. F., & Aziz, M. F. (2021). Pelindungan data pribadi di Indonesia Menyikapi Liberalisasi Ekonomi Digital. *Indonesia for Global Justice*.
- Indriani, M., & Putri, A. A. (2023). Persetujuan Dinamis sebagai Sarana Optimalisasi Pelindungan Data Pribadi dan Hak atas Privasi. *Jurnal HAM*, 14(2), 105–122. <https://doi.org/10.30641/ham.2023.14.105-122>
- Indriani, M., & Widiati, E. P. (2019). The Privacy Challenge in the 'Smart Era': A Study of the Implementation of e-Government in Surabaya. *ICPS 2018 Proceeding*, 641–644. <https://doi.org/10.5220/0007548606410644>
- Irsyad, F. R., Siregar, F. A., Marbun, J., & Hasyim, H. (2024). Menghadapi Era Baru: Strategi Perbankan Dalam Menghadapi Perubahan Pasar Dan Teknologi di Indonesia. *Transformasi: Journal of Economics and Business Management*, 3(2).
- JDIH Kota Semarang. (2024, Desember 2). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP): Menjaga Keamanan dan Privasi Data Warga Negara. <https://jdih.semarangkota.go.id/artikel/view/undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-pdp-menjaga-keamanan-dan-privasi-data-warga-negara>
- Kostic, B., & Penagos, E. V. (2017). The freely given consent and the “bundling” provision under the GDPR.
- Lubis, D. (2023). Pengaruh Persepsi Kegunaan, Kemudahan dan Keamanan Terhadap Kepuasan Nasabah Menggunakan Mobile Banking. *JEKSya Jurnal Ekonomi dan Keuangan Syariah*, 2(2), 445.
- Pertot, T. (2023). Personal data supplying: the issue of bundled consent. *Università degli Studi di Trieste*, 3.
- Ramdana Irsyad, F., Siregar, F. A., Marbun, J., & Hasyim, H. (2024). Menghadapi Era Baru: Strategi Perbankan Dalam Menghadapi Perubahan Pasar Dan Teknologi di Indonesia. *Transformasi: Journal of Economics and Business Management*, 3(2).
- Riza Diandra Tanjung, & Nurhilmiah. (2024). Aspek Pelindungan Hukum Atas Data Pribadi Nasabah pada Penyelenggaraan Layanan Mobile Banking pada PT. Bank Rakyat Indonesia Cabang Stabat. *Dinasti Review*, 4(5).
- Rosadi, S. D. (2016). Pelindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara. In *Kebebasan Berekspresi di Indonesia: Hukum, Dinamika, Masalah dan Tantangannya*, 210.
- Schweyen, E. (2018, Maret 7). Making Sense of Consent Under The GDPR. <https://blog.returnpath.com/making-sense-consent-gdpr/>
- Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Pelindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum (JAH)*, 6(1), 132–146.
- Tjatur, H., Debora Irene, C., Wardhana, B., & Riyanto, G. D. (2024). *Pelindungan Data Pribadi dalam Jurnalisme dan Media*. Jakarta: Asosiasi Media Siber Indonesia.
- Vida. (2023, April 18). Peran verifikasi identitas Biometrik Untuk pendaftaran rekening online. <https://vida.id/id/blog/the-role-of-biometric-identity-verification-for-online-account-registration>

- Tiana Dermendjieva. (n.d.). PIPEDA's Guidelines for Obtaining Meaningful Consent. *GDPR Local*. <https://gdprlocal.com/pipedas-guidelines-for-obtaining-meaningful-consent/>
- PT Bank Rakyat Indonesia (Persero) Tbk. Pemberitahuan Privasi. <https://bri.co.id/privacy>
- Bank Mandiri. (n.d.). ESG Customer Rights. <https://www.bankmandiri.co.id/esg-customer-rights>