



# Urgensi Penerapan Minimalisasi Data dalam Upaya Pencegahan Penyalahgunaan Data Pribadi Nasabah di Sektor Perbankan Berdasarkan Undang-Undang Pelindungan Data Pribadi

Wishnu Angga Yudha

Fakultas Hukum, Universitas Padjadjaran, Indonesia

Alamat: Jl. Ir. Soekarno KM. 21, Jatinangor, Kabupaten Sumedang, Jawa Barat, 45363

Korespondensi penulis: [wishnu21001@mail.unpad.ac.id](mailto:wishnu21001@mail.unpad.ac.id)

**Abstract:** *The development of the banking sector has led to an increase in the processing of customers' personal data, which can pose a risk of data misuse. One of the efforts to prevent this is the implementation of data minimisation, which emphasises that the personal data collected must be relevant, limited, and consistent with the legitimate purposes of processing, as well as transparent in accordance with the provisions of Article 27 of Law No. 27 of 2022 on Personal Data Protection (PDP Law). This study employs a normative legal analysis method with a descriptive-analytical approach, incorporating transformative legal theory and privacy rights protection to examine the application of the data minimisation by banks. The findings indicate that excessive data collection practices still frequently occur and may violate customers' privacy rights. Therefore, banks are required to disclose the types and relevance of customer data, conduct regular mapping and evaluation of the data required, and implement selective and secure information technology systems. This implementation constitutes banks' compliance with data protection principles, particularly security and accountability. Additionally, active customer involvement and oversight by authorities are crucial factors in ensuring the effectiveness of data minimisation implementation in the banking sector.*

**Keywords:** *Customer Personal Data, Data Minimisation, Banking, Personal Data Protection, PDP Law.*

**Abstrak:** Perkembangan sektor perbankan mendorong peningkatan pemrosesan data pribadi nasabah yang dapat menimbulkan risiko penyalahgunaan data. Salah satu bentuk upaya dalam mencegah hal tersebut adalah penerapan minimalisasi data yang menekankan bahwa data pribadi yang dikumpulkan harus relevan, terbatas, dan sesuai dengan tujuan pemrosesan yang sah serta transparan sesuai amanat Pasal 27 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Penelitian ini menggunakan metode analisis yuridis normatif dengan pendekatan deskriptif analitis dengan penggunaan teori hukum transformatif serta pelindungan hak atas privasi untuk mengkaji penerapan minimalisasi data oleh bank. Hasil kajian menunjukkan bahwa praktik pengumpulan data yang berlebihan masih sering terjadi dan berpotensi melanggar hak privasi nasabah. Oleh karena itu, bank wajib melakukan penyampaian informasi jenis dan relevansi data nasabah, melaksanakan proses pemetaan beserta evaluasi secara berkala terhadap data yang dibutuhkan, serta menerapkan sistem teknologi informasi yang selektif dan aman. Penerapan ini menjadi bentuk kepatuhan bank terhadap prinsip pelindungan data pribadi khususnya keamanan dan akuntabilitas. Selain itu, keterlibatan aktif nasabah dan pengawasan dari otoritas, menjadi faktor penting dalam menjamin efektivitas pelaksanaan minimalisasi data di sektor perbankan.

**Kata kunci:** Data Pribadi Nasabah, Minimalisasi Data, Perbankan, Pelindungan Data Pribadi, UU PDP.

## 1. LATAR BELAKANG

Perkembangan aktivitas perbankan tidak lepas dari meningkatnya kebutuhan masyarakat akan mendapatkan layanan keuangan yang aman dan efisien. Kini, masyarakat mengandalkan sistem perbankan dalam hal melakukan kegiatan transaksi keuangan, penyimpanan dana, dan penyediaan kredit. Salah satu bukti berkembangnya aktivitas perbankan yakni kehadiran layanan digital yang dipengaruhi dengan meningkatnya pengguna teknologi berupa *smartphone* dan internet. Dilansir dari data Bank Indonesia bahwa terhitung hingga periode

September 2024, jumlah transaksi dalam layanan perbankan digital terus meningkat yakni tercatat sebanyak 1.929,33 juta transaksi dengan tumbuh sebesar 40,45% (persen) secara tahunan, jika dibandingkan dengan periode yang sama tahun sebelumnya sebanyak 1.373,63 juta transaksi (Sayekti, 2025). Kemajuan ini tidak hanya memengaruhi cara bank beroperasi, tetapi juga mengubah perilaku nasabah, serta mendorong munculnya regulasi baru yang menyesuaikan dengan tantangan dan risiko dari perbankan. Perbankan memiliki peran penting dalam membantu sektor-sektor seperti perdagangan, industri, dan jasa dalam hal membiayai aktivitas mereka dan membantu memperkuat perekonomian Indonesia melalui penyaluran kredit dan produk-produk keuangan (Rohman, 2023).

