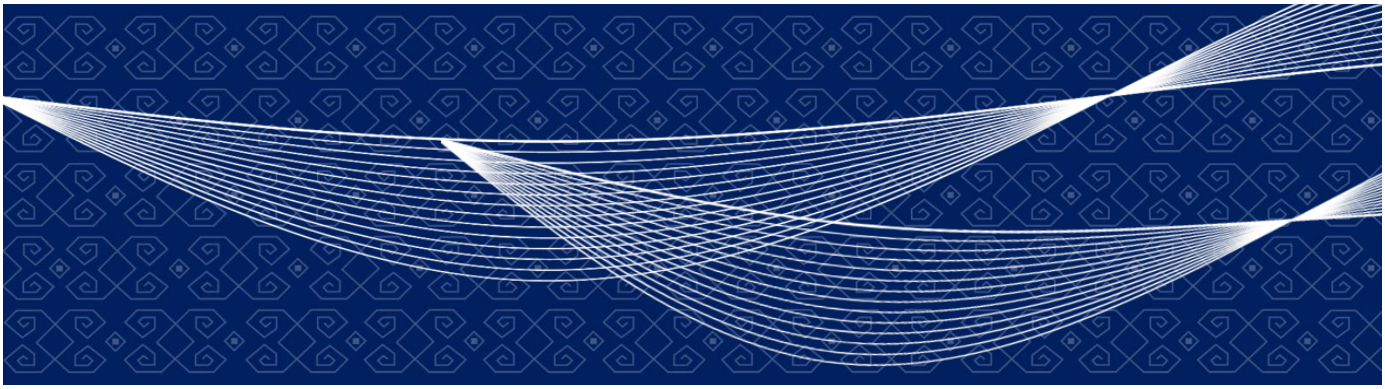
BANK INDONESIA
BANK SENTRAL REPUBLIK INDONESIA



RP/LBG/02/2024

WORKING PAPER

PELINDUNGAN DATA PRIBADI DI BANK INDONESIA DAN LEMBAGA JASA KEUANGAN: REKOMENDASI KEBIJAKAN DAN TEKNIS PENGATURAN

R. Dwi Tjahja K. Wardhono, Wishnu Badrawani, Ayu Deviana, Melati Pramudyastuti, Nadhia Shalehanti

2024

PELINDUNGAN DATA PRIBADI DI BANK INDONESIA DAN LEMBAGA JASA KEUANGAN: REKOMENDASI KEBIJAKAN DAN TEKNIS PENGATURAN

R. Dwi Tjahja K. Wardhono, Wishnu Badrawani, Ayu Deviana, Melati Pramudyastuti, Nadhia Shalehanti

Abstract

Pelindungan data pribadi di era digital menjadi krusial, khususnya di Indonesia, mengingat risiko kebocoran data yang tinggi. Pelindungan terhadap subjek data pribadi merupakan bagian dari hak asasi manusia sehingga risiko kebocoran data pribadi mengharuskan adanya aturan dan pedoman bagi lembaga jasa keuangan yang menggunakan data pribadi dalam kegiatan bisnisnya. UU No.27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) meskipun telah berlaku sejak dua tahun, namun belum didukung peraturan teknis yang cukup memadai. Bank Indonesia (BI), sebagai regulator dan penyelenggara sistem pembayaran, memiliki mandat dan kepentingan dalam menjaga keamanan terhadap subyek data pribadi, sehingga perlu mengatur sebagai tindak lanjut mandat yang diberikan oleh UU PDP. Penelitian ini akan mengeksplorasi prinsip-prinsip yang dapat menjadi aturan dan pedoman bagi industri lembaga jasa keuangan (LJK) yang di bawah kewenangannya, termasuk mengatur mengenai pertukaran data (*data sharing*) dalam penanganan *fraud,* dan koordinasi pengawasan, serta menyusun kerangka hukum yang diperlukan terkait pelindungan data pribadi di BI. Hasil dari penelitian ini menyimpulkan bahwa pentingnya BI membuat peraturan yang menjadi payung hukum yang spesifik mengenai pelindungan data pribadi serta peraturan teknis dan perlunya koordinasi yang harmonis antar-lembaga pengawas terkait.

Keywords: pelindungan data pribadi, subjek data pribadi, *data sharing,* Lembaga pengawas, koordinasi antar lembaga.

Disclaimer: The views and analysis from this study are solely responsible for the authors, without implicating to Bank Indonesia.

1. Latar Belakang

Dalam era digitalisasi yang semakin pesat, pelindungan dan keamanan data pribadi menjadi isu krusial yang memerlukan perhatian serius di beberapa negara, khususnya di Indonesia. Semakin meningkatnya volume data pribadi yang dihasilkan dan diproses oleh entitas bisnis dan organisasi, tantangan keamanan data pun semakin kompleks. Pengawasan (*oversight*) dan penegakan hukum (*law enforcement*) dalam pelindungan data pribadi menjadi pokok perhatian di samping pengaturannya (*regulation*) di Bank Indonesia, mengingat potensi risiko kebocoran dan/atau penyalahgunaan data/informasi pribadi, dapat merugikan subjek data pribadi dan juga lembaga jasa keuangan yang terkait dengan pengelolaan dan pemrosesan data tersebut.

Perkembangan teknologi yang cepat dan perdagangan lintas batas melalui perdagangan elektronik, menarik perhatian pemerintah untuk menetapkan standar minimum global untuk pelindungan data. Hal ini juga menarik perhatian akademisi dan masyarakat umum. Pelindungan data pribadi diperlukan untuk melaksanakan hak privasi yang berakar dalam Deklarasi Universal Hak Asasi Manusia pada Pasal 12 yang menyatakan "*Tidak seorangpun boleh diganggu secara sewenang-wenang dalam urusan pribadi, keluarga, rumah tangga atau hubungan surat-menyuratnya, juga tidak boleh dilakukan serangan terhadap kehormatan dan reputasinya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan atau penyerangan seperti itu*".[1] Selain itu, pelindungan data juga diperlukan untuk memungkinkan dan memfasilitasi aliran data pribadi lintas batas.[2]

Perkembangan teknologi informasi saat ini telah membuka potensi peningkatan efisiensi, tetapi sekaligus memberikan celah bagi potensi pelanggaran keamanan data yang dilakukan oleh pihak eksternal maupun nasabah sendiri yang notabene juga merupakan subjek data pribadi. Tantangan ini semakin rumit, antara lain dengan perkembangan metode serangan siber dan *social engineering*[3] yang terus berkembang dan meningkatkan risiko ancaman terhadap kerahasiaan data pribadi. Berdasarkan pandangan Wiwoho dkk karakteristik penggunaan pembayaran digital (transaksi yang bersifat *real-time*, tidak tatap muka, dan tanpa batasan geografis) rentan terhadap penyalahgunaan seperti pencucian uang dan pendanaan terorisme.[4] Menurut pendapat Opderbeck, pelanggaran data pribadi bersifat luas dan menimbulkan konsekuensi biaya yang cukup tinggi, contohnya antara lain penyalahgunaan kartu kredit konsumen di industri ritel.[5]

Di era yang semakin digital, pengelolaan pelindungan data digital pribadi menjadi sangat penting tidak hanya bagi individual sebagai *end-user*, namun juga penyedia layanan, pemilik *platform*, dan bahkan pemerintah sebagai badan publik. Koordinasi dan harmonisasi antar pihak merupakan keharusan dalam pengelolaan data. Wardhono dkk, menegaskan bahwa koordinasi antarlembaga dan lintas sektoral merupakan prasyarat untuk menjalankan respons yang terkoordinasi dan terintegrasi dalam mengatasi krisis/hazard.[6] Koordinasi antarlembaga ini menjadi penting terutama terkait dengan pelindungan data pribadi dan juga pengawasannya. Sinergi antar instansi pemerintah, swasta, dan masyarakat sipil dapat meningkatkan efisiensi dan efektivitas dalam menghadapi tantangan yang kompleks di masa yang akan datang.

