Sinergi : Jurnal Ilmiah Multidisiplin
E-ISSN : 3109-0559
Volume 2 Nomor 4 April 2026

https://publikasi.ahlalkamal.com/index.php/sinergi

Perlindungan Hukum Data Nasabah Dalam Bank Digital Berbasis General Data Protection Regulation Di Indonesia

Affan Najmun Nahar[1], Putra Bagus Oktavian[2], Adrian Hadiputra[3], Dismas Arya Diputra[4], Ahmad Rezal Rizkyansyah[5], Baidhowi[6]
[1,2,3,4,5,6] Fakultas Hukum Negeri Semarang, Indonesia
Email: affannajmun@students.unnes.ac.id[1], ptraabagus@students.uunes.ac.id[2], adrianhadiputra1835@students.unnes.ac.id[3], dismasary@students.unnes.ac.id[4], ahmadrezalrizkyansyah@students.unnes.ac.id[5], baidhowi@mail.unnes.ac.id[5]

Abstract
Advances in digital technology have driven the transformation of banking services from conventional systems to digital banks that rely on electronic data processing. This transformation brings convenience to customers, but at the same time increases the risk of personal data breaches, unauthorized access, and cyberattacks. This study aims to analyze legal regulations governing digital banks regarding customer data breaches,legal protections for customer data, and to compare regulations in Indonesia with the General Data Protection Regulation (GDPR) in the European Union. The research methodology employed is a normative legal approach using legislative, conceptual, and comparative analyses. The research results indicate that Indonesia already has a legal framework for customer data protection through the principle of bank secrecy in the Banking Law, the Information and Electronic Transactions Law, and the Personal Data Protection Law, which require data controllers to ensure data security and report data protection failures within a maximum of 3 x 24 hours. However, the implementation of such protection still faces challenges in the areas of supervision, compliance, and enforcement. Compared to the GDPR, regulations in Indonesia still lag behind in terms of accountability, the severity of sanctions, the obligation to notify data breaches, and the authority of the supervisory body. Therefore, legal protection of customer data in digital banks in Indonesia needs to be strengthened through supervision
Keywords: personal data protection, data breaches, Personal Data Protection Act, GDPR.

Abstrak
Perkembangan teknologi digital telah mendorong transformasi layanan perbankan dari sistem konvensional menjadi bank digital yang mengandalkan pengolahan data elektronik. Transformasi ini membawa kemudahan bagi nasabah, tetapi sekaligus meningkatkan risiko kebocoran data pribadi, penyalahgunaan akses, dan serangan siber. Penelitian ini bertujuan untuk menganalisis regulasi hukum bank digital atas kebocoran data nasabah, perlindungan hukum terhadap data nasabah, serta membandingkan pengaturan di Indonesia dengan General Data Protection Regulation (GDPR) di Uni Eropa. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan. Hasil penelitian menunjukkan bahwa Indonesia telah memiliki dasar hukum perlindungan data nasabah melalui prinsip kerahasiaan bank dalam Undang-Undang Perbankan, Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Pelindungan Data Pribadi yang mewajibkan pengendali data menjaga keamanan data dan memberitahukan kegagalan pelindungan data paling lambat 3 x 24 jam. Namun implementasi perlindungan tersebut masih menghadapi kendala pada aspek pengawasan, kepatuhan, dan penegakan hukum. Dibandingkan dengan GDPR, pengaturan di Indonesia masih tertinggal dalam hal akuntabilitas, ketegasan sanksi, kewajiban notifikasi kebocoran data, dan kekuatan otoritas pengawas. Oleh karena itu, perlindungan hukum data nasabah dalam bank digital di Indonesia perlu diperkuat

melalui pengawasan yang independen, standar keamanan yang lebih ketat, serta penerapan prinsip perlindungan data yang benar-benar efektif.
Kata kunci: perlindungan data pribadi, kebocoran data, UU PDP, GDPR.

PENDAHULUAN

Teknologi yang terus berkembang saat ini telah menyebabkan banyak perubahan di banyak hal, salah satunya adalah dalam bidang perbankan. Bank tradisional yang awalnya hanya menyediakan layanan secara konvensional kini beralih ke memberikan layanan digital (Kurniawan & Yuspin, 2023), Kehadiran bank digital menjadi bagian dari transformasi tersebut, di mana seluruh aktivitas perbankan mulai dari pembukaan rekening, verifikasi identitas, transaksi keuangan, hingga komunikasi dengan nasabah dilakukan melalui sistem elektronik. Tetapi setiap informasi pribadi yang tersimpan dalam sistem digital, baik berupa identitas, riwayat transaksi, maupun data autentikasi, berpotensi menjadi sasaran kebocoran data, penyalahgunaan akses, maupun serangan siber. Di Indonesia perlindungan data nasabah memiliki dasar hukum yang bersumber dari prinsip kerahasiaan bank sebagaimana diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, yang mewajibkan bank merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya. Kemudian terdapat Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang mewajibkan pengendali data pribadi melindungi keamanan data yang diprosesnya dan memberitahukan kegagalan pelindungan data kepada subjek data paling lambat 3 x 24 jam sejak diketahui.

Apabila dibandingkan dengan General Data Protection Regulation (GDPR) di Uni Eropa, terlihat bahwa rezim perlindungan data di Eropa telah dirumuskan secara lebih rinci dan berorientasi pada akuntabilitas. GDPR menempatkan perlindungan data pribadi sebagai hak fundamental, mewajibkan informasi yang jelas kepada subjek data, membatasi pemrosesan berdasarkan tujuan yang sah, serta mengharuskan notifikasi kebocoran data kepada otoritas pengawas paling lambat 72 jam setelah diketahui. Perbandingan ini menunjukkan bahwa kajian mengenai regulasi hukum bank digital atas kebocoran data nasabah menjadi penting untuk menilai efektivitas perlindungan hukum di Indonesia, sekaligus melihat kebutuhan penguatan implementasi, pengawasan, dan kepatuhan agar perlindungan nasabah tidak berhenti pada norma tertulis, tetapi benar-benar menghadirkan kepastian dan keamanan hukum.