Seiring meningkatnya akses perbankan, maka kebutuhan akan pemrosesan data pribadi nasabah juga semakin meningkat. Data pribadi nasabah sebagai salah satu unsur penting yang menyangkut privasi sehingga dibutuhkan pelindungan terhadap pemrosesan data pribadi. Pasal 1 angka 1 UU PDP memberikan definisi terkait data pribadi yakni berupa data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lain, baik secara langsung maupun tidak langsung melalui sistem elektronik atau non-elektronik. Sebagai contoh terdapat tulisan nomor pada secarik kertas kosong dapat dikatakan sebagai data. Berbeda halnya apabila di dalam secarik kertas tersebut tertulis sebuah nomor telepon dan nama pemilik nomor telepon yang bersangkutan, maka data tersebut merupakan data pribadi (Hanaya, 2023).

Data pribadi merupakan elemen kunci bagi kebebasan dan harga diri individu (Rosadi, Pembahasan Undang-Undang Pelindungan Data Pribadi, 2023). Oleh karena itu, bank wajib untuk menjamin kerahasiaan data pribadi yang diberikan nasabah. Kerahasiaan informasi dalam kegiatan perbankan tersebut diperlukan untuk kepentingan bank dan nasabah (Rivaldo & Syailendra, 2024). Sebelum nasabah dapat melakukan transaksi berupa mengirim dan menerima dana, terdapat proses pembukaan rekening baru atau pembuatan akun yang wajib dilakukan. Praktiknya, dalam pembukaan rekening baru melalui aplikasi yang mereka miliki, bank sering kali meminta data pribadi dari nasabahnya. Bank biasanya membutuhkan data seperti nama lengkap nasabah, tempat dan tanggal lahir, alamat domisili ataupun KTP, pekerjaan, termasuk data biometrik seperti pengenalan wajah dan sidik jari. Bahkan terdapat bank yang membutuhkan data berupa pendidikan, agama, nama ibu kandung, serta jabatan pekerjaan. Meskipun data ini penting untuk meningkatkan kualitas layanan perbankan dan efisiensi operasional, pengumpulan yang berlebihan tanpa pengendalian yang tepat dapat menimbulkan risiko serius, terutama terkait penyalahgunaan data pribadi.

Salah satu akar dari risiko tersebut adalah praktik pengumpulan data yang berlebihan (*over collection*), di mana bank sering kali mengambil lebih banyak informasi dari yang seharusnya dibutuhkan untuk suatu tujuan layanan tertentu. Ketika data dikumpulkan tanpa batas yang jelas, maka semakin besar pula kemungkinan data tersebut digunakan di luar konteks atau disalahgunakan. Hal ini menimbulkan ancaman bagi hak privasi nasabah terkait data pribadi yang dimiliki. Ancaman tersebut sejalan dengan adanya fenomena kebocoran dan penyalahgunaan data pribadi oleh oknum di dalam maupun di luar pihak perbankan sendiri menjadi isu yang semakin sering muncul di berbagai negara, termasuk Indonesia. Kondisi ini diperburuk dengan masih banyak ditemukan praktik pengumpulan data yang melampaui kebutuhan, minimnya transparansi kepada nasabah, serta lemahnya sistem kontrol internal dalam pengelolaan data. Dalam berbagai kasus, penyalahgunaan data dapat terjadi oleh internal pihak bank itu sendiri ataupun karena kebocoran data akibat serangan siber yang berhasil dan ketidakpatuhan terhadap prosedur keamanan yang berlaku. Selain itu, kurangnya transparansi dalam pengelolaan data dapat mengakibatkan nasabah tidak menyadari risiko yang mereka hadapi, sehingga mereka tidak mengambil langkah-langkah pencegahan yang diperlukan (Antoine, Farizqa, Hasna, & Pasaribu, 2025).

Walaupun demikian UU PDP mengamanatkan bahwa pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan. Salah satu penerapannya adalah dengan adanya minimalisasi data sebagai upaya dalam mencegah penyalahgunaan data nasabah. Oleh karena itu, penting lebih lanjut untuk dikaji mengenai penerapan minimalisasi data pribadi nasabah berdasarkan UU PDP.