Mengingat sangat pentingnya data dalam *platform* ekonomi untuk penciptaan nilai, maka menyeimbangkan privasi dan penciptaan nilai dalam pemanfaatan data bagi ekonomi

---

[1]Wahyudi Djafar dan M. Jodi Santoso, "Perlindungan Data Pribadi: Konsep, Instrumen, dan Prinsipnya", Lembaga Studi dan Advokasi Masyarakat, 2019. https://elsam.or.id/storage/files/2/Policy%20Brief%20Perlindungan%20Data%20Pribadi%20KOnsep,%20instrumen%20dan%20prinsipnya%20oke.pdf. Di akses pada: 1 Agustus 2024

[2]Christian Pauletto, "Options towards a global standard for the protection of individuals with regard to the processing of personal data", Computer Law & Security Review, 2020. https://doi.org/10.1016/j.clsr.2020.105433. Diakses pada: 23 April 2024

[3]Kapersky, "What is Social Engineering?**"**, 2024, https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering?srsltid=AfmBOop2s3NUclvverDH5qoRAEiycJcAk-HggLo9ZOBRHQYZDWFb-VKx. Di akses pada: 23 April 2024

[4]Jamal Wiwoho, Dona Budi Kharisma, Dwi Tjahja K. Wardhono, "Financial Crime in Digital Payments", *Journal of Central Banking Law and Institutions Vol 1 No 1,* 2022, DOI: 10.21098/jcli.v1i1.7. Diakses pada: 24 April 2024

[5]Opderbeck, D. W, "Cybersecurity, data breaches, and the economic loss doctrine in the payment card industry", Maryland Law Review Vol.75, 2016. Diakses pada: 23 April 2024

[6]Dwi Tjahja K. Wardhono, Retno Muhardini, Dian Puji Nugraha Simatupang, Nadhia Shalehanti, "Crisis, Hazard, and Disaster Management: A Study of Regulatory Formulation and Institutional Coordination", *Journal of Central Banking Law and Institutions Vol 2 No 3,* 2023, ttps://doi.org/10.21098/jcli.v2i3.193. Di akses pada: 20 November 2024

menjadi sangat krusial.[7] Namun demikian, studi empiris menunjukkan bahwa konsumen tidak terlalu sensitif terhadap pelindungan data pribadi mereka.[8]

Sejak tahun 2019 sampai dengan 2023, Kementerian Kominfo telah menemukan 98 kasus dugaan pelanggaran pelindungan data pribadi. Hal tersebut bukan hanya kebocoran data pribadi tapi termasuk pelanggaran pelindungan data pribadi lainnya. Berdasarkan jumlah Penyelenggara Sistem Elektronik (PSE) yang ditangani sebanyak 65 PSE Privat dan 33 PSE Publik.[9] Namun, penulis menilai bahwa pelanggaran yang terjadi nampaknya lebih banyak yang belum dilaporkan karena kurang sensitifnya atau keengganan subyek data yang dilanggar untuk melaporkan ke pihak terkait. Hal ini menunjukkan UU PDP belum berdampak sampai pada Masyarakat, karena belum memiliki ketentuan pelaksanaannya.

Salah satu lembaga negara publik yang ikut terdampak dengan mandat peraturan perundang-undangan mengenai pelindungan data pribadi ini adalah Bank Indonesia (BI). Pertama, BI selaku regulator memiliki tanggung jawab untuk menjaga keamanan data dalam mengatur dan mengawasi sektor keuangan yang berada di bawah kewenangannya yaitu lembaga jasa keuangan. Kedua, BI sebagai Badan Publik dan sekaligus Penyelenggara Sistem Pembayaran (a.l. RTGS, BI-SSSS, dan SKN), atau selaku implementor, juga bertanggung jawab terhadap pelindungan data pribadi dalam sistem tersebut dan juga data pribadi lain yang dikelolanya seperti data pegawai, data kesehatan pegawai dan data *stakeholders* terkait lainnya. Terhadap poin kedua, Bank Indonesia belum memiliki peraturan eksternal yang secara khusus mengatur pelindungan data pribadi tersebut. Ketiga, BI sebagai pengawas sistem pembayaran atau selaku *overseer* juga memiliki peran dan tanggung jawab terhadap pihak-pihak yang diawasi terkait dengan data pribadi yang mereka kelola termasuk data sharing dalam penanganan *fraud* antar lembaga jasa keuangan.

Selain BI, perubahan ke arah digitalisasi ini juga berdampak pada sektor lembaga jasa keuangan seperti perbankan dan *financial technology* (*fintech*). Hal ini dapat terlihat dari cara kerja perbankan, mulai dari cara nasabah mengakses layanan perbankan hingga cara bank mengelola operasionalnya. Secara umum, pengaruh digitalisasi dalam sektor perbankan dapat dikategorikan menjadi dua, yaitu[10]: Pertama, peningkatan aksesibilitas layanan perbankan menjadi semakin luas dalam memberikan pelayanan kepada masyarakat sehingga mendorong inklusifitas sektor perbankan yang didorong dengan meningkatnya penggunaan *smartphone* dan internet. Berdasarkan data Bank Indonesia, transaksi uang elektronik di Indonesia mencapai Rp 38,51 triliun hingga Agustus 2023. Nilai ini tumbuh 8,62% jika dibandingkan dengan tahun sebelumnya dengan nilai transaksi yang di dominasi oleh QRIS sebesar 18,33 triliun (tumbuh sekitar 89,64%),[11] Transaksi uang elektronik ini diantaranya transaksi pembayaran, seperti pembelian pulsa, pembelian barang dan jasa, dan pembayaran tagihan. Kedua, digitalisasi juga meningkatkan efisiensi operasional perbankan dengan mengurangi biaya operasionalnya, seperti biaya tenaga kerja dan biaya infrastruktur. Hal ini karena bank tidak perlu lagi menyediakan kantor cabang yang besar dan banyak. Namun penggunaan teknologi dan digitalisasi ini juga berdampak pada risiko timbulnya *fraud* sehingga diperlukan koordinasi antar lembaga jasa keuangan dan juga dengan Bank Indonesia untuk memitigasi risiko tersebut.

Pada sektor *fintech*, hingga Q3 tahun 2022, industri *fintech* di Indonesia mendominasi hingga sekitar 33% dari total pendanaan perusahaan *fintech* di Asia Tenggara, kedua terbesar setelah Singapura.[12] Peningkatan yang cukup signifikan ini tidak terlepas dari upaya Pemerintah dan regulator dalam mendukung perkembangan *fintech* melalui regulasi seperti diterbitkannya UU No. 27 tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)

---

[7]Astfalk, S., & Schunck, C. H, "Balancing Privacy and Value Creation in the Platform Economy: The Role of Transparency and Intervenability", Balancing Privacy and Value Creation in the Platform Economy. 10.18420/OID2023_12, 2023. Diakses pada: 23 April 2024

[8]Hui, K. L., & Png, I. P, "Economics of privacy. Handbooks in Information Systems", Vol. 1. Elsevier. https://www.comp.nus.edu.sg/~ipng/research/privacy_HISE.pdf, 2005. Diakses pada: 24 April 2024

[9]Siaran Pers No.138/HM/KOMINFO/07/23, "Perkembangan Penanganan Dugaan Kebocoran Data Paspor 34,9 Juta Warga Indonesia", https://www.kominfo.go.id/content/detail/50065/siaran-pers-no-138hmkominfo072023-tentang-perkembangan-penanganan-dugaan-kebocoran-data-paspor-349-juta-warga-indonesia/0/siaran_pers. Diakses pada: 18 April 2024

[10]Otoritas Jasa Keuangan, "Roadmap Perusahaan Pembiayaan 2023-2027", 2023. Diakses pada: 16 April 2024

[11] Siaran Pers Bank Indonesia, "BI 7-Day Reverse Repo Rate Tetap 5,75%: Sinergi Menjaga Stabilitas Dan Mendorong Pertumbuhan". Diakses pada: 16 April 2024

[12]Siaran Pers AFTECH AMS 2022/2023, "Industri Fintech Indonesia Mantap Melangkah Menuju Arah Keberlanjutan dan Inklusi", https://fintech.id/id/dokumen/siaran-pers-aftech-annual-members-survey-20222023-industri-fintech-indonesia-mantap-melangkah-menuju-arah-keberlanjutan-dan-inklusi27 Juli 2023. Diakses pada: 17 April 2024

dan UU No. 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK). Dukungan tersebut bertujuan untuk menghindari adanya permasalahan yang perlu untuk diwaspadai seperti *tech winter*, pinjaman online, penggunaan QRIS Mancanegara, dan perkembangan *artificial intelligence* (AI).[13] Namun demikian, disamping dua undang-undang di atas, masih diperlukan peraturan teknis guna memberi pemahaman dalam pelaksanaan di lapangan sehingga pengawasan dan *law enforcement* nya bisa lebih optimal dan efisien.