Berdasarkan uraian tersebut, kajian mengenai perlindungan hukum data nasabah dalam bank digital berbasis GDPR di Indonesia menjadi relevan untuk dianalisis, terutama dalam menilai sejauh mana regulasi nasional telah mampu mengadopsi prinsip-prinsip

perlindungan data internasional. Artikel ini bertujuan untuk menganalisis regulasi hukum bank digital atas kebocoran data nasabah, perlindungan hukum terhadap kebocoran data nasabah dalam bank digital, perbandingan perlindungan data nasabah dalam bank digital uni eropa dan indonesia, serta mekanisme perlindungan data nasabah dalam bank digital berdasarkan *general data protection regulation* (gdpr) di Indonesia. Dengan demikian penelitian ini diharapkan dapat memberikan kontribusi akademik dalam pengembangan konsep perlindungan hukum data pribadi di sektor perbankan digital Indonesia yang selaras dengan standar internasional.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif atau penelitian hukum kepustakaan, yaitu penelitian yang menelaah norma-norma hukum yang berkaitan dengan perlindungan hukum data nasabah dalam bank digital. Pendekatan yang digunakan adalah pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan perbandingan (*comparative approach*). Pendekatan perundang-undangan digunakan untuk menganalisis ketentuan hukum yang mengatur kerahasiaan bank, perlindungan data pribadi, serta kewajiban pelaporan kebocoran data dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, dan ketentuan terkait bank digital. Pendekatan konseptual digunakan untuk mengkaji prinsip-prinsip perlindungan data pribadi, akuntabilitas, transparansi, keamanan data, dan hak subjek data. Sementara itu pendekatan perbandingan digunakan untuk membandingkan pengaturan perlindungan data nasabah di Indonesia dengan *General Data Protection Regulation* (GDPR) di Uni Eropa, khususnya terkait kewajiban pengendali data, notifikasi kebocoran data, serta mekanisme perlindungan hukum bagi nasabah.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang relevan, sedangkan bahan hukum sekunder meliputi buku, jurnal ilmiah, artikel, dan hasil penelitian terdahulu yang membahas perlindungan data pribadi, bank digital, serta GDPR. Adapun bahan hukum tersier digunakan untuk membantu memperjelas istilah-istilah hukum yang digunakan dalam penelitian ini. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan menelusuri literatur, regulasi, dan dokumen hukum yang berkaitan dengan topik penelitian. Selanjutnya, bahan hukum yang telah diperoleh dianalisis secara

kualitatif, yaitu dengan cara menafsirkan norma hukum, menghubungkan antar ketentuan, serta menarik kesimpulan secara logis dan sistematis guna menjawab permasalahan penelitian mengenai perlindungan hukum data nasabah dalam bank digital berbasis GDPR di Indonesia.

HASIL DAN PEBAHASAN

A. Regulasi Hukum Bank Digital atas Kebocoran Data Nasabah

Perkembangan teknologi informasi telah mendorong transformasi sektor perbankan menuju sistem layanan berbasis digital yang memungkinkan transaksi keuangan dilakukan secara cepat, efisien, dan tanpa batas ruang serta waktu. Kehadiran bank digital merupakan konsekuensi logis dari revolusi industri berbasis teknologi yang mengubah pola interaksi antara bank dan nasabah dari sistem konvensional menjadi ekosistem elektronik yang sepenuhnya bergantung pada pengolahan data digital. Dalam sistem ini, data nasabah menjadi aset utama sekaligus komponen paling rentan terhadap risiko keamanan. Digitalisasi layanan perbankan menyebabkan data pribadi nasabah tidak lagi terbatas pada dokumen fisik, melainkan tersimpan dalam jaringan sistem elektronik yang saling terhubung, termasuk cloud computing, aplikasi mobile banking, dan sistem pembayaran digital (Rini, 2025). Kondisi tersebut meningkatkan potensi ancaman kebocoran data akibat serangan siber, kegagalan sistem, kesalahan manusia, maupun penyalahgunaan akses internal. Transformasi dari bank konvensional ke bank digital tidak hanya meningkatkan efisiensi layanan, tetapi juga secara fundamental mengubah struktur risiko kebocoran data nasabah. Pada bank konvensional, pengelolaan data cenderung bersifat terpusat dan berada dalam kendali internal bank. Sebaliknya, bank digital beroperasi dalam ekosistem terbuka yang sangat bergantung pada keterlibatan pihak ketiga, seperti vendor teknologi informasi, penyedia layanan cloud computing, serta mitra fintech melalui mekanisme Open API. Kondisi ini menyebabkan data nasabah tidak lagi berada dalam satu sistem tertutup, melainkan tersebar dan diproses oleh berbagai entitas eksternal, sehingga memperbesar potensi kebocoran data secara sistemik.

Secara teknis, penggunaan Open API memungkinkan pertukaran data secara real-time antar sistem yang berbeda, namun pada saat yang sama menciptakan celah keamanan apabila tidak disertai dengan kontrol yang ketat. Setiap integrasi dengan pihak ketiga menjadi titik rawan kebocoran, baik akibat kelemahan sistem, serangan siber, maupun kegagalan pengamanan pada pihak mitra. Dengan demikian, risiko kebocoran data dalam

bank digital bukan hanya disebabkan oleh peretasan terhadap sistem internal bank, tetapi juga oleh kerentanan dalam rantai ekosistem digital yang lebih luas. Dari perspektif hukum, kondisi ini memunculkan persoalan serius terkait pembagian tanggung jawab antara bank sebagai pengendali data dengan pihak ketiga sebagai pemroses data. Dalam praktiknya, bank digital seringkali menggunakan klausul persetujuan dalam Terms and Conditions sebagai dasar untuk membenarkan pembagian data kepada pihak ketiga. Persetujuan tersebut pada umumnya bersifat formalitas administratif, di mana nasabah tidak memiliki posisi tawar yang seimbang dan tidak sepenuhnya memahami implikasi dari persetujuan yang diberikan. Akibatnya, ketika terjadi kebocoran data pada sistem pihak ketiga, bank cenderung mengalihkan tanggung jawab dengan alasan bahwa pemrosesan dilakukan oleh vendor atau mitra, serta telah memperoleh persetujuan dari nasabah. Pola ini menunjukkan adanya kecenderungan "lepas tangan" yang pada dasarnya merupakan celah hukum dalam praktik perlindungan data di Indonesia, karena tanggung jawab pengendali data menjadi tidak jelas dan berpotensi dibebankan secara tidak proporsional kepada nasabah.

Oleh karena itu, regulasi hukum yang mengatur perlindungan data nasabah menjadi elemen fundamental dalam menjaga stabilitas sistem keuangan serta mempertahankan kepercayaan publik terhadap bank digital. Dalam konteks hukum Indonesia, perlindungan terhadap data nasabah berakar pada prinsip kerahasiaan bank yang diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan sebagai perubahan atas Undang-Undang Nomor 7 Tahun 1992. Prinsip kerahasiaan bank merupakan norma dasar yang mewajibkan bank untuk menjaga informasi mengenai nasabah penyimpan dan simpanannya agar tidak diungkapkan kepada pihak lain tanpa dasar hukum yang sah. Ketentuan Pasal 40 ayat (1) menegaskan kewajiban bank untuk merahasiakan data nasabah, kecuali dalam kondisi tertentu yang secara limitatif diatur oleh undang-undang, seperti kepentingan perpajakan, penyelesaian perkara pidana, atau permintaan otoritas yang berwenang. Norma ini mencerminkan hubungan kepercayaan (fiduciary relationship) antara bank dan nasabah, di mana bank memegang tanggung jawab hukum sekaligus moral untuk melindungi informasi finansial nasabah. Dalam konteks bank digital, prinsip kerahasiaan bank tidak hanya berkaitan dengan kerahasiaan informasi secara administratif, tetapi juga mencakup kewajiban menjaga keamanan sistem teknologi yang menyimpan data tersebut.