## **2. KAJIAN TEORITIS**

Pada kajian teoritis dalam penelitian ini menggunakan teori hukum transformatif dan hukum perlindungan hak atas privasi. Di era yang terus berkembang, hukum harus adaptif dengan dinamika zaman agar tetap relevan dan efektif dalam menegakkan keadilan sebagaimana teori hukum transformatif yang dikemukakan oleh Ahmad M. Ramli mengenai hukum tidak semata-mata difungsikan untuk menjaga ketertiban, kepastian, dan keadilan, tetapi lebih jauh menambah satu fungsi hukum sebagai infrastruktur informasi layaknya teknologi sebagai akselerator transformasi Indonesia dalam menghadapi kompetisi global dan perubahan sosial budaya masyarakat yang tidak bisa dibatasi lagi secara teritorial akibat transformasi digital (Ramli & Ramli, Hukum Sebagai Infrastruktur Transformasi Indonesia (Regulasi dan Kebijakan Digital),, 2022)

Implementasi dari Indonesia sebagai negara hukum salah satunya dengan menjamin hak-hak dasar warga negara. Hal ini sejalan dengan pemikiran John Locke mengenai negara hukum yang berlandaskan pada sebuah pemikiran adanya kewajiban negara untuk melindungi hak asasi warga negaranya. John Locke berpendapat bahwa dalam diri manusia terdapat hak kodrati (*natural rights*) yang meliputi hak atas hidup, hak kebebasan, serta hak memiliki (Gunakaya, 2017). Salah satu hak yang diatur dalam Konstitusi Indonesia ialah hak privasi sebagaimana amanat Pasal 28G ayat (1) UUD 1945 yang menjelaskan bahwa:

“Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya, serta atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.”

Lebih lanjut Pasal 28H ayat (4) UUD 1945 menegaskan mengenai hak milik pribadi bahwa:

“Setiap orang berhak mempunyai hak milik pribadi dan hak milik pribadi tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapapun.”

Kedua pasal tersebut sejalan dengan Pasal 12 Deklarasi Universal tentang Hak Asasi Manusia (Universal Declaration of Human Rights 1948) yang menyatakan bahwa:

*“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honours and reputation. Everyone has the right to the protection of the law against such interference or attacks.”*

Pasal tersebut menjelaskan bahwa tidak ada seorangpun yang boleh diganggu secara sewenang-wenang dalam urusan pribadinya serta setiap orang berhak atas perlindungan hukum terhadap gangguan atau serangan semacam itu.

Pelindungan hak privasi seseorang sangat penting untuk menjaga kebebasan dan martabat individu dalam kehidupan sosial. Warren dan Brandeis mengembangkan teori privasi dalam sebuah artikel yang berjudul hak untuk tidak diganggu atau *“The Right to Privacy”* (Warren & Brandies, 1890). Menurut Warren dan Brandies dengan adanya perkembangan dan kemajuan teknologi maka muncul suatu kesadaran masyarakat mengenai telah lahirnya suatu kesadaran bahwa ada hak seseorang untuk menikmati hidup. Hak tersebut berupa hak untuk tidak diganggu dalam kehidupan pribadinya. Dalam hal ini hukum harus mengakui dan melindungi hak privasi tersebut. Hak tersebut berkaitan dengan kebutuhan spiritual manusia yaitu kebutuhan untuk dihargai perasaan, pikiran dan hak untuk menikmati kehidupannya atau disebut dengan *the right to be let alone*, sehingga privasi suatu hak yang harus dilindungi (Rosadi, Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional, 2022).

Hak privasi mencakup perlindungan terhadap data pribadi. Pelindungan yang mengacu pada konsep dan prinsip dengan tujuan untuk melindungi hak individu dalam menjaga informasi pribadi mereka dari penyalahgunaan, karena pada dasarnya setiap individu memiliki hak untuk mengontrol informasi yang berkaitan dengan diri mereka, serta bagaimana data tersebut digunakan. Konsep perlindungan data pribadi menegaskan pentingnya pengakuan atas hak individual untuk mengontrol informasi pribadinya. Hal ini mencakup kebebasan setiap individu dalam memutuskan untuk berpartisipasi dalam kehidupan bermasyarakat yang melibatkan pertukaran atau pembagian data pribadi. (Rosadi, Prinsip-prinsip Perlindungan Data Privasi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya, 2017). Selain itu, setiap individu memiliki kewenangan berupa hak untuk menetapkan syarat-syarat tertentu sebelum data pribadinya dapat diakses, digunakan, atau disebarluaskan oleh pihak lain. Dengan demikian, perlindungan data pribadi tidak hanya bersifat teknis, tetapi juga merupakan wujud dari penghormatan terhadap hak asasi manusia, khususnya hak atas privasi.

### **3. METODE PENELITIAN**

Metode penelitian yang digunakan dalam penelitian ini merupakan metode analisis yuridis normatif yang menitikberatkan pada penggunaan data sekunder yang meliputi bahan hukum primer, sekunder dan tersier sebagai alat untuk menyelesaikan permasalahan yang ada. Penelitian ini akan mengkaji mengenai penerapan minimalisasi data dalam pemrosesan data pribadi dalam sektor perbankan yang ditinjau dari UU PDP.