Selain itu, era digitalisasi ini pun telah mendorong pemrosesan data pribadi semakin masif dan telah menimbulkan kebutuhan untuk pelindungan hukum yang komprehensif, spesifik, dan memadai bagi subjek data pribadi[14], terutama saat terjadi kebocoran data atau *fraud* di sektor keuangan. Terdapat beberapa kasus kebocoran data, baik terjadi internal di Bank Indonesia maupun eksternal di perbankan di bawah kewenangan Bank Indonesia. Kasus kebocoran data yang terjadi pada internal Bank Indonesia terjadi pada akhir 2021, dimana Bank Indonesia terkena ransomware dan hacker nya mengambil beberapa data internal Bank Indonesia.[15] Dari sisi eksternal, Pada November 2023, nasabah PT Bank Central Asia Tbk di Salatiga mengalami kehilangan saldo sebesar 68,5 juta rupiah dari rekeningnya melalui transaksi QRIS yang dilakukan beberapa kali.[16] Pakar Siber, Dr. Pratama Persadha mengatakan terkait kasus ini, selain mitigasi, hal yang harus mendapat perhatian pada kebocoran data adalah kesadaran keamanan siber sejak membangun sistem dan faktor keamanan menjadi prioritas.[17] Kesadaran pentingnya keamanan sejak membangun sistem perlu menjadi prioritas bagi penyelenggara untuk menggandeng ahli hukum sejak awal agar dapat dikawal sampai dengan penyusunan peraturannya untuk membantu mengatur mitigasi risikonya. Peneliti memandang bahwa Bank Indonesia memiliki kepentingan dan tanggung jawab untuk membuat aturan terkait PDP guna mencegah hal tersebut terjadi di kemudian hari. Oleh karena itu, pentingnya BI menyusun peraturan baik bagi eksternal (bagi lembaga jasa keuangan yang berada di bawah kewenangannya) dan juga bagi internal (bagi satuan kerja terkait) yang memiliki risiko dalam mengamankan data pribadi.

Kepercayaan digital/*digital trust* dan keamanan data pribadi menjadi pilar penting dalam era teknologi modern saat ini. *Digital trust* dapat memberikan dampak positif pada hubungan komunikasi dengan nasabah atau calon nasabah. Nasabah akan lebih nyaman dalam menggunakan instrument digital dalam system pembayaran tanpa khawatir datanya disalahgunakan atau diretas. Membangun kepercayaan digital memerlukan kombinasi pendekatan yang menggabungkan teknologi, keamanan, komunikasi dan transparansi, serta literasi kepada pelanggan. Pengembangan *digital trust* juga penting untuk memitigasi risiko, meningkatkan keyakinan konsumen, serta memanfaatkan layanan dan produk keuangan digital yang menyakinkan konsumen bahwa aset, data, dan privasinya terjaga dengan aman.[18]

Banyaknya aktivitas yang dilakukan secara online, mulai dari transaksi keuangan hingga interaksi sosial, perlindungan data pribadi menjadi sebuah kebutuhan. Kepercayaan digital dibangun melalui kredibilitas, transparansi, keamanan yang andal, serta kepatuhan terhadap regulasi yang berlaku/integritas.[19] Data pengguna harus dikelola dengan integritas, tidak disalahgunakan, dan terlindungi dari ancaman seperti peretasan atau pencurian identitas. Dalam ekosistem digital yang sehat, baik individu maupun perusahaan memiliki tanggung jawab bersama untuk menerapkan praktik keamanan terbaik sehingga

[13]Rezkiana Nisaputra, "Permasalahan Fintech yang harus diwaspadai di 2024", 29 Desember 2023. https://infobanknews.com/ini-dia-7-permasalahan-fintech-yang-harus-diwaspadai-di-2024/. Diakses pada: 19 April 2024

[14] Purnama, T.D. & Alhakim, A. (2021). Pentingnya UU Perlindungan Data Pribadi sebagai bentuk Perlindungan Hukum terhadap Privasi di Indonesia. e-Journal Komunitas Yustisia Universitas Pendidikan Ganesha. Diakses pada: 19 April 2024

[15]Tempo.co," Data Bank Indonesia diretas Geng Ramsomware, Kaspersky sebut Conti sangat Aktif", 20 Januari 2022. https://tekno.tempo.co/read/1552218/data-bank-indonesia-diretas-geng-ransomware-kaspersky-sebut-conti-sangat-aktif, 20 Januari 2022. Diakses pada: 25 April 2024

[16]CNBC Indonesia, "Heboh Nasabah BCA Kebobolan Rp68,5 Juta, Begini Kronologinya". https://www.cnbcindonesia.com/market/20231113141815-17-488611/heboh-nasabah-bca-kebobolan-rp685-juta-begini-kronologinya. Diakses pada: 25 April 2024

[17]Antara News, "Pakar sebut kebocoran data BI perlu segera dihentikan", 31 Januari 2022. https://www.antaranews.com/berita/2674793/pakar-sebut-kebocoran-data-bi-perlu-segera-dihentikan. Diakses pada: 25 April 2024

[18]Kominfo, "Urgensi Digital Trust dalam Pengaplikasian TTE Sektor Keuangan", 2022, https://aptika.kominfo.go.id/2022/10/urgensi-digital-trust-dalam-pengaplikasian-tte-sektor-keuangan/. Di akses pada: 30 November 2024

[19]KPMG, "Digital Trust", 2015, https://assets.kpmg.com/content/dam/kpmg/pdf/2015/12/digital-trust.pdf. Di akses pada: 30 November 2024

kepercayaan digital dapat ditingkatkan dan menciptakan lingkungan digital yang lebih aman dan terpercaya.

Munculnya kasus-kasus kebocoran data pribadi/*data fraud* di Indonesia menandakan diperlukannya suatu peraturan yang melindungi subjek data pribadi guna memitigasi risiko tersebut. Seperti yang dituliskan oleh Wiwoho dkk (2022), diperlukan kerangka hukum yang komprehensif untuk mengatasi tantangan yang ditimbulkan oleh penggunaan pembayaran digital dan untuk mencegah penyalahgunaan yang dapat mengarah pada kejahatan keuangan seperti pencucian uang dan pendanaan terorisme.[20] Di sektor keuangan, penulis menilai industri perlu memiliki payung hukum untuk dapat dipatuhi, dipahami, dan diimplementasikan dengan baik, sehingga *legal function* terkait PDP dapat dijalankan secara efisien. Oleh sebab itu, selain hadirnya UU PDP, perlu diatur ketentuan pelaksanaan teknis berupa Peraturan Pemerintah dan Peraturan yang dibuat oleh BI. Bank Sentral selaku otoritas moneter, sistem pembayaran dan makroprudensial, juga memiliki kepentingan dan tanggung jawab untuk ikut mengatur dan mengawasi keamanan dan pelindungan data pribadi untuk sektor keuangan di bawah kewenangannya dan juga di internalnya. Pengaturan tersebut termasuk pula mengatur mengenai koordinasi antar regulator di sektor keuangan terkait pelindungan data pribadi, dalam hal ini khususnya, antara Bank Indonesia dan Lembaga pengawas PDP. Oleh karena itu, penelitian ini akan menggali lebih dalam untuk mengeksplorasi prinsip-prinsip yang dapat menjadi pedoman/*guideline* bagi lembaga jasa keuangan (LJK), pertukaran data di antara lembaga jasa keuangan serta kerangka hukum pelindungan data pribadi di BI sebagai mandat dari UU PDP. Harapannya dalam pengaturan tersebut dapat memberikan panduan bagi penguatan sistem pelindungan data pribadi di masa depan serta prinisip-prinsip umum yang dijadikan sebagai pedoman terkait pelindungan data pribadi sehingga dapat dipatuhi dan diimplementasikan oleh berbagai pihak (baik eksternal maupun internal), namun tetap mempertimbangkan kepentingan dan pengembangan lembaga jasa keuangan.

Penelitian terkait topik ini belum banyak di-eksplorasi khususnya mengenai bagaimana Bank Indonesia selaku otoritas di sektor keuangan menindaklanjuti mandat yang diberikan UU PDP dalam mempersiapkan pengaturan baik bersifat eksternal maupun internal dalam rangka implementasi UU PDP yang akan berlaku tahun 2024 ini. Penelitian ini juga untuk melihat bagaimana bentuk pengaturan koordinasi/hubungan kelembagaan antara BI dan industri di bawah kewenangannya. Riset ini diharapkan dapat memberikan rekomendasi kebijakan dan rekomendasi teknis bagi BI selaku regulator, implementor dan *overseer* terhadap industri di sektor keuangan (perbankan dan *fintech*) dan juga sebagai pengelola data pribadi secara internal terkait kepegawaian dan *stakeholders* terkait.