Seiring berkembangnya teknologi digital, perlindungan data nasabah tidak lagi cukup hanya bertumpu pada konsep kerahasiaan bank. Negara kemudian memperkuat kerangka hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang memberikan pengaturan lebih komprehensif mengenai pengelolaan data pribadi. UU ini menempatkan data pribadi sebagai bagian dari hak privasi yang harus dilindungi oleh negara. Dalam sistem bank digital, lembaga perbankan dikualifikasikan sebagai pengendali data pribadi karena memiliki kewenangan menentukan tujuan dan proses pengolahan data nasabah (Bastari, 2026). Sebagai pengendali data, bank memiliki kewajiban hukum untuk memastikan pemrosesan data dilakukan secara sah, transparan, dan terbatas pada tujuan yang jelas. Kewajiban tersebut menegaskan bahwa bank tidak hanya bertanggung jawab atas penggunaan data, tetapi juga atas keamanan seluruh siklus pengolahan data, mulai dari pengumpulan, penyimpanan, penggunaan, hingga pemusnahan data.

Pasal 35 UU Perlindungan Data Pribadi mengatur bahwa pengendali data wajib melindungi data pribadi dari akses yang tidak sah, pengungkapan tanpa izin, perubahan data, maupun kehilangan data. Ketentuan ini secara langsung menempatkan tanggung jawab keamanan pada bank digital apabila terjadi kebocoran data nasabah. Bank wajib menerapkan langkah teknis dan organisatoris yang memadai, termasuk penggunaan sistem enkripsi, autentikasi berlapis, manajemen akses berbasis otorisasi, serta audit keamanan sistem secara berkala. Dalam perspektif hukum modern, kewajiban tersebut mencerminkan prinsip accountability, yaitu tanggung jawab aktif lembaga pengelola data untuk mencegah risiko pelanggaran, bukan sekadar bertindak setelah terjadi kerugian.

Selain kewajiban perlindungan data, UU PDP juga mengatur mekanisme tanggung jawab pascakebocoran data melalui kewajiban notifikasi kepada subjek data pribadi. Pasal 46 mengharuskan pengendali data memberitahukan kepada pemilik data paling lambat 3 x 24 jam sejak ditemukannya kegagalan perlindungan data. Ketentuan ini memiliki fungsi penting dalam menciptakan transparansi serta memberikan kesempatan kepada nasabah untuk melakukan langkah mitigasi, seperti mengganti kata sandi, memblokir rekening, atau menghindari potensi penipuan digital. Regulasi ini menunjukkan perubahan paradigma hukum dari pendekatan tertutup menuju pendekatan perlindungan berbasis hak individu.

Di samping UU PDP, aspek keamanan sistem elektronik bank digital juga diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah

melalui Undang-Undang Nomor 19 Tahun 2016. Pasal 15 UU ITE menegaskan bahwa setiap penyelenggara sistem elektronik wajib menyelenggarakan sistem secara andal, aman, dan bertanggung jawab atas operasionalnya. Ketentuan ini memperluas tanggung jawab bank digital tidak hanya sebagai lembaga keuangan, tetapi juga sebagai penyelenggara sistem elektronik. Artinya, kegagalan sistem keamanan yang menyebabkan kebocoran data dapat dikualifikasikan sebagai pelanggaran kewajiban hukum apabila bank tidak menerapkan standar keamanan yang layak. Dengan demikian, tanggung jawab hukum bank digital mencakup aspek teknis teknologi informasi, bukan semata aspek administratif perbankan.

Pengawasan terhadap implementasi perlindungan data dalam sektor perbankan dilakukan oleh Otoritas Jasa Keuangan (OJK) sebagai regulator dan pengawas industri jasa keuangan (Rohmah, 2025). OJK memiliki kewenangan menetapkan standar manajemen risiko teknologi informasi dan perlindungan konsumen dalam layanan keuangan digital. Melalui berbagai regulasi, termasuk Peraturan OJK mengenai perlindungan konsumen sektor jasa keuangan, bank diwajibkan menjaga kerahasiaan serta keamanan data konsumen sebagai bagian dari prinsip perlindungan konsumen. Pengawasan ini bertujuan memastikan bank digital menerapkan tata kelola teknologi informasi yang baik (good IT governance) dan manajemen risiko siber secara berkelanjutan.

Meskipun kerangka regulasi telah tersedia secara relatif komprehensif, efektivitas perlindungan hukum terhadap kebocoran data nasabah masih menghadapi berbagai tantangan. Salah satu persoalan utama adalah meningkatnya kompleksitas serangan siber yang berkembang lebih cepat dibandingkan adaptasi regulasi. Serangan ransomware, phishing, dan eksploitasi celah keamanan menunjukkan bahwa keamanan digital tidak hanya bergantung pada regulasi, tetapi juga pada kesiapan teknis dan budaya keamanan dalam organisasi perbankan. Banyak kasus kebocoran data terjadi bukan karena ketiadaan aturan, melainkan lemahnya implementasi dan pengawasan internal.