Adapun, spesifikasi penelitian yang digunakan yakni spesifikasi deskriptif analitis yang dilakukan dengan menelaah peraturan perundang-undangan yang berlaku, kemudian menghubungkannya dengan teori-teori hukum serta praktik pelaksanaan hukum yang sesuai dengan isu yang dikaji. Teori yang digunakan dalam penelitian ini yakni teori hukum transformatif dan teori perlindungan hak atas privasi dengan permasalahan mengenai pengumpulan data pribadi nasabah secara berlebihan yang menimbulkan potensi penyalahgunaan data. Metode deskriptif analisis akan memberikan sebuah gambaran yang sistematis yang mudah dipahami dalam penelitian ini. Teknik pengumpulan data yang digunakan dalam melakukan penelitian ini berupa studi dokumen dan studi dokumen digital. Pengumpulan data akan memuat pengkajian penelitian yang ditinjau dari berbagai aspek meliputi teori, filosofi, penjelasan umum, dan kekuatan hukum yang mengikat.

#### **4. HASIL DAN PEMBAHASAN**

##### **Pengaturan Penerapan Minimalisasi Data dalam UU PDP**

Secara umum, regulasi yang mengatur mengenai pelindungan data pribadi di Indonesia ialah mengacu pada UU PDP. UU PDP adalah produk legislasi *lex specialis* yang merupakan instrumen legislasi primer yang mengatur PDP secara spesifik dan tidak tersekat oleh sektor atau rezim hukum tertentu (Ramli, Tafsir Undang-Undang Pelindungan Data Pribadi, 2023). UU PDP juga menyeimbangkan antara kepentingan individu sebagai pemilik data dan tanggung jawab pengendali data sebagai pihak yang memproses data dalam rangka pemenuhan hak tersebut. UU PDP bertindak sebagai *legal framework* atau payung hukum dalam pelindungan data pribadi di Indonesia yang mengatur prinsip pelindungan data pribadi dan menjadi acuan bagi ketentuan peraturan perundang-undangan lain yang mengatur mengenai data pribadi, termasuk peraturan yang bersifat khusus bagi sektor tertentu (Lustarini, 2022). Prinsip pelindungan data pribadi merupakan pedoman yang wajib dipatuhi bagi setiap pengendali data dalam melakukan pemrosesan data pribadi. Selain itu, prinsip pelindungan data pribadi juga berfungsi untuk meningkatkan kepercayaan dari subjek data, salah satunya yakni nasabah, karena adanya penghormatan terhadap hak privasinya. Adapun dengan hanya mengumpulkan dan mengolah data yang relevan dan diperlukan, pengendali data juga dapat meningkatkan efisiensi operasional dan mengurangi risiko kebocoran data.

Minimalisasi data berarti bahwa data pribadi yang dikumpulkan harus bersifat seminim mungkin, terbatas dengan apa yang benar diperlukan untuk mencapai tujuan pemrosesan yang sah. Pengendali data tidak boleh mengumpulkan informasi berlebihan yang tidak relevan atau tidak proporsional terhadap tujuan pemrosesan data. Penerapan minimalisasi data secara khusus tidak diatur eksplisit dalam UU PDP. Namun, penerapan minimalisasi data ini merupakan salah satu bentuk implementasi prinsip pelindungan data pribadi berdasarkan Pasal 16 ayat (2) huruf a UU PDP bahwa pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan. Hal ini dijelaskan kembali dalam Pasal 27 UU PDP bahwa adanya kewajiban pengendali data untuk mengumpulkan data pribadi secara terbatas dan spesifik, sah secara hukum, dan transparan. Konsep minimalisasi data sebagai salah satu implementasi dalam perlindungan data pribadi yang bertujuan untuk memastikan bahwa data pribadi yang dikumpulkan oleh pengendali data hanya sebatas yang benar-benar dibutuhkan untuk tujuan yang sah dan telah ditentukan sebelumnya. Dengan kata lain, hanya data yang relevan, memadai, dan terbatas yang boleh dikumpulkan dan diproses. Tujuannya tidak hanya melindungi privasi subjek data, tetapi juga mencegah risiko penyalahgunaan data akibat pengumpulan yang berlebihan.