2. Studi Literatur

2.1 Konsep Dasar Keamanan Data Pribadi

Dalam era digital yang makin berkembang pesat, data pribadi telah menjadi salah satu isu yang dibicarakan secara global saat ini karena merupakan salah satu aset paling berharga bagi setiap subjek data sehingga perlu adanya pengaturan mengenai kewajiban untuk menjaga kerahasiaan dan keamanan datanya. Pelindungan data pribadi merupakan hak dasar sebagaimana Pasal 8(1) Charter of Fundamental Rights of the European Union dan Pasal 16(1) dari Treaty on the Functioning of the European Union (TFEU) yang menyatakan bahwa setiap orang memiliki hak atas pelindungan data pribadi yang berkaitan dengan dirinya.[21] Prinsip dan aturan mengenai pelindungan data pribadi, terlepas dari kebangsaan atau tempat tinggal mereka, menghormati hak-hak dan kebebasan dasar mereka, khususnya hak atas pelindungan data pribadi.[22]

Menurut General Data Protection Regulation (GDPR), data pribadi ialah informasi apa pun yang berkaitan dengan individu yang teridentifikasi atau dapat diidentifikasi. Individu yang dapat diidentifikasi adalah orang yang dapat diidentifikasi, baik secara langsung atau

[20]Jamal Wiwoho, Dona Budi Kharisma, Dwi Tjahja K. Wardhono, "Financial Crime in Digital Payments", *Journal of Central Banking Law and Institutions Vol 1 No 1,* 2022.
[21]European Union Law, "Directive (EU) 2016/680 of the European Parliament and of the Council", 27 April 2016 https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC. Diakses pada: 13 Mei 2024
[22]Ibid

tidak langsung, khususnya dengan mengacu pada suatu pengidentifikasi seperti nama, nomor identifikasi, data lokasi, pengidentifikasi online atau pada satu atau lebih faktor yang spesifik terhadap kondisi fisik, fisiologis, identitas genetik, mental, ekonomi, budaya atau sosial dari orang perseorangan tersebut.[23] GDPR ini menjadi acuan dan diadop oleh negara-negara di Uni Eropa dan juga beberapa negara di ASEAN seperti Indonesia,Singapura dan Thailand.[24]

Di Indonesia sendiri, pelindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi. Pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi yang berasaskan pelindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan.[25]

Berlandaskan UU PDP, data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.[26] Data pribadi sendiri terdiri dari data yang bersifat spesifik dan umum. Data pribadi yang bersifat spesifik meliputi: data dan informasi kesehatan; data biometrik; data genetika; catatan kejahatan; data anak; data keuangan pribadi; dan/ atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Sedangkan data pribadi yang bersifat umum meliputi: nama lengkap; jenis kelamin; kewarganegaraan; agama; status perkawinan; dan/ atau data pribadi yang dikombinasikan mengidentifikasi seseorang.[27]

Dirjen Aplikasi dan Informatika (Aptika) Kemenkominfo dalam laman resmi Kominfo menjelaskan bahwa terdapat 4 (empat) tujuan yang menjadi latar belakang disusunnya UU PDP.[28] Pertama, bertujuan untuk memiliki kontrol atas data pribadi yang termasuk hak asasi dan privasi dimana ditegaskan dalam Pasal 12 Deklarasi Universal Manusia 1948 dan Pasal 16 Konvensi Internasional tentang Hak Sipil dan Politik (ICCPR) 1966, dimana Indonesia telah meratifikasi keduanya. Kedua, data pribadi merupakan aset atau komoditas bernilai tinggi di era *big data* dan ekonomi digital. Ketiga, UU PDP dimaksudkan untuk meminimalisir pelanggaran privasi dengan pengenaan sanksi. Terakhir, penyalahgunaan data pribadi dan meningkatkan kesadaran masyarakat untuk menjaga data pribadi sendiri. Penulis menilai bahwa tujuan penerbitan UU PDP dan aturan teknis nya ini memiliki 3 (tiga) fungsi utama yaitu pertama melindungi dan meningkatkan kesadaran masyarakat terhadap hak kendali atas subjek data pribadi yang merupakan hak dasar/asasi, kedua, mengatur pemerintah, pelaku bisnis dan pihak terafiliasi untuk memahami hak dan kewajibannya mematuhi peraturan yang berlaku dan kewajiban menjaga kerahasiaan dan keamanan data, dan ketiga, memberi kepastian hukum dan mendorong pertumbuhan industri teknologi, informasi dan komunikasi.

Selanjutnya, Personal Information Protection and Electronic Documents Act (PIPEDA) di Kanada, menerangkan bahwa keamanan data pribadi diperlukan guna melindungi informasi pribadi yang dikumpulkan, digunakan atau diungkapkan. Data pribadi adalah informasi tentang individu yang dapat diidentifikasi, seperti nama, alamat, nomor identifikasi, informasi biometrik, rekaman kesehatan, atau informasi yang dapat mengidentifikasi individu tersebut.[29] Selain itu, PIPEDA Act menetapkan aturan dasar tentang cara organisasi sektor swasta mengumpulkan, menggunakan, dan mengungkapkan

[23]European Union Law, "Regulation (EU) 2016/679 of the European Parliament and of the Council", https://eur-lex.europa.eu/eli/reg/2016/679/oj. Diakses pada: 20 Maret 2024

[24]ASEANBriefing, "Indonesia's Comprehensive Personal Data Protection Law Guide", https://www.aseanbriefing.com/doing-business-guide/indonesia/company-establishment/personal-data-protecti on-law; One Trust Data Guidance, "Comparing Privacy Laws: GDPR VS. Singapore's PDPA", https://www.dataguidance.com/sites/default/files/gdpr_v_singapore_2022_july_update.pdf; One Trust Data Guidance, "Comparing Privacy Laws: GDPR VS. Thai Personal Data Protection Act", https://www.dataguidance.com/sites/default/files/gdpr_v_thailand_updated.pdf. Diakses pada: 24 Mei 2024

[25]JDIH BPK, "Undang-Undang Perlindungan Data Pribadi", 2022, Diakses pada: 18 Maret 2024

[26]Ibid

[27]JDIH BPK, "Undang-Undang Perlindungan Data Pribadi", 2022, Diakses pada: 18 Maret 2024

[28]Kominfo, "5 Alasan Mengapa Data Pribadi Perlu Dilindungi", 16 Juli 2019, https://www.kominfo.go.id/content/detail/19991/5-alasan-mengapa-data-pribadi-perlu-dilindungi/0/sorotan _media. Diakses pada: 18 Maret 2024

[29]Personal Information Protection and Electronic Documents Act. 2000. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html#h-416889. Diakses pada: 20 Maret 2024

informasi pribadi dalam rangka kegiatan komersial. PIPEDA juga berlaku untuk informasi pribadi karyawan bisnis yang diatur oleh pemerintah federal.[30]

Pada California Consumer Privacy Act (CCPA), dirancang untuk melindungi hak konsumen dengan memastikan bahwa perusahaan bertanggung jawab dalam pengelolaan data pribadi dan bahwa konsumen memiliki hak untuk mengontrol informasi mereka. California Consumer Privacy Act (CCPA) concern terhadap keamanan data pribadi dari konsumen.[31] CCPA memberi konsumen kontrol lebih besar atas informasi pribadi yang dikumpulkan oleh perusahaan. CCPA sendiri mendefinisikan data pribadi merupakan informasi yang mengidentifikasi, berkaitan dengan konsumen atau rumah tangga tertentu. Hal tersebut termasuk namun tidak terbatas pada nama, alamat, nomor jaminan sosial, pengenal pribadi unik, alamat IP, alamat email, informasi akun, dan informasi geolokasi.[32]

Pada keamanan data, terdapat langkah-langkah yang dilakukan untuk melindungi data dari akses, perubahan, atau penghapusan yang tidak sah dan memastikan data tetap aman. Hal ini penting untuk melindungi data pribadi, finansial, atau informasi sensitif lainnya dari ancaman. Langkah-langkah ini merupakan elemen yang digunakan untuk mengubah data mentah menjadi informasi yang dapat digunakan dan dipahami oleh seluruh organisasi. Melalui serangkaian langkah sistematis yang mencakup pengumpulan, penyaringan, pengurutan, pemrosesan, analisis, penyimpanan, dan penyajian data untuk mendukung keamanan data pengambilan keputusan.[33,34] Terdapat 6 langkah dalam proses data yang digambarkan berikut **(Lampiran 1)**.