B. Perlindungan Hukum terhadap Kebocoran Data Nasabah dalam Bank Digital

Perlindungan terhadap data nasabah merupakan salah satu aspek fundamental dalam penyelenggaraan layanan perbankan, khususnya dalam sistem bank digital yang mengandalkan teknologi informasi dalam pengelolaan data dan transaksi keuangan. Digitalisasi layanan perbankan menyebabkan data nasabah tidak hanya disimpan dalam bentuk dokumen fisik, tetapi juga dalam sistem elektronik yang terhubung dengan jaringan

digital sehingga kondisi ini meningkatkan risiko terjadinya kebocoran data akibat serangan siber, kesalahan sistem, maupun penyalahgunaan akses oleh pihak yang tidak berwenang (Ervian dkk., 2025). Oleh karena itu, keberadaan perlindungan hukum yang efektif menjadi sangat penting untuk menjamin keamanan data nasabah serta menjaga kepercayaan masyarakat terhadap sistem perbankan digital. Dalam sistem hukum Indonesia, perlindungan terhadap data nasabah pada dasarnya berakar pada prinsip kerahasiaan bank sebagaimana diatur dalam UU No. 10 Tahun 1998 tentang Perubahan atas UU No. 7 Tahun 1992 tentang Perbankan (Alia, 2024). Prinsip ini menegaskan bahwa bank memiliki kewajiban untuk menjaga kerahasiaan informasi mengenai nasabah penyimpan dan simpanannya. Ketentuan tersebut tercantum dalam Pasal 40 ayat (1) yang menyatakan bahwa bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya kecuali dalam kondisi tertentu yang ditentukan oleh UU. Ketentuan ini menunjukkan bahwa secara normatif bank memiliki tanggung jawab hukum untuk melindungi informasi yang dimiliki nasabah dari penyalahgunaan maupun pengungkapan kepada pihak yang tidak berwenang. Oleh karena itu, perlindungan hukum terhadap data nasabah juga diatur dalam UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang memberikan kerangka hukum yang lebih komprehensif terkait pengelolaan data pribadi. Dalam UU tersebut ditegaskan bahwa setiap pengendali data pribadi wajib memproses data secara sah, transparan, serta menjamin keamanan data yang dikelola.

Bank digital memiliki lembaga perbankan bertindak sebagai pengendali data pribadi yang memiliki kewajiban hukum untuk melindungi data nasabah dari pemrosesan yang tidak sah, termasuk kebocoran data. Pasal 35 UU Perlindungan Data Pribadi menegaskan bahwa pengendali data pribadi wajib melindungi data pribadi dari akses yang tidak sah, pengungkapan yang tidak sah, maupun kehilangan data. Kewajiban tersebut mengharuskan bank digital untuk menerapkan langkah-langkah teknis dan organisasi yang memadai guna memastikan keamanan data nasabah yang tersimpan dalam sistem elektronik. Langkah-langkah tersebut dapat berupa penerapan sistem keamanan siber, pengendalian akses terhadap data, enkripsi data, serta pengawasan terhadap aktivitas pengolahan data dalam sistem perbankan digital. Selain itu, perlindungan hukum terhadap nasabah juga tercermin melalui mekanisme pemberitahuan apabila terjadi kebocoran data. Dalam Pasal 46 UU Perlindungan Data Pribadi diatur bahwa pengendali data pribadi wajib memberitahukan kepada subjek data pribadi mengenai terjadinya kegagalan perlindungan

data pribadi paling lambat 3 x 24 jam sejak diketahui terjadinya insiden tersebut. Ketentuan ini merupakan bentuk perlindungan hukum yang bertujuan untuk memberikan transparansi kepada nasabah serta memungkinkan mereka mengambil langkah-langkah mitigasi terhadap potensi kerugian yang dapat timbul akibat kebocoran data. Di samping pengaturan mengenai perlindungan data pribadi, aspek keamanan sistem elektronik yang digunakan dalam layanan bank digital juga diatur dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah melalui UU No. 19 Tahun 2016 tentang Perubahan atas UU Informasi dan Transaksi Elektronik. Dalam Pasal 15 UU tersebut ditegaskan bahwa setiap penyelenggara sistem elektronik wajib menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik yang digunakan. Ketentuan ini mengharuskan bank digital sebagai penyelenggara sistem elektronik untuk memastikan bahwa sistem teknologi informasi yang digunakan memiliki tingkat keamanan yang memadai guna mencegah terjadinya kebocoran data nasabah.

Selain itu, pengawasan terhadap penerapan perlindungan data dalam sektor perbankan juga dilakukan oleh Otoritas Jasa Keuangan sebagai lembaga yang memiliki kewenangan untuk mengatur dan mengawasi kegiatan jasa keuangan di Indonesia. Otoritas ini menetapkan berbagai ketentuan mengenai manajemen risiko teknologi informasi serta tata kelola keamanan sistem pada lembaga perbankan, termasuk bank digital (Aziz & Zaidan, 2025). Melalui mekanisme pengawasan tersebut, bank diwajibkan untuk menerapkan sistem keamanan informasi yang memadai guna melindungi data nasabah dari ancaman kebocoran maupun penyalahgunaan data. Pengaturan tersebut antara lain tercermin dalam PJOK No, 6/PJOK.07/2022 yang menegaskan kewajiban pelaku usaha jasa keuangan untuk menjaga kerahasiaan serta keamanan data dan informasi konsumen. Meskipun kerangka hukum yang mengatur perlindungan data nasabah dalam sistem perbankan digital telah tersedia, efektivitas perlindungan tersebut masih menghadapi sejumlah tantangan. Salah satu tantangan utama adalah meningkatnya kompleksitas ancaman keamanan siber yang dapat menargetkan sistem perbankan digital (Wijaya, 2025). Selain itu, mekanisme penegakan hukum terhadap pelanggaran perlindungan data masih memerlukan penguatan agar mampu memberikan perlindungan yang optimal bagi nasabah. Kondisi ini menunjukkan bahwa perlindungan hukum terhadap kebocoran data nasabah tidak hanya bergantung pada keberadaan regulasi, tetapi juga pada efektivitas

implementasi serta sistem pengawasan yang mampu menjamin kepatuhan lembaga perbankan terhadap standar perlindungan data yang berlaku.

C. Perbandingan Perlindungan Data Nasabah dalam Bank Digital Uni Eropa dan Indonesia

Perbandingan antara sistem perlindungan data nasabah di Uni Eropa dan Indonesia merupakan perbedaan yang cukup mendasar antara dua kerangka hukum tersebut. Uni Eropa telah memiliki regulasi perlindungan data yang komprehensif sejak disahkannya General Data Protection Regulation (GDPR) atau Regulation (EU) 2016/679 oleh Parlemen Eropa dan Dewan Uni Eropa pada tanggal 27 April 2016, yang mulai berlaku secara penuh pada 25 Mei 2018. Sebagaimana dinyatakan dalam Pasal 1 GDPR, regulasi ini bertujuan untuk melindungi hak-hak fundamental dan kebebasan setiap orang, khususnya hak atas perlindungan data pribadi, sekaligus memastikan kebebasan arus data pribadi di seluruh wilayah Uni Eropa. Filosofi dasar GDPR bertumpu pada pengakuan bahwa perlindungan data bukan semata-mata kewajiban administratif, melainkan merupakan hak asasi manusia yang harus dijamin oleh negara. Indonesia, di sisi lain, baru mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) setelah bertahun-tahun mengandalkan regulasi yang tersebar di berbagai ketentuan sektoral, seperti Peraturan Bank Indonesia (PBI) dan Peraturan Otoritas Jasa Keuangan (POJK). Kondisi ini mencerminkan tingkat kematangan yang berbeda secara signifikan dalam hal tata kelola data antara kedua yurisdiksi, meskipun keduanya mengakui bahwa perlindungan data nasabah bank digital merupakan prioritas yang tidak dapat diabaikan.