*Pertama*, frasa "terbatas dan spesifik" secara langsung menggambarkan esensi dari konsep minimalisasi data, yaitu membatasi ruang lingkup pengumpulan data agar tidak melebihi kebutuhan yang telah ditentukan. Terbatas dan spesifik ditujukan pada dua hal yakni pembatasan tujuan dan pembatasan data pribadi yang diperoleh. Berdasarkan penjelasan Pasal 27 UU PDP yakni "secara terbatas dan spesifik berarti data pribadi harus terbatas sesuai dengan tujuan pemrosesannya serta tujuan pemrosesan data pribadi harus secara eksplisit, sah, dan telah ditentukan pada saat pengumpulan data pribadi." *Kedua*, sah secara hukum dan transparan juga menguatkan bahwa setiap tindakan pengumpulan data harus dapat dipertanggungjawabkan secara hukum dan diketahui oleh subjek data. Hal ini mencegah praktik pengumpulan data secara berlebihan, tidak relevan, atau dilakukan tanpa dasar hukum yang jelas. Data yang diperoleh oleh pengendali data harus berdasarkan legalitas dan berdasarkan cara-cara yang tidak melanggar hukum. Selain itu, subjek data dapat mengetahui jenis data-data apa saja yang dapat diperoleh dan relevansi jenis data tersebut menggunakan bahasa yang mudah dipahami.

Penerapan minimalisasi data juga sejalan dengan pengaturan yang tercantum dalam Pasal 5 ayat 1 c General Data Protection Regulation, 2018 (EU-GDPR) mengenai prinsip *data minimisation* bahwa data yang diproses harus *adequate* artinya layak untuk mencapai tujuan pemrosesan data dan *relevant* yakni memiliki hubungan dengan tujuan yang dimaksud, serta *limited to what is necessary* bahwa pemrosesan tidak mengumpulkan data lebih dari tujuan yang telah disepakati. Meski berasal dari dua yurisdiksi yang berbeda, penerapan minimalisasi data dalam kedua regulasi tersebut menunjukkan orientasi yang sama yakni adanya perlindungan terhadap hak individu atas data pribadi dan pembatasan kewenangan pengendali data.

Selain itu, penerapan minimalisasi data juga sebagai bentuk penerapan prinsip keamanan (*security*) dan akuntabilitas. Semakin sedikit dan semakin spesifik data yang diperoleh oleh pengendali data, maka semakin kecil risiko kebocoran, pencurian, atau penyalahgunaan data. Di sisi lain, akuntabilitas memberikan kepastian bahwa pengendali data sebagai pihak yang memproses data dapat mempertanggungjawabkan tindakan yang dilakukan dalam hal melaksanakan pemrosesan data pribadi subjek data termasuk untuk melindungi hak subjek data dan membangun kepercayaan publik terhadap pengelolaan data.

### **Penerapan Minimalisasi Data oleh Bank dalam Pemrosesan Data Pribadi Nasabah**

Pentingnya bank melakukan minimalisasi data supaya data yang diperoleh tidak disalahgunakan baik oleh pihak bank maupun pihak ketiga yang diberi akses oleh bank dalam melakukan pemrosesan data pribadi atas persetujuan nasabah. Umumnya, setiap bank dapat

melaksanakan pemrosesan data pribadi nasabah jika telah mendapatkan persetujuan (*consent*) nasabah secara eksplisit. Hal ini mengacu pada prinsip keabsahan secara hukum (*lawfulness*). Persetujuan nasabah dijadikan sebagai legalitas atau dasar pemrosesan data pribadi nasabah. Umumnya, persetujuan dari pemilik data itu dilakukan dengan menyediakan kolom ceklis syarat dan ketentuan (*terms and condition*) termasuk mengenai kebijakan privasi yang dapat diakses oleh nasabah. Persetujuan juga harus diperoleh berdasarkan hukum yang artinya, tidak boleh ada unsur penipuan ataupun pemaksaan terhadap nasabah.

Dalam hal persetujuan tersebut, Pasal 21 ayat (1) UU PDP menegaskan bahwa adanya penyampaian kewajiban informasi mengenai pemrosesan data pribadi kepada subjek data yakni nasabah yang salah satu muatannya informasi mengenai jenis dan relevansi data yang akan diproses. Hal ini menunjukkan data yang diperoleh oleh bank harus ada kesesuaian dengan tujuan yang hendak dicapai. Adanya, informasi ini sejalan dengan prinsip transparansi kepada nasabah terkait data yang mereka kumpulkan kepada bank. Nasabah dapat mengetahui alasan-alasan bank dalam menggunakan data tersebut. Misalnya data biometrik pengenalan wajah digunakan untuk proses verifikasi nasabah dan untuk keperluan pelaksanaan proses *Know-Your-Customer* (KYC). Oleh karena itu, bank wajib untuk menyampaikan informasi se jelas mungkin dan menjabarkan setiap data yang diperlukan oleh bank. Hal ini dapat meningkatkan kepercayaan nasabah agar data yang digunakan dengan cara yang benar dan tidak disalahgunakan. Penerapan ini sejalan dengan prinsip perbankan mengenai “Prinsip Kepercayaan.” Nasabah mempercayakan dananya disimpan di bank dalam suatu portofolio dan dikelola dengan aman dan jujur (Putera, 2020). Praktik yang terjadi beberapa bank masih belum transparan dalam hal menjelaskan relevansi dari setiap data. Umumnya bank hanya memberi intruksi kepada nasabah untuk segera menyentang kolom persetujuan tanpa adanya penjelasan lebih lanjut mengenai setiap data yang diproses. Menilik pada praktik layanan bank digital, bank umumnya menyampaikan informasi mengenai pemrosesan data pribadi pada kebijakan privasinya. Namun, masih ditemukannya kebijakan privasi yang informasinya bersifat minim tanpa penjelasan yang memadai. Bank cenderung menyertakan jenis-jenis datanya, tetapi tidak disertai penjelasan kegunaan dari setiap data tersebut.