Dari gambar di atas, menjelaskan data proses yang dimulai dari pengumpulan data sebagai langkah pertama. Data mentah yang dikumpulkan memiliki dampak besar pada output yang dihasilkan karena data mentah yang dikumpulkan harus dari sumber yang terdefinisi dan akurat sehingga temuan selanjutnya valid dan dapat digunakan. Selanjutnya, langkah kedua, persiapan data atau pembersihan data adalah proses pengurutan dan penyaringan data mentah untuk menghapus data yang tidak perlu dan tidak akurat. Data mentah diperiksa kesalahannya, duplikasi, salah perhitungan atau data yang hilang, dan diubah menjadi bentuk yang sesuai untuk analisis dan pemrosesan lebih lanjut. Ini dilakukan untuk memastikan bahwa hanya data berkualitas tinggi yang dimasukkan ke dalam unit pemrosesan.

Langkah ketiga ialah input data. Dalam langkah ini, data mentah diubah menjadi bentuk yang dapat dibaca mesin dan dimasukkan ke dalam unit pemrosesan. Input data dapat berupa entri data melalui *keyboard*, pemindai, atau sumber input lainnya. Langkah keempat, pemrosesan data. Data mentah dikenakan berbagai metode pemrosesan data menggunakan algoritma pembelajaran mesin dan kecerdasan buatan untuk menghasilkan output yang diinginkan. Langkah ini dapat sedikit bervariasi dari satu proses ke proses lainnya tergantung pada sumber data yang diproses.

Langkah kelima, output, yaitu proses transmisi dan ditampilkannya data kepada pengguna dalam bentuk yang dapat dibaca seperti grafik, tabel, file vektor, audio, video, atau dokumen. Langkah terakhir pemrosesan yaitu penyimpanan, di mana data dan metadata disimpan untuk penggunaan lebih lanjut. Hal tersebut akan mempermudah akses dalam pengambilan informasi kapan pun dibutuhkan, serta memungkinkan data tersebut digunakan sebagai input langsung dalam siklus pemrosesan data berikutnya.

Dalam pemrosesan data terdapat pemrosesan lintas batas yang terdiri dari 2 hal, yaitu pemrosesan data pribadi yang terjadi dalam konteks aktivitas perusahaan di lebih dari satu Negara Anggota yang memiliki pengontrol atau pemroses di perhimpunan di mana pengontrol atau pemroses tersebut didirikan lebih dari satu Negara Anggota; atau pemrosesan data pribadi yang terjadi dalam konteks aktivitas satu lembaga pengontrol atau

[30]Privacy Commissioner of Canada, "PIPEDA requirements in brief", 2024, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/. Di akses pada: 20 Maret 2024

[31]State of California Department of Justice Office of the Attorney General, "California Consumer Privacy Act (CCPA)", 2024, https://oag.ca.gov/privacy/ccpa. Diakses pada: 21 Maret 2024

[32]California Consumer Privacy Act (CCPA), California Department of Justice, 2024. https://oag.ca.gov/privacy/ccpa. Diakses pada: 21 Maret 2024

[33]Nikita Duggal, "What Is Data Processing: Cycle, Types, Methods, Steps and Examples", 24 Juli 2023, https://www.simplilearn.com/what-is-data-processing-article#examples_of_data_processing. Diakses pada: 20 Agustus 2024

[34]Fullstory, "What is data processing? Definition, steps & methods", 14 Maret 2024, https://www.fullstory.com/blog/what-is-data-processing/. Diakses pada: 15 Mei 2024

pemroses di Uni Eropa, namun yang secara substansial berdampak atau kemungkinan besar akan berdampak signifikan terhadap subjek data di lebih dari satu Negara Anggota.

2.2 Peraturan dan Kebijakan Pelindungan Data Pribadi di Beberapa Negara

Peraturan dan Kebijakan Pelindungan Data Pribadi di berbagai negara mencerminkan upaya negara untuk melindungi privasi individu di tengah pesatnya perkembangan teknologi informasi. Setiap negara memiliki pendekatan yang berbeda-beda dalam menetapkan regulasi ini, disesuaikan dengan kebutuhan dan kondisi di masing-masing negara. Misalnya, Uni Eropa dengan General Data Protection Regulation (GDPR)-nya telah menetapkan standar ketat yang diikuti banyak negara lain sebagai model.

Pelindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi.[35] Pelindungan terhadap orang perseorangan sehubungan dengan pemrosesan data pribadi merupakan hak mendasar. Pasal 8 ayat (1) *the Charter of Fundamental Rights of the European Union* dan Pasal 16(1) *Treaty on the Functioning of the European Union* (TFEU) menyatakan bahwa setiap orang berhak atas pelindungan data pribadi tentang dirinya yang merupakan hak asasi manusia.[36]

General Data Protection Regulation (GDPR) adalah regulasi yang diberlakukan oleh Uni Eropa untuk melindungi data pribadi warga negara dan penduduknya. Diterapkan sejak 25 Mei 2018, GDPR menggantikan Data Protection Directive 95/46/EC dan dirancang untuk meningkatkan privasi dan memberikan kendali lebih besar kepada individu atas data pribadi mereka.[37] GDPR berlaku untuk semua organisasi yang memproses data pribadi individu di Uni Eropa, termasuk perusahaan di luar Uni Eropa yang menawarkan barang atau jasa kepada individu di Uni Eropa atau memantau perilaku mereka.[38] GDPR juga mewajibkan perusahaan untuk penunjukkan *Data protection Officer* (DPO).[39]

Sementara itu, Amerika Serikat memiliki pendekatan yang lebih terfragmentasi, dengan berbagai undang-undang federal dan negara bagian yang mengatur aspek-aspek spesifik pelindungan data. Sebagai contoh, California Consumer Privacy Act (CCPA), merupakan undang-undang privasi data di California, yang memberikan hak kepada konsumen untuk mengontrol bagaimana data pribadi mereka dikumpulkan, digunakan, dan dibagikan oleh perusahaan. CCPA tidak mewajibkan organisasi untuk menunjuk DPO. Namun, organisasi yang mengumpulkan atau memproses data pribadi diharuskan menunjuk orang yang bertanggung jawab untuk mengawasi kepatuhan organisasi terhadap CCPA. Orang yang bertanggung jawab dapat berupa karyawan atau vendor pihak ketiga.[40]

Di negara-negara ASEAN, seperti Malaysia memberlakukan Personal Data Protection Act (PDPA) melalui Personal Data Protection Department/Departemen Pelindungan Data Pribadi.[41] Di tahun 2024, Malaysia melakukan amandemen pada PDPA, dengan salah satu kebaruan yang dilakukan ialah penunjukan wajib DPO, dimana semua pengendali dan pemroses data harus menunjuk setidaknya satu DPO. Persyaratan ini berlaku tanpa memandang ukuran bisnis.[42]

Di negara Singapura, Personal Data Protection Act telah berlaku sejak tahun 2014, dan diterapkan oleh The Personal Data Protection Commission (PDPC)/Komisi Pelindungan

[35]JDIH BPK, "Undang-Undang Perlindungan Data Pribadi, https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022. Diakses pada: 18 Maret 20

[36]European Union Law, "Directive (EU) 2016/680 of the European Parliament and of the Council", https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC. Diakses pada: 13 Mei 2024

[37]Intersoft Consulting, "General Data Protection Regulation (GDPR)", 2018, https://gdpr-info.eu/. Diakses pada: 13 Mei 2024

[38]Official Journal of the European Union, "Regulations", 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Diakses pada: 13 Mei 2024

[39]Intersoft Consulting, "GDPR: Data Protection Officer", 2024, https://gdpr-info.eu/issues/data-protection-officer/. Diakses pada: 13 Mei 2024

[40]Secure Privacy, "What Is a Data Protection Officer and Do You Need One?", 19 Januari 2024, https://secure privacy.ai/blog/data-protection-officer-guide#:~:text=The%20CCPA%20does%20not%20require,or%20a%20third%2Dparty%20vendor. Diakses pada: 20 Mei 2024

[41]Malaysia Government, "Personal Data protection Actt 2010", 2010, https://www.pdp.gov.my/jpdpv2/assets/2019/09/Personal-Data-Protection-Act-2010.pdf. Diakses pada: 20 Mei 2024

[42]Hall Booth Smith, "Understanding Malaysia's 2024 Data Privacy Reform: Essential Insights for Business Leaders", 1 Oktober 2024. Diakses pada: 20 Mei 2024

Data Pribadi.[43] Berdasarkan Pasal 11(3) UU Pelindungan Data Pribadi, setiap organisasi yang tunduk pada UU Pelindungan Data Pribadi harus menunjuk setidaknya satu orang sebagai DPO. Semua organisasi yang menangani data pribadi di Singapura, terlepas dari ukuran atau industrinya, harus mematuhinya.[44]