Dari segi definisi dan ruang lingkup, GDPR memberikan cakupan yang sangat luas terhadap apa yang dimaksud dengan data pribadi. Berdasarkan Pasal 4 angka 1 GDPR, data pribadi didefinisikan sebagai segala informasi yang berkaitan dengan orang perseorangan yang telah teridentifikasi atau dapat diidentifikasi, termasuk di dalamnya nama, nomor identifikasi, data lokasi, pengenal daring, hingga faktor-faktor yang bersifat fisik, fisiologis, genetik, mental, ekonomi, budaya, maupun identitas sosial. Kemudian pasal 9 GDPR secara eksplisit mengidentifikasi kategori data yang mendapat perlindungan lebih ketat, yaitu data yang mengungkapkan asal-usul ras atau etnis, pandangan politik, keyakinan agama atau filosofi, keanggotaan serikat pekerja, serta data genetik, data biometrik, data kesehatan, dan data kehidupan seksual. Kategori data khusus ini dilarang untuk diproses kecuali dalam kondisi-kondisi tertentu yang telah diatur secara limitatif.

Dalam konteks bank digital, cakupan ini secara otomatis melindungi seluruh data nasabah, mulai dari data identitas, riwayat transaksi keuangan, pola perilaku penggunaan aplikasi, hingga data biometrik yang semakin umum digunakan sebagai metode autentikasi. UU PDP Indonesia juga mengadopsi definisi yang relatif luas mengenai data pribadi dan membedakan antara data pribadi umum dan data pribadi yang bersifat spesifik (sensitif), namun pengaturan teknisnya yang lebih rinci masih menunggu penerbitan peraturan pelaksana dari pemerintah.

Perbedaan yang paling mencolok antara GDPR dan regulasi Indonesia terletak pada kejelasan dan ketegasan prinsip-prinsip dasar pemrosesan data. Pasal 5 GDPR merinci tujuh prinsip yang wajib dipatuhi oleh setiap pengendali data, yakni: *lawfulness, fairness, and transparency* (data harus diproses secara sah, adil, dan transparan); *purpose limitation* (data hanya boleh dikumpulkan untuk tujuan yang spesifik, eksplisit, dan sah); data *minimisation* (data yang dikumpulkan harus memadai, relevan, dan terbatas sesuai tujuan); *accuracy* (data harus akurat dan senantiasa diperbarui); *storage limitation* (data tidak boleh disimpan lebih lama dari yang diperlukan); serta *integrity and confidentiality* (data harus diproses dengan menjamin keamanan yang memadai). Selain keenam prinsip tersebut, Pasal 5 ayat (2) GDPR menambahkan prinsip *accountability*, yaitu kewajiban pengendali data untuk dapat membuktikan secara aktif bahwa seluruh pemrosesan data telah dilakukan sesuai dengan ketentuan GDPR. Prinsip akuntabilitas ini merupakan pergeseran paradigmatik yang sangat signifikan: tidak cukup hanya mematuhi ketentuan, pengendali harus mampu mendokumentasikan dan membuktikan kepatuhannya. Pendekatan ini memperkuat komitmen Eropa terhadap teknologi yang berpusat pada manusia, di mana inovasi digital tidak hanya mendorong pertumbuhan ekonomi tetapi juga meningkatkan hak-hak dasar, privasi nasional, dan kesadaran lingkungan .Komitmen Eropa terhadap teknologi yang berpusat pada manusia, di mana inovasi digital tidak hanya mendorong pertumbuhan ekonomi tetapi juga meningkatkan hak-hak dasar, privasi nasional, dan kesadaran lingkungan.(Pd & Tefa, 2026) Bagi bank digital yang beroperasi di Uni Eropa, hal ini berarti kewajiban untuk membuat kebijakan perlindungan data yang terperinci, melakukan penilaian dampak perlindungan data (Data Protection Impact Assessment/DPIA), dan menyimpan catatan seluruh aktivitas pemrosesan data.

Aspek penting lainnya adalah ketentuan mengenai dasar hukum pemrosesan data dan hak-hak yang dimiliki nasabah sebagai subjek data. GDPR menetapkan enam dasar hukum yang sah untuk pemrosesan data dalam Pasal 6, yaitu: persetujuan subjek data,

pelaksanaan kontrak, kepatuhan terhadap kewajiban hukum, perlindungan kepentingan vital, pelaksanaan tugas kepentingan publik, dan kepentingan sah (legitimate interest) pengendali. Berkenaan dengan persetujuan, Pasal 7 GDPR menetapkan standar yang sangat tinggi: persetujuan harus diberikan secara bebas, spesifik, terinformasi, dan tidak ambigu melalui pernyataan atau tindakan afirmatif yang jelas. Nasabah juga berhak menarik kembali persetujuannya kapan saja tanpa syarat, dan penarikan tersebut tidak boleh lebih sulit dari pemberian persetujuan itu sendiri. Lebih dari itu, Bab III GDPR (Pasal 12 hingga 22) memberikan seperangkat hak yang komprehensif kepada nasabah, meliputi hak untuk mengakses data mereka sendiri, hak untuk meminta rektifikasi data yang tidak akurat, hak untuk meminta penghapusan data atau right to be forgotten, hak untuk membatasi pemrosesan, hak portabilitas data yang memungkinkan nasabah memindahkan data keuangan mereka dari satu lembaga ke lembaga lain, serta hak untuk menolak keputusan yang sepenuhnya diambil berdasarkan pemrosesan otomatis termasuk profiling. Keseluruhan hak ini wajib dapat diakses nasabah secara gratis, dan bank digital wajib merespons setiap permintaan nasabah dalam jangka waktu satu bulan.