Lebih lanjut, sebelum bank melaksanakan pemrosesan data pribadi nasabah dan menyampaikan informasi mengenai jenis serta relevansi data tersebut, bank dapat melaksanakan proses pemetaan data. Pemetaan data merupakan proses penting berupa mengidentifikasi dan memetakan jenis-jenis data yang memang diperlukan untuk proses layanan seperti pembukaan rekening, pemberian kredit, atau proses verifikasi. Dalam hal ini juga perlu adanya pengukuran batasan sejauh mana dan seberapa banyak data-data yang dapat

digunakan dalam melakukan verifikasi ataupun pengenalan terhadap nasabah. Alangkah lebih baik jika bank tidak menggunakan jenis data secara berlebihan hanya untuk keperluan pembukaan rekening dan proses verifikasi. Pada praktiknya seringkali bank meminta data pribadi nasabah yang tidak sesuai relevansinya. Misalnya untuk kebutuhan verifikasi bank banyak memerlukan data berupa nama, NIK, agama, nama ibu kandung, nomor telepon, alamat, status perkawinan. Adapun agama, golongan darah, dan status perkawinan tidak diperlukan (Rosadi, Pembahasan Undang-Undang Pelindungan Data Pribadi, 2023). Selain itu, dalam penerapan kewajiban penyampaian mengenai jenis dan relevansi data, mayoritas bank tidak menjelaskan relevansinya. Misalnya bank tidak menjelaskan maksud kegunaan dari pemerolehan data berupa nama ibu kandung, agama, jabatan, pekerjaan, dan data lainnya. Padahal relevansi ini penting untuk disampaikan meninjau bahwa pemrosesan harus dilaksanakan sesuai tujuan, terbatas, spesifik, dan tidak mengumpulkan data yang berlebihan dari tujuan awal.

Proses pemetaan ini juga harus didukung dengan adanya penerapan evaluasi. Evaluasi berkala terhadap jenis data yang dikumpulkan untuk memastikan masih relevan. Adanya keharusan penghapusan data jika memang data yang dikumpulkan tidak relevan lagi dengan tujuan ataupun sudah tidak digunakan lagi. Hal ini sejalan dengan Pasal 43 ayat (1) UU PDP mengenai kewajiban bank sebagai pengendali data pribadi untuk menghapus data pribadi dalam hal data pribadi tidak lagi diperlukan untuk pencapaian tujuan pemrosesan data pribadi. Evaluasi ini juga menjadi bahan pertimbangan di kemudian hari, untuk dapat lebih mengurangi data yang sudah dianggap tidak berkaitan dengan tujuan pemrosesan data pribadi nasabah.

Kemudian, bank juga dapat menerapkan sistem teknologi informasi yang selektif. Sistem yang digunakan oleh bank untuk dapat mendukung pengumpulan data secara terbatas. Adapun dengan pendekatan ini, bank dapat meminimalkan risiko kebocoran data dan pelanggaran privasi. Selain itu, sistem selektif tersebut harus dilengkapi dengan pengelolaan kontrol terhadap akses yang ketat, sehingga hanya pihak yang berwenang dan diizinkan yang dapat mengakses informasi sensitif nasabah dan tidak ada penyalahgunaan terhadap data pribadi nasabah. Mekanisme seperti otentikasi ganda, enkripsi data, dan *audit log* menjadi komponen penting dalam menjaga integritas dan kerahasiaan data. Melalui penerapan sistem teknologi informasi yang selektif dan aman, bank tidak hanya memenuhi kewajiban dalam menjaga keamanan saja, tetapi dapat membangun kepercayaan nasabah terhadap komitmen perlindungan data pribadi.