Thailand telah memiliki Personal Data Protection Act, B.E. 2562 yang diterbitkan pada tahun 2019.[45] Pengendali Data dan Pengolah Data hanya diharuskan menunjuk petugas pelindungan data (DPO) jika memenuhi salah satu syarat diantaranya; 1) badan publik sebagaimana ditentukan dan diumumkan oleh Regulator; 2) memerlukan pemantauan berkala terhadap Data Pribadi atau sistem karena pengumpulan, penggunaan atau pengungkapan sejumlah besar Data Pribadi sebagaimana ditentukan oleh Regulator; atau 3) aktivitas inti Pengendali Data atau Pengolah Data melibatkan pengumpulan, penggunaan, atau pengungkapan Data Pribadi yang sensitif.[46]

Beberapa peraturan ini diperlukan untuk memastikan data setiap orang dilindungi dan digunakan sesuai peruntukannya dengan benar dan adil.[47] Sebab, jika data pribadi jatuh ke tangan yang salah, maka masyarakat bisa dirugikan, seperti korban pencurian identitas, diskriminasi atau bahkan kekerasan fisik.[48] Oleh karena itu, setiap pengaturan di atas mewajibkan untuk menunjuk DPO untuk memitigasi timbulnya kesalahan.

Di Indonesia sendiri telah diterbitkan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi yang substansinya mengacu pada GDPR. Dalam Bab VI Pasal 53 mewajibkan pengendali data menunjuk pejabat atau petugas yang melaksanakan fungsi Pelindungan Data Pribadi atau dikenal dengan *Data Protection Officer* (DPO).

2.3 Lembaga Pengawas Pelindungan Data Pribadi

Lembaga pengawas pelindungan data pribadi memainkan peran penting dalam mengawasi dan menegakkan hukum dan kebijakan terkait privasi dan keamanan data. Di Eropa, misalnya, General Data Protection Regulation (GDPR) menetapkan bahwa setiap negara anggota Uni Eropa harus memiliki otoritas pelindungan data nasional yang bertugas memastikan kepatuhan terhadap regulasi tersebut.[49]

Dewan Pelindungan Data Eropa (European Data Protection Board/EDPB) adalah badan independen Eropa yang didirikan oleh GDPR yang bertugas memastikan penerapan aturan pelindungan data yang konsisten di seluruh Uni Eropa. EDPB terdiri dari perwakilan otoritas pelindungan data nasional dari negara-negara UE/EEA (European Economic Area) dan Pengawas Pelindungan Data Eropa (European Data Protection Supervisor).[50]

Tugas-tugas EDPB terutama terdiri dari memberikan panduan umum tentang konsep utama GDPR dan Arahan Penegakan Hukum, memberikan saran kepada Komisi Eropa tentang isu-isu terkait pelindungan data pribadi dan undang-undang baru yang diusulkan di Uni Eropa, serta mengadopsi keputusan yang mengikat dalam perselisihan antara otoritas pengawas nasional.[51]

Di Amerika Serikat, meskipun tidak ada undang-undang pelindungan data yang seragam di tingkat federal, berbagai badan pengatur seperti Federal Trade Commission (FTC) berperan dalam melindungi konsumen dari praktik bisnis yang tidak adil atau menipu

[43]Personal Data Protection Commission Singapore, "PDPA Overview", 2024, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act. Diakses pada: 29 Mei 2024 dan 17 September 2024

[44]VeraSafe, "Singapore Data Protection Officers: Everything You Need to Know", 4 oktober 2024, https://verasafe.com/blog/singapore-data-protection-officers-everything-you-need-to-know/#:~:text=What%20law%20regulates%20data%20protection,data%20and%20bolster%20individuals'%20rights. Diakses pada: 29 Mei 2024

[45]Thailand Government, "Personal Data Protection Act, B.E. 2562", 2019, https://www.dataguidance.com/sites/default/files/entranslation_of_the_personal_data_protection_act_0.pdf. Diakses pada: 29 Mei 2024

[46]DLA PIPER, "Data Protection Officer in Thailand", 2024. Diakses pada: 29 Mei 2024

[47]Information Commissioner's Office, "The benefits of data protection laws", https://ico.org.uk/for-organisations/advice-for-small-organisations/the-benefits-of-data-protection-laws/#:~:text=And%20you%20have%20to%20protectdiscrimination%20or%20even%20physical%20harm. Diakses pada: 31 Mei 2024

[48]Ibid

[49]European Commission, "Data protection in the EU", 2016, https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en. Diakses pada: 3 Juni 2024

[50] Ibid

[51]European Data Protection Board, "task and duties", https://www.edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en. Diakses pada: 3 Juni 2024

terkait data pribadi.[52] FTC telah menjadi badan federal utama dalam kebijakan privasi dan penegakannya sejak tahun 1970-an. Perubahan teknologi yang cepat telah menimbulkan tantangan privasi baru, tetapi pendekatan keseluruhan FTC tetap konsisten. Badan ini menggunakan penegakan hukum, inisiatif kebijakan, serta edukasi konsumen dan bisnis untuk melindungi informasi pribadi konsumen. FTC akan mengambil tindakan hukum terhadap organisasi yang melanggar hak privasi konsumen, gagal menjaga keamanan informasi sensitif konsumen, atau menyebabkan kerugian signifikan bagi konsumen. Dalam banyak kasus ini, FTC menuntut organisasi karena melanggar Section 5 dari FTC Act, yang melarang tindakan dan praktik yang tidak adil dan menipu dalam atau yang mempengaruhi perdagangan.[53]

Di Indonesia, pengaturan mengenai lembaga pengawas tertuang pada Pasal 58 UU PDP Bab IX dimana penyelenggaraan pelindungan data pribadi dilakukan oleh lembaga yang ditetapkan dan bertanggung jawab kepada Presiden.[54] Lembaga Pengawas dimaksud dapat berkoordinasi dengan Bank Indonesia dalam kegiatan pengawasannya terhadap lembaga jasa keuangan yang berada di bawah kewenangan Bank Indonesia.

Dari pemaparan di atas, penulis menilai pentingnya memiliki adanya sinergi dan koordinasi yang erat antara lembaga pengawas Pelindungan Data Pribadi (PDP) dengan lembaga pengawas yang merupakan otoritas dari Lembaga yang berada di bawahnya. Dalam hal ini, BI sebagai otoritas pengawas, perlu berkoordinasi dengan Lembaga pengawas PDP, terkait dengan pengawasan terhadap industri keuangan. Koordinasi ini perlu di atur lebih lanjut oleh Bank Indonesia untuk memastikan pelindungan data pribadi diterapkan di sektor keuangan secara efektif, sehingga tidak menghambat pengembangan industri di sektor keuangan.

2.4 Prinsip-prinsip Pelindungan Data Pribadi

Prinsip-prinsip Pelindungan Data Pribadi merupakan landasan dalam menjaga keamanan dan privasi informasi individu serta memberi pedoman atau panduan dalam menyelesaikan permasalahan sehingga penyelenggaraan terkait pelindungan data pribadi dapat berjalan dengan baik. Prinsip-prinsip ini dirancang untuk memastikan bahwa pengumpulan, penggunaan, dan penyimpanan data pribadi dilakukan dengan cara yang sesuai prosedur dan bertanggung jawab. Rupp (2024) membagi 3 elemen dalam pelindungan data, yaitu elemen "tentang", “tujuan”, dan “hasil”. [55] Elemen “tentang” digunakan untuk menilai risiko privasi dengan benar, berguna untuk lebih memisahkan antara berbagai bidang privasi yang terpengaruh oleh pemrosesan data yang terdiri dari privasi inti seperti informasi intim atau konten percakapan pribadi. Lingkup pribadi biasa yang mencakup segala sesuatu yang terlindungi dari pandangan orang lain serta privasi di ruang publik, mencakup segala sesuatu yang dilakukan di tempat umum. Elemen tujuan berfokus pada risiko terhadap otonomi individu yang bertujuan untuk menilai apakah data digunakan untuk mengevaluasi dan memengaruhi status atau perilaku individu. Elemen hasil berfokus pada risiko terhadap hak dan kepentingan fundamental lainnya yang menyoroti efek negatif dari pemrosesan data terhadap hak dan kepentingan individu.[56]

Elemen-elemen ini memberikan kerangka kerja untuk menganalisis dampak pemrosesan data terhadap hak individu. Selain itu, memahami bahwa status data sebagai personal atau non-personal dapat berubah seiring waktu berdasarkan tujuan pemrosesan. Hal ini menekankan perlunya pendekatan dinamis dalam menilai pelindungan data. Paper ini juga memberikan wawasan yang mendalam tentang pentingnya pelindungan data pribadi, pengelompokan data, dan perlunya pendekatan yang tepat dalam mengatasi isu privasi

[52]Federal Trade Commission: Protecting America’s Consumers, “Protecting Consumer Privacy and Security”, 2024, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security. Diakses pada: 4 Juni 2024

[53]Federal Reserve, “Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices”, https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf. Diakses pada: 5 Juni 2024

[54]JDIH BPK, “Undang-Undang Perlindungan Data Pribadi”, 2022, https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022. Diakses pada: 18 Maret 2024

[55]Valentin Rupp dan Max von Grafenstein, “Clarifying “personal data” and the role of anonymisation in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection”,Computer Law & Security Review Vol. 52, April 2024, https://doi.org/10.1016/j.clsr.2023.105932. Diakses pada: 5 Juni 2024

[56]Ibid

dalam pemrosesan data.[57] Dengan memahami elemen-elemen tersebut, maka prinsip-prinsip mengenai pelindungan data pribadi menjadi hal yang penting untuk menjadi pedoman para pihak dalam mengelola dan memproses data pribadi.