Dalam hal tata kelola kelembagaan dan kewajiban teknis, GDPR menetapkan sejumlah ketentuan yang jauh lebih terperinci dibandingkan regulasi Indonesia. Pasal 37 GDPR mewajibkan penunjukan Data Protection Officer (DPO) oleh organisasi yang secara rutin dan sistematis melakukan pemrosesan data dalam skala besar, termasuk lembaga keuangan dan bank digital. DPO bertanggung jawab memantau kepatuhan internal, memberikan saran terkait DPIA, serta menjadi titik kontak antara organisasi dan otoritas pengawas. Selain itu, Pasal 33 dan 34 GDPR menetapkan kewajiban notifikasi pelanggaran data yang sangat ketat: apabila terjadi kebocoran data, bank digital wajib melaporkannya kepada otoritas pengawas yang berwenang paling lambat 72 jam setelah mengetahui terjadinya insiden tersebut. Apabila pelanggaran berpotensi menimbulkan risiko tinggi bagi hak dan kebebasan nasabah, bank digital juga wajib memberitahukan hal tersebut langsung kepada nasabah yang terdampak tanpa penundaan yang tidak wajar. Ketentuan ini sangat penting karena memungkinkan nasabah segera mengambil langkah-langkah perlindungan diri, misalnya mengganti kata sandi atau memantau aktivitas rekening mereka. Di Indonesia, kewajiban notifikasi pelanggaran data telah diatur dalam UU PDP, namun belum ada ketentuan yang secara eksplisit menetapkan batas waktu 72 jam sebagaimana standar GDPR, dan mekanisme notifikasi langsung kepada nasabah belum sepenuhnya diimplementasikan secara konsisten oleh industri perbankan digital.

Pengawasan di Indonesia pun masih terbagi antara OJK dan Bank Indonesia, menimbulkan potensi tumpang tindih dan inefisiensi dalam penegakan hukum perlindungan data, berbeda dengan GDPR yang mewajibkan setiap negara anggota membentuk satu otoritas pengawas independen dengan wewenang penuh berdasarkan Pasal 51 GDPR.

Dari perspektif sanksi dan penegakan hukum, perbedaan antara GDPR dan regulasi Indonesia semakin terasa signifikan. Pasal 83 GDPR membagi sanksi administratif ke dalam dua tingkatan yang sangat besar. Tingkatan pertama mencakup denda hingga EUR 10.000.000 atau 2% dari total omset tahunan global perusahaan (mana yang lebih tinggi), berlaku untuk pelanggaran terhadap kewajiban teknis seperti keamanan data, kewajiban DPO, dan kewajiban DPIA. Tingkatan kedua mencakup denda hingga EUR 20.000.000 atau 4% dari total omset tahunan global (mana yang lebih tinggi), berlaku untuk pelanggaran terhadap prinsip-prinsip dasar pemrosesan data, hak-hak subjek data, dan ketentuan transfer data ke negara ketiga. Mekanisme penetapan denda berbasis persentase omset global ini memastikan bahwa sanksi tetap signifikan dan memberikan efek jera bahkan bagi perusahaan teknologi keuangan atau bank digital raksasa sekalipun. Selain itu, Pasal 82 GDPR menjamin hak kompensasi bagi nasabah yang mengalami kerugian baik materil maupun non-materil akibat pelanggaran GDPR, sehingga membuka jalur ganti rugi yang nyata bagi korban.

Pembentukan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan suatu langkah maju dalam upaya memperkuat sistem perlindungan data pribadi di Indonesia. Regulasi ini telah menetapkan standar hukum terkait pengumpulan, pemrosesan, dan penyimpanan data pribadi (Azizi, 2026). Undang-undang ini mengadopsi sejumlah prinsip yang berasal dari *General Data Protection Regulation* (GDPR) di Uni Eropa, seperti prinsip keabsahan dalam pemrosesan data, hak untuk mengakses dan menghapus data, serta kewajiban pelaporan atas kebocoran data. Implementasi UU PDP masih menghadapi berbagai kendala, antara lain rendahnya tingkat kesadaran masyarakat terhadap hak-haknya, belum optimalnya kesiapan institusi pengendali data, serta keterbatasan infrastruktur dan sumber daya manusia di bidang keamanan siber.

Uni Eropa (UE) mengimplementasikan GDPR sebagai upaya regulasi perlindungan data pribadi yang komprehensif pada tahun 2018 (Permana dkk., 2026). *General Data Protection Regulation* (GDPR) merupakan regulasi yang mengatur secara komprehensif mengenai bagaimana data pribadi individu dikumpulkan, diakses, dan

dikelola oleh pihak-pihak tertentu. Ketentuan ini berlaku secara luas dan mengikat tidak hanya instansi pemerintah, tetapi juga perusahaan dan organisasi, sepanjang mereka memproses data pribadi yang berkaitan dengan individu di Uni Eropa. Sebagai salah satu regulasi perlindungan data yang paling ketat, GDPR bertujuan untuk menjamin keamanan data pribadi serta mencegah berbagai bentuk kejahatan, seperti kebocoran data, penyalahgunaan data pribadi, dan kejahatan siber yang dapat merugikan pemilik data. Untuk mencapai tujuan tersebut, GDPR menetapkan prinsip-prinsip standar dalam pengelolaan data pribadi, termasuk pengaturan yang rinci mengenai proses pengumpulan dan pemrosesan data.

Dalam konteks perbankan digital, ketentuan GDPR mengharuskan bank untuk memberikan informasi yang jelas kepada nasabah mengenai proses pemrosesan data serta memperoleh persetujuan secara eksplisit, khususnya terkait penggunaan data sensitif seperti data biometrik. Mengatur mengenai pemrosesan data pribadi haruslah mendapatkan persetujuan dari pihak pemilik data, hal ini sejalan dengan hak pemilik data dalam aturan tersebut (Syarifah dkk., 2024). Persetujuan tersebut harus diberikan secara sadar, dapat dicabut sewaktu-waktu, dan seluruh prosesnya wajib dicatat oleh pihak bank sebagai bentuk akuntabilitas.

Jika dibandingkan, ketentuan Pasal 28 General Data Protection Regulation (GDPR) secara tegas menutup celah praktik “lepas tangan” yang sering terjadi dalam ekosistem bank digital. Pasal tersebut mewajibkan setiap pengendali data untuk hanya menggunakan pihak pemroses yang memberikan jaminan perlindungan data yang memadai, serta mengikat hubungan tersebut dalam perjanjian hukum yang rinci dan mengikat (data processing agreement). Dalam skema ini, tanggung jawab utama tetap berada pada pengendali data, sehingga keterlibatan pihak ketiga tidak dapat dijadikan alasan untuk menghindari pertanggungjawaban apabila terjadi kebocoran data.

Sebaliknya, dalam kerangka regulasi di Indonesia, khususnya pengaturan oleh Otoritas Jasa Keuangan (OJK), kewajiban terkait penggunaan pihak ketiga dalam pengelolaan data nasabah masih bersifat umum dan berfokus pada prinsip kehati-hatian serta manajemen risiko teknologi informasi. Pengaturan tersebut belum secara tegas mengatur batas tanggung jawab hukum antara bank sebagai pengendali data dengan pihak ketiga sebagai pemroses data, terutama dalam konteks kegagalan perlindungan data.