Penerapan minimalisasi data dalam sektor perbankan dapat berjalan dengan efektif jika semua elemen dapat mematuhi kewajiban dalam UU PDP, khususnya bank sebagai pengendali

data pribadi nasabah. Selain itu juga diperlukan pengawasan yang ketat terhadap praktik-praktik bank jika terjadi permintaan data yang berlebihan, tidak sesuai tujuan, dan melanggar secara hukum. Perlunya, sistem pengawasan yang kuat dalam hal menjamin pelindungan data pribadi nasabah. Otoritas pengawas dan regulator sektor perbankan memiliki peran strategis dalam memastikan kepatuhan terhadap prinsip-prinsip perlindungan data pribadi yang mencakup pelaksanaan pengawasan yang berkelanjutan dan sebagai langkah preventif guna mencegah potensi risiko yang dapat timbul akibat kelalaian dalam pengelolaan data pribadi nasabah (Prayogo, Korah, Soepeno, & Kasenda, 2024).

UU PDP sendiri telah mengatur mengenai sanksi berdasarkan Pasal 57 UU PDP yang menyatakan pelanggaran terhadap kewajiban pengendali data untuk melakukan pemrosesan data pribadi secara terbatas dan spesifik, sah secara hukum, dan transparan akan mendapatkan sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan/atau denda administratif dengan tata cara yang akan diatur dalam peraturan pemerintah. Hal ini menjadi tantangan tersendiri juga karena belum adanya aturan khusus lebih lanjut mengenai sanksi dan lembaga pengawas. Pemerintah saat ini sedang menyusun peraturan pemerintah terkait perlindungan data pribadi untuk mendukung pelaksanaan UU PDP. Kendati demikian, bank sebagai bagian dari sektor jasa keuangan memiliki pengawas dalam hal aktivitas perbankan yakni oleh Otoritas Jasa Keuangan (OJK). OJK sebagai lembaga independen dapat mengawasi bank dalam menjalankan aktivitas perbankan termasuk dalam hal melindungi kepentingan nasabah sebagai konsumen. Oleh karena itu, diharapkan OJK dapat mengawasi aktivitas dalam sektor perbankan khususnya jika terjadi penyalahgunaan data pribadi dalam hal melanggar perlindungan konsumen.

Adapun peran nasabah sebagai subjek data dapat melakukan pengaduan dalam hal terjadi permintaan pemerolehan data yang tidak sesuai dengan tujuan, penggunaan data yang tidak sesuai dengan persetujuan (*consent*), dan/atau penyalahgunaan data yang merugikan nasabah. Nasabah yang mengalami kerugian seharusnya tidak hanya diam saja, melainkan harus proaktif dalam melakukan berbagai upaya untuk memperjuangkan haknya mulai dari melaporkan mengenai kejadian yang dialami kepada pihak bank atau melalui jalur hukum (Ernanti, Turisno, & Aminah, 2016). Tindakan aktif dari nasabah tidak hanya penting dalam rangka pemulihan hak individu, tetapi juga berkontribusi pada peningkatan akuntabilitas lembaga keuangan dalam melindungi data pribadi nasabah secara menyeluruh. Oleh karena itu, bank wajib memiliki platform untuk menanggapi atau menyediakan pemenuhan hak nasabah atas

pengaduan atau pelaporan. Hal ini didasarkan pada hak nasabah dalam Pasal 12 UU PDP bahwa:

“Subjek data pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.”

Demikian nasabah diharapkan dapat turut serta aktif mengawasi pelaksanaan pemrosesan data pribadi dan melaporkan jika terjadi penyalahgunaan data.

## **KESIMPULAN DAN SARAN**

Penerapan minimalisasi data dalam sektor perbankan merupakan upaya penting untuk mencegah penyalahgunaan data pribadi nasabah, baik oleh bank maupun pihak ketiga, dengan memastikan bahwa data yang dikumpulkan relevan, terbatas, dan sesuai dengan tujuan pemrosesan yang sah. Pengendali data tidak boleh mengumpulkan informasi berlebihan yang tidak proporsional terhadap tujuan pemrosesan data. Minimalisasi data sebagai implementasi kepatuhan bank terhadap prinsip perlindungan data pribadi mengenai pengumpulan data yang harus dilakukan secara terbatas, spesifik, sah secara hukum, dan transparan sesuai dengan amanat Pasal 27 UU PDP yang sejalan dengan prinsip *data minimisation* dalam Pasal 5 ayat 1 c EU-GDPR.