GDPR juga mengeluarkan prinsip-prinsip terkait Pelindungan Data pribadi yang terdiri dari 7 Prinsip, yaitu[58]:

1. Prinsip-prinsip yang berkaitan dengan pemrosesan data pribadi (diproses secara sah, adil, dan transparan, dikumpulkan untuk tujuan-tujuan tertentu, akurat, serta tidak melanggar hukum
2. Keabsahan pemrosesan (sesuai dengan perjanjian)
3. Persyaratan persetujuan (menunjukkan bahwa subjek data telah menyetujui pemrosesan data pribadinya)
4. Kondisi yang berlaku untuk persetujuan anak dalam kaitannya dengan layanan masyarakat informasi
5. Pemrosesan kategori khusus data pribadi (pengolahan data genetik, data biometrik untuk tujuan mengidentifikasi seseorang secara unik)
6. Pemrosesan data pribadi yang berkaitan dengan hukuman pidana dan pelanggaran
7. Pemrosesan yang tidak memerlukan identifikasi

Organisation for Economic Co-operation and Development (OECD) mengeluarkan beberapa prinsip dasar pedoman privasi meliputi[59]:

1. Prinsip Pembatasan Pengumpulan Data (*Collection Limitation Principle*): Data pribadi hanya boleh dikumpulkan dalam batas-batas tertentu dan harus diperoleh dengan cara yang sah dan adil, serta dengan pengetahuan atau persetujuan subjek data jika diperlukan.
2. Prinsip Kualitas Data (*Data Quality Principle*): Data pribadi harus relevan dengan tujuan penggunaannya, akurat, lengkap, dan diperbarui sesuai kebutuhan.
3. Prinsip Spesifikasi Tujuan (*Purpose Specification Principle*): Tujuan pengumpulan data pribadi harus ditentukan sebelum pengumpulan dan data tersebut hanya boleh digunakan untuk tujuan yang telah ditentukan.
4. Prinsip Pembatasan Penggunaan (*Use Limitation Principle*): Data pribadi tidak boleh diungkapkan, dibuat tersedia, atau digunakan untuk tujuan selain yang telah ditentukan kecuali dengan persetujuan subjek data atau oleh otoritas hukum.
5. Prinsip Pelindungan Keamanan (*Security Safeguards Principle*): Data pribadi harus dilindungi dengan langkah-langkah keamanan yang memadai terhadap risiko-risiko seperti akses tidak sah, perusakan, modifikasi, atau pengungkapan data.
6. Prinsip Keterbukaan (*Openness Principle*): Harus ada kebijakan keterbukaan tentang perkembangan, praktik, dan kebijakan terkait data pribadi, serta sarana untuk memastikan bahwa informasi ini dapat diakses.
7. Prinsip Partisipasi Individu (*Individual Participation Principle*): Individu harus memiliki hak untuk mengetahui apakah data tentang dirinya disimpan dan, jika memungkinkan, harus diberikan akses kepada data tersebut untuk verifikasi dan koreksi jika diperlukan.
8. Prinsip Akuntabilitas (*Accountability Principle*): Pihak yang mengendalikan data harus bertanggung jawab untuk mematuhi langkah-langkah yang memastikan prinsip-prinsip di atas diterapkan.

Di Indonesia, UU PDP juga mengatur mengenai prinsip-prinsip pengelolaan data pribadi yang tertuang pada Pasal 16 ayat 2, yang terdiri dari **8 prinsip** yaitu:

[57]Valentin Rupp dan Max von Grafenstein, "Clarifying "personal data" and the role of anonymisation in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection",Computer Law & Security Review Vol. 52, April 2024, https://doi.org/10.1016/j.clsr.2023.105932. Diakses pada: 5 Juni 2024

[58]GDPR, "Principles", https://gdpr-info.eu/chapter-2/, 2018, Diakses pada: 13 Mei 2024

[59]OECD Legal Instrument, "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", 2013, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Diakses pada: 10 Juni 2024

1. Prinsip terbatas, spesifik, sah secara hukum dan transparan

Prinsip ini menentukan, bahwa data pribadi hanya boleh dikumpulkan untuk tujuan tertentu yang sah dan eksplisit, serta tidak boleh digunakan untuk tujuan lain yang tidak sesuai dengan tujuan awal pengumpulan.

2. Prinsip Pemrosesan sesuai dengan tujuan

Dalam prinsip ini, pemrosesan data pribadi harus **dibatasi hanya untuk tujuan yang disepakati**. Data pribadi yang dikumpulkan tidak boleh digunakan untuk tujuan lain tanpa persetujuan lebih lanjut dari pemilik data.

3. Prinsip Pemrosesan menjamin hak subjek data

Prinsip ini menjamin **Hak Subjek Data** sebagai inti dari regulasi pelindungan data pribadi, yang memastikan bahwa individu memiliki kendali atas data pribadi mereka dalam kegiatan pemrosesan data. Prinsip ini mengatur bagaimana data pribadi harus diproses oleh pengendali data dengan tetap menjamin hak-hak subjek data terlindungi dengan baik.

4. Prinsip Akurasi

Prinsip Akurasi dalam konteks pelindungan data pribadi mengacu pada kewajiban Pengendali Data untuk memastikan bahwa data pribadi yang dikumpulkan, disimpan, dan diproses harus selalu **akurat**, **relevan**, dan **diperbarui/dikoreksi** sesuai dengan kebutuhan tujuannya. Prinsip ini bertujuan untuk mencegah kesalahan atau ketidakakuratan dalam data pribadi yang dapat merugikan subjek data dan menjamin kualitas data yang digunakan.

5. Prinsip Keamanan

Prinsip Keamanan ini merujuk pada kewajiban pengendali data untuk memastikan bahwa data pribadi yang dikumpulkan, disimpan, dan diproses agar selalu dilindungi kerahasiaannya dengan baik dari segala ancaman, seperti akses yang tidak sah, pencurian, kerusakan, atau kehilangan. Prinsip ini mengharuskan organisasi atau entitas yang memproses data pribadi untuk mengambil langkah-langkah teknis dan organisasi yang tepat guna melindungi integritas, kerahasiaan, dan ketersediaan data.

6. Prinsip Pemberitahuan Tujuan dan aktivitas pemrosesan

Prinsip ini merupakan salah satu prinsip penting dalam pelindungan data pribadi yang menuntut transparansi dan keterbukaan dari pengendali data. Prinsip ini mengharuskan bahwa setiap kali data pribadi dikumpulkan, digunakan, atau diproses, subjek data harus **diberi tahu dengan jelas** mengenai tujuan pengumpulan dan aktivitas pemrosesan data tersebut.

7. Prinsip Pemusnahan dan Penghapusan

Prinsip ini berkaitan dengan kewajiban pengendali data untuk **menghapus** atau **memusnahkan** data pribadi yang tidak lagi diperlukan dalam kegiatan dan tujuan pemrosesan data yang sah. Prinsip ini menjamin bahwa data pribadi tidak disimpan dalam jangka waktu yang lebih lama dari yang diperlukan, sehingga mengurangi risiko penyalahgunaan, akses tidak sah, atau pelanggaran atas data privasi.

8. Prinsip Akuntabilitas

Prinsip ini mewajibkan pengendali data untuk **bertanggung jawab** dan mampu **membuktikan kepatuhan** mereka terhadap peraturan pelindungan data. Inti dari prinsip ini menekankan bahwa pengendali data tidak hanya harus mematuhi aturan yang berlaku, tetapi juga harus menunjukkan bahwa mereka telah melakukan langkah-langkah yang diperlukan untuk melindungi data pribadi secara efektif.

Prinsip-prinsip ini menurut hemat penulis, dapat dijadikan pedoman dan panduan pada pengaturan teknis untuk dapat diimplementasikan oleh pihak terkait, seperti Bank Indonesia selaku regulator, dan juga untuk mengatur industri, dan masyarakat yang pada akhirnya memberikan kejelasan dan jaminan serta kepastian hukum kepada privasi individu tentang bagaimana data mereka akan dikelola dan dilindungi. Prinsip-prinsip di atas selanjutnya di atur untuk menjadi Pedoman sehingga dapat dijadikan semacam protokol atau *standard operating procedure* (SOP) yang seragam, sebagai salah satu instrumen hukum paling umum dan efektif yang melindungi privasi individu.[60]

[60]Joanna Kulesza, "Privacy", In: Schintler, L., McNeely, C. (eds) Encyclopedia of Big Data. Springer, Cham. 2019, https://doi.org/10.1007/978-3-319-32001-4_314-1. Diakses pada: 11 Juli 2024

3. Data dan Metodologi

3.1 Jenis Data

Berdasarkan jenis data, sumber data yang diperoleh adalah data primer dan sekunder. Data primer didapat antara lain melalui *Focus Group Discussion* (FGD) dengan pihak Kominfo, satuan kerja Bank Indonesia, perbankan, perusahaan FinTech, serta otoritas terkait untuk melihat kebutuhan aturan teknis dalam rangka implementasi UU PDP, praktik kepatuhan, kesiapan dan tantangan yang di hadapi. Data sekunder, yaitu data yang diperoleh dari kepustakaan dan dokumen-dokumen terkait seperti peraturan pelaksana (UU dan PP), keputusan regulator, literatur-literatur dan berita yang berkaitan dengan permasalahan di Indonesia, termasuk dari lembaga pemerintah dan otoritas (antara lain dari bank sentral negara lain, Kominfo dan Badan Siber dan Sandi Negara) dan lembaga yang mengkaji PDP, guna mendukung penulisan riset PDP ini.

3.2 Metodologi

Pada penelitian ini, menggunakan metode yuridis normatif dengan menganalisis teks UU PDP dan peraturan pelaksana eksisting lainnya untuk memahami kerangka hukum yang mengatur pelindungan data pribadi di Indonesia serta melihat pengaturan yang dilakukan beberapa negara lainnya. Dari penggunaan metode ini diharapkan dapat memberikan rekomendasi kebijakan dan rekomendasi teknis bagi Bank Indonesia mengenai kerangka hukum dan substansi yang perlu diatur dalam peraturan pelaksana sesuai mandat yang diberikan PDP sehingga diharapkan peraturan yang dikeluarkan BI tersebut dapat harmonis dan seimbang dengan kebutuhan *stakeholders* terkait.

4. Hasil Penelitian

4.1 Pelindungan Data Pribadi di Bank Sentral Beberapa Negara

Pelindungan data pribadi memainkan peranan penting dalam upaya menjamin hak konstitusional subjek data pribadi sebagai salah satu aspek penting dari hak asasi manusia.[61] rinsip-prinsip pelindungan data pribadi merupakan pedoman dan menjadi landasan penting dalam menjaga privasi dan keamanan individu di era digital, terutama di sektor keuangan yang secara rutin dan masif mengelola data. Prinsip-prinsip ini berfungsi sebagai *guideline* bagi lembaga keuangan untuk memastikan bahwa data pribadi dikumpulkan, diproses, dan disimpan dengan cara yang aman dan sesuai dengan peraturan yang berlaku. Dengan menerapkan prinsip-prinsip ini, lembaga keuangan tidak hanya dapat memenuhi kewajiban hukum, tetapi juga membangun kepercayaan nasabahnya. Beberapa negara telah mengimplementasikan prinsip-prinsip Pelindungan Data Pribadi melalui pengaturan-pengaturan oleh bank sentralnya sebagai berikut.

4.1.1 Bank of England (BoE)

BoE menetapkan bahwa data pribadi akan ditangani sesuai dengan fungsinya sebagai bank sentral. BoE juga mengumpulkan data pribadi baik data *stakeholder*s yang di atur oleh BoE termasuk pegawainya. BoE berkomitmen untuk tetap menjaga keamanan data pribadi yang di proses untuk kepentingannya. BoE menghormati setiap hak-hak subjek data yang mereka simpan.[62]

BoE memiliki wewenang dalam pengawasan dan pendisiplinan berdasarkan Financial Services and Markets Act 2000 (FSMA), Banking Act 2009, dan berdasarkan pasal 8 European Union (Withdrawal) Act 2018 yang mungkin melibatkan pemrosesan data pribadi seperti pengumpulan data pribadi tentang kontak bisnis, pelanggan atau staf perusahaan, staf atau anggota masyarakat.[63]

BoE juga dapat memberikan kesempatan kepada subjek data untuk meminta koreksi atas informasi yang tidak lengkap atau tidak akurat serta dapat menyimpan data pribadi selama diperlukan untuk tujuan pengumpulannya, dan setiap tujuan lain yang tidak

[61]Lu Sudirman, Hari Sutra Disemadi, dan Arwa Meida Aninda, 2023, *Comparative Analysis of Personal Data Protection Laws in Indonesia and Thailand: A Legal Framework Perspective,* Journal of Etika Demokrasi, Vol. 8 No. 4.
[62]Bank of England, "Privacy and the Bank of England", 2024, https://www.bankofengland.co.uk/legal/privacy. Diakses pada: 7 Agustus 2024
[63]Ibid

bertentangan dengan hal ini. Periode penyimpanan untuk berbagai jenis informasi pribadi ditetapkan dalam Skema Klasifikasi Catatan Bank. Jika memungkinkan, BoE akan berusaha untuk menganonimkan informasi pribadi sehingga tidak dapat lagi dikaitkan dengan individu.

Penulis berpendapat bahwa BoE selaku regulator, disamping memberikan hak-hak tertentu bagi subjek data, namun juga dapat mengelola dan mengolah data yang dia terima untuk dapat digunakan dalam menjalankan kebijakannya sepanjang dibuat dalam bentuk anonym antara lain seperti *data masking*[64]. Data dalam bentuk *anonym/ pseudonymization* merupakan pelindungan tambahan yang harus digunakan dalam prinsip minimalisasi data, misalnya untuk melakukan riset tentang kesehatan.[65] Upaya BoE untuk melakukan *anonym* atau data masking dapat menjadi contoh bagi Bank Indonesia untuk mengatur penggunaan data masking atau data yang terenkripsi yang digunakan untuk pertukaran data antar lembaga jasa keuangan maupun dengan Bank Indonesia dalam penanganan *fraud*.

Hal ini tentu bermanfaat dalam rangka pertukaran data dengan tetap mempertimbangkan menjaga keamanan data bagi pihak-pihak terkait yang menjadi *stakeholders* untuk dapat saling bertukar informasi guna menjaga keamanan, kelancaran, dan juga pengembangan bagi ekosistem di lingkungan lembaga jasa keuangan, namun tetap menjalankan prinsip kehati-hatian.

4.1.2 Bangko Sentral Ng Pilipinas (BSP)

Pemerintah Filipina menerbitkan Undang-Undang Data Pribadi Tahun 2012 yang berfungsi sebagai dasar hukum untuk melindungi data pribadi dan berdasarkan mandat Undang-Undang No. 11211, atau dikenal sebagai "Undang-Undang Bank Sentral Baru", Bangko Sentral Ng Pilipinas (BSP) berkomitmen untuk secara proaktif menyediakan lingkungan yang melindungi hak-hak subjek data pribadi, menjaga data/informasi pribadi mereka, dan melembagakan tanggung jawab para pemangku kepentingan terkait.[66]

BSP memberikan kesempatan untuk mengubah atau memperbarui informasi pribadi serta permintaan koreksi dengan alasan yang memadai dan dalam jangka waktu yang wajar. BSP dapat memproses informasi pribadi yang mencakup, namun tidak terbatas pada informasi yang terkait dengan personil, kontak bisnis, nasabah atau staf lembaga keuangan dan non-keuangan yang diawasi dan diatur oleh BSP, atau masyarakat umum dalam rangka survei dan kegiatan serupa yang dimaksudkan untuk penelitian dan pembuatan kebijakan.[67]

4.1.3 Monetary Authority of Singapore (