Akibatnya, dalam praktiknya masih terdapat ruang bagi bank digital untuk mengalihkan tanggung jawab kepada vendor atau mitra teknologi dengan dasar bahwa

pemrosesan dilakukan oleh pihak lain atau telah disetujui oleh nasabah melalui Terms and Conditions. Kondisi ini berbeda secara fundamental dengan pendekatan GDPR yang menempatkan prinsip akuntabilitas sebagai dasar utama, di mana pengendali data tetap memikul tanggung jawab penuh atas seluruh rantai pemrosesan data, termasuk yang dilakukan oleh pihak ketiga.

Untuk memberikan gambaran yang lebih sistematis mengenai persamaan dan perbedaan antara Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia dengan *General Data Protection Regulation* (GDPR) di Uni Eropa, diperlukan penyajian dalam bentuk tabel perbandingan. Tabel ini bertujuan untuk mengidentifikasi aspek-aspek utama dalam perlindungan data pribadi, sekaligus menilai sejauh mana kesesuaian dan perbedaan antara kedua rezim hukum tersebut, baik dari sisi substansi maupun implementasinya.

Aspek	UU No. 27 Tahun 2022 (UU PDP - Indonesia)	GDPR (Uni Eropa)
Tujuan Regulasi	Undang-Undang PDP bertujuan untuk memberikan perlindungan menyeluruh terhadap data pribadi warga negara Indonesia dalam berbagai sektor.	GDPR bertujuan untuk melindungi data pribadi warga Uni Eropa secara komprehensif dengan standar perlindungan yang tinggi.
Cakupan Wilayah (Ekstrateritorial)	UU PDP berlaku bagi setiap pihak, baik di dalam maupun di luar wilayah Indonesia, yang memproses data pribadi warga negara Indonesia.	GDPR memiliki cakupan ekstrateritorial yang mengikat setiap entitas di luar Uni Eropa yang memproses data warga Uni Eropa.

	UU PDP membedakan antara data pribadi umum dan data pribadi spesifik yang bersifat sensitif.	UU PDP membedakan antara data pribadi umum dan data pribadi spesifik yang bersifat sensitif.
Sanksi	Lebih ringan (maksimal 2% pendapatan atau Rp6 miliar) + ada sanksi pidana	Sangat berat (hingga €20 juta atau 4% omzet global)
Penegakan Hukum	Otoritas pengawas belum sepenuhnya terbentuk dan masih dalam tahap pengembangan	Didukung otoritas pengawas independen yang sudah mapan di tiap negara UE
Hak Subjek Data	Secara normatif ada, tapi implementasi masih terbatas	Sangat kuat dan implementatif (right to be forgotten, data portability berjalan efektif)
Data Protection Impact Assessment (DPIA)	Sudah diatur, tapi belum seketat dan sejelas GDPR	Wajib dan detail jika berisiko tinggi
Data Protection Officer (DPO)	Diatur, tetapi implementasi masih berkembang	Wajib dalam kondisi tertentu, dengan standar jelas
Transfer Data Lintas Negara	Diizinkan, tapi mekanisme “kesetaraan perlindungan” belum jelas	Ketat (harus ada adequacy decision, SCC, BCR)

Consent (Persetujuan)	Prinsip sama, tapi praktik masih sering formalitas	Harus bebas, spesifik, terinformasi, dan tidak ambigu
Kesiapan Sistem	Masih dalam tahap transisi dan penyesuaian	Sudah matang (hukum, teknologi, dan pengawasan)

Tabel tersebut menunjukkan bahwa meskipun secara normatif kerangka hukum di Indonesia telah mengadopsi berbagai prinsip yang sejalan dengan *General Data Protection Regulation* (GDPR), implementasinya masih menghadapi kesenjangan yang signifikan. Dalam praktiknya, mekanisme perlindungan data seperti persetujuan (*consent*), transparansi pemrosesan, serta pengendalian akses data seringkali belum berjalan secara substantif, melainkan cenderung bersifat formalitas administratif. Kondisi ini terlihat dari masih maraknya kebocoran data dan rendahnya kesadaran nasabah terhadap hak-haknya sebagai subjek data, yang menunjukkan bahwa perlindungan data belum sepenuhnya berorientasi pada kepentingan individu. Salah satu contoh konkret yang menunjukkan lemahnya implementasi perlindungan data pribadi di sektor perbankan digital di Indonesia adalah kasus kebocoran data yang menimpa Bank Jatim dan BRI Life pada tahun 2021, serta dugaan serangan siber terhadap Bank Syariah Indonesia pada tahun 2023. Dalam kasus terakhir, gangguan sistem yang menyebabkan layanan perbankan lumpuh selama beberapa hari diduga kuat merupakan akibat serangan ransomware yang kemudian diklaim oleh kelompok peretas LockBit. Kelompok tersebut bahkan menyatakan telah berhasil mencuri sekitar 1,5 terabyte data, yang mencakup kurang lebih 15 juta data pribadi nasabah dan pegawai, termasuk informasi sensitif seperti identitas pribadi, nomor rekening, data transaksi, hingga informasi keuangan lainnya.

Jika dibandingkan dengan standar GDPR, perlindungan data nasabah di Indonesia masih lemah pada aspek penegakan hukum dan pengawasan. GDPR tidak hanya mengatur kewajiban secara rinci, tetapi juga didukung oleh otoritas pengawas yang kuat dan sanksi yang tegas, sehingga mendorong kepatuhan yang lebih tinggi. Sebaliknya, di Indonesia, keterbatasan kelembagaan dan belum optimalnya regulasi teknis menyebabkan mekanisme perlindungan data belum berjalan secara efektif. Penguatan perlindungan data

pribadi nasabah perbankan di Indonesia tidak cukup hanya dengan mengadopsi norma-norma yang sejalan dengan General Data Protection Regulation, tetapi harus diikuti dengan penerapan mekanisme penegakan yang setara secara substantif yang mencakup penguatan prinsip consent yang benar-benar bebas dan terinformasi, kewajiban transparansi pemrosesan data secara real-time, penerapan Data Protection Impact Assessment (DPIA) secara ketat, serta penunjukan Data Protection Officer (DPO) yang independen dan profesional. Selain itu, diperlukan pembentukan otoritas pengawas yang kuat dan independen, disertai dengan mekanisme penegakan hukum yang tegas melalui sanksi administratif yang proporsional dan efektif. Dengan mengadopsi model tersebut secara komprehensif, perlindungan data pribadi nasabah bank digital di Indonesia tidak hanya bersifat formalitas regulatif, tetapi mampu memberikan jaminan keamanan, kepastian hukum, serta meningkatkan kepercayaan publik terhadap sistem keuangan digital.. Tanpa transformasi menuju model tersebut, perlindungan data pribadi dalam sektor perbankan digital di Indonesia akan tetap bersifat semu dan tidak mampu menjawab risiko kebocoran serta penyalahgunaan data yang semakin kompleks.

KESIMPULAN

Berdasarkan pembahasan tersebut, dapat disimpulkan bahwa perkembangan bank digital telah membawa kemudahan sekaligus meningkatkan risiko kebocoran data nasabah, sehingga perlindungan hukum terhadap data pribadi menjadi semakin penting. Di Indonesia, perlindungan data nasabah telah memiliki dasar hukum melalui prinsip kerahasiaan bank dalam UU Perbankan, UU ITE, serta UU Perlindungan Data Pribadi yang mewajibkan pengendali data menjaga keamanan data dan memberitahukan kegagalan pelindungan data kepada subjek data paling lambat 3 x 24 jam. Namun, efektivitas perlindungan tersebut masih menghadapi kendala pada aspek implementasi, pengawasan, dan penegakan hukum, terutama dalam menghadapi ancaman siber yang terus berkembang.

Dibandingkan dengan GDPR di Uni Eropa, regulasi Indonesia memang telah mengadopsi sejumlah prinsip yang sejalan, tetapi masih tertinggal dalam hal kedetailan pengaturan, akuntabilitas, kelembagaan pengawas, serta kekuatan sanksi. GDPR memberikan perlindungan yang lebih komprehensif melalui prinsip transparansi, pembatasan tujuan, akuntabilitas, hak subjek data yang kuat, kewajiban notifikasi kebocoran dalam 72 jam, dan sanksi yang tegas. Oleh karena itu perlindungan hukum data nasabah dalam bank digital di Indonesia perlu diperkuat tidak hanya melalui pembaruan norma, tetapi juga melalui

pengawasan yang independen, kepatuhan yang konsisten, serta penerapan standar keamanan data yang lebih ketat agar benar-benar memberikan kepastian hukum, keamanan, dan perlindungan yang optimal bagi nasabah.

DAFTAR PUSTAKA

ANALISIS HUKUM PERLINDUNGAN DATA PRIBADI TERHADAP NASABAH BADAN PADA PERBANKAN DI INDONESIA DALAM PERSPEKTIF UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI | Law and Communication Journal. (t.t.). Diambil 7 April 2026, dari https://jurnalsjam.com/lcj/article/view/28

Art. 6 GDPR – Lawfulness of processing. (t.t.). General Data Protection Regulation (GDPR). Diambil 7 April 2026, dari https://gdpr-info.eu/art-6-gdpr/

Aziz, A. S., & Zaidan, M. A. (2025). Perlindungan Hukum Nasabah Terhadap Penyalahgunaan Data Pribadi oleh Pihak Ketiga dalam Kerja Sama Perbankan Digital. Ekopedia: Jurnal Ilmiah Ekonomi, 1(2), 120–129. https://doi.org/10.63822/qwcqac23

DIGITAL BANKING DAN KUALITAS LAYANAN DIGITAL (MENDUKUNG KEMUDAHAN, KEPUASAN ... - Rini Rahayu Kurniati, Sri Nuring Wahyu, Muhammad Rafli Daidan—Google Buku. (t.t.). Diambil 7 April 2026, dari https://books.google.co.id/books?hl=id&lr=&id=3b1nEQAAQBAJ&oi=fnd&pg=PR1&dq=Kurniati,+R.+R.,+Wahyu,+S.+N.,+%26+Daidan,+M.+R.+(2025).+Digital+Banking+dan+Kualitas+Layanan+Digital+(Mendukung+Kemudahan,+Kepuasan+Nasabah+Bertransaksi).+Unisma+Press.&ots=0FMV6T5z5W&sig=uEaECqdXTjR_DLVJALvfLEpNKR0&redir_esc=y#v=onepage&q&f=false

Ervian, A. N., Hamzah, & S, S. A. (2025). Perlindungan Hukum terhadap Nasabah atas Kebocoran Data Pribadi dalam Layanan Perbankan Digital di Indonesia. Al-Zayn : Jurnal Ilmu Sosial & Hukum, 3(6), 8785–8793. https://doi.org/10.61104/alz.v3i6.2783

Garuda—Garba Rujukan Digital. (t.t.). Diambil 7 April 2026, dari https://garuda.kemdiktisaintek.go.id/documents/detail/4749474

Kurniawan, D., & Yuspin, W. (2023). Menggagas Pendirian Bank Digital di Indonesia: Sebuah Telaah Yuridis. Jurnal Supremasi, 1–14. https://doi.org/10.35457/supremasi.v13i1.2158

Pd, & Tefa, S. (2026). EKONOMI DIGITAL Dampak dan Peluang di Era Globalisasi.

Perlindungan Data Pribadi dalam Ekosistem Kecerdasan Buatan: Tantangan Hukum dan Etika di Indonesia | SEIKAT: Jurnal Ilmu Sosial, Politik dan Hukum. (t.t.). Diambil 7 April 2026, dari https://ejournal.45mataram.ac.id/index.php/seikat/article/view/1696

Perlindungan Hukum Nasabah Bank Digital Syariah di Indonesia yang Berkepastian Hukum | Jurnal Ilmu Hukum, Humaniora dan Politik. (t.t.). Diambil 7 April 2026, dari https://dinastirev.org/JIHHP/article/view/4087

Permana, R. S. M., Sumarlina, E. S. N., Darsa, U. A., & Rasyad, A. (2026). Jejak Transformasi Budaya: Evolusi Komunikasi Manusia dari Era Lisan hingga Algoritma Digital. Jurnal Humanitas: Katalisator Perubahan Dan Inovator Pendidikan, 12(1), 80–94. https://doi.org/10.29408/jhm.v12i1.32459

Problematika Pengungkapan Rahasia Bank Antara Kepentingan Negara Dan Perlindungan Kepada Nasabah | Esensi Hukum. (t.t.). Diambil 7 April 2026, dari https://journal.upnvj.ac.id/index.php/esensihukum/article/view/22

Regulasi Dan Pengawasan Perbankan Oleh Otoritas Jasa Keuangan | Menulis: Jurnal Penelitian Nusantara. (t.t.). Diambil 7 April 2026, dari https://padangjurnal.web.id/index.php/menulis/article/view/274

Syarifah, A., Ananda, A., Azzahra, Z., Rakhmawati, C. S., & Nurjihad. (2024). Implikasi Pasal 20 dan 21 Undang Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi terhadap Bank dalam Pemrosesan Data Biometrik Nasabah. Prosiding Seminar Hukum Aktual Fakultas Hukum Universitas Islam Indonesia, 481–493.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Jakarta: Sekretariat Negara.