Penerapan minimalisasi data harus didukung oleh peran bank, nasabah, serta pengawas. Bank dapat melaksanakan penerapan dengan transparansi informasi jenis dan relevansi data kepada nasabah, melaksanakan proses pemetaan dan evaluasi data yang berkelanjutan, serta penerapan teknologi informasi yang aman dan selektif. Dalam pelaksanaannya, bank sebagai pengendali data pribadi wajib mematuhi ketentuan UU PDP, termasuk kewajiban untuk menghapus data yang tidak lagi relevan dan menyediakan akses serta sarana pengaduan bagi nasabah. Lembaga pengawas perlindungan data pribadi dan perbankan juga wajib untuk mengawasi bank dalam melaksanakan minimalisasi data. Kemudian, peran aktif nasabah sebagai subjek data menjadi faktor dalam membantu mengawasi serta memastikan akuntabilitas bank dalam membangun kepercayaan dalam pemrosesan data pribadi di sektor perbankan.

## DAFTAR REFERENSI

- Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2025). Penyalahgunaan data pribadi dalam teknologi transaksi digital di industri perbankan digital (Studi kasus PT. Bank Syariah Indonesia). *Jurnal Multidisiplin Ilmu Akademik*, 2(1).
- Ernanti, Q., Turisno, B. E., & Aminah. (2016). Perlindungan hukum bagi konsumen perbankan dalam penggunaan data pribadi nasabah (Studi pada PT BRI Kantor Wilayah Semarang). *Diponegoro Law Journal*, 5(3). <https://www.neliti.com/id/publications/19263/perlindungan-hukum-bagi-konsumen-perbankan-dalam-penggunaan-data-pribadi-nasabah>
- Gunakaya, A. W. (2017). *Hukum hak asasi manusia*. Penerbit Andi.
- Hanaya, E. (2023). Perlindungan data pribadi di era digital dalam perspektif perbandingan hukum. *Jurnal Bevinding*, 1(9).
- Lustarini, M. (2022). Kepastian hukum pelindungan data pribadi pasca pengesahan UU Nomor 27 Tahun 2022. Kementerian Komunikasi dan Informatika. [https://jdih.komdigi.go.id/pdfjs/web/viewer.html?file=/storage/file-artikel-hukum/1729219695-Kepastian\\_Hukum\\_PDP.pdf](https://jdih.komdigi.go.id/pdfjs/web/viewer.html?file=/storage/file-artikel-hukum/1729219695-Kepastian_Hukum_PDP.pdf)
- Prayogo, P., Korah, R. S., Soepeno, M. H., & Kasenda, V. (2024). Analisis perlindungan hukum data pribadi nasabah pada transaksi internet banking di Sulawesi Utara. *Jurnal Nuansa Akademik: Jurnal Pembangunan Masyarakat*, 9(1).
- Putera, A. P. (2020). Prinsip kepercayaan sebagai fondasi utama kegiatan perbankan. *Jurnal Hukum Bisnis Bonum Commune*, 3(1). <https://www.neliti.com/publications/457294/prinsip-kepercayaan-sebagai-fondasi-utama-kegiatan-perbankan>
- Ramli, A. M. (2023). *Tafsir Undang-Undang Pelindungan Data Pribadi*. Refika Aditama.
- Ramli, A. M., & Ramli, T. S. (2022). *Hukum sebagai infrastruktur transformasi Indonesia (regulasi dan kebijakan digital)*. Refika Aditama.
- Rivaldo, A., & Syailendra, M. R. (2024). Tanggung jawab penyedia layanan perbankan terhadap penyalahgunaan data nasabah berdasarkan Pasal 46 Ayat 1 UU PDP (Kasus Putusan 615/Pdt.G/2023/PN Surabaya). *UNES Law Review*, 6(4). <https://review-unes.com/index.php/law/article/view/2045>
- Rohman, A. (2023). Peran perbankan dalam perekonomian Indonesia saat ini. Fakultas Ekonomi dan Bisnis Universitas Brawijaya. <https://feb.ub.ac.id/peran-perbankan-dalam-perekonomian-indonesia-saat-ini/>
- Rosadi, S. D. (2017). Prinsip-prinsip perlindungan data privasi nasabah kartu kredit menurut ketentuan nasional dan implementasinya. *Jurnal Sosiohumaniora*, 19(3). <https://jurnal.unpad.ac.id/sosiohumaniora/article/view/11380/0>
- Rosadi, S. D. (2022). *Cyber law: Aspek data privasi menurut hukum internasional, regional, dan nasional*. Refika Aditama.

Rosadi, S. D. (2023). *Pembahasan Undang-Undang Pelindungan Data Pribadi*. Sinar Grafika.

Sayekti, I. M. (Ed.). (2025). *Tren perkembangan bank dengan layanan digital di Indonesia*. Pressrelease.id. <https://pressrelease.kontan.co.id/news/tren-perkembangan-bank-dengan-layanan-digital-di-indonesia>

Warren, S., & Brandies, L. D. (1890). The right of privacy. *Harvard Law Review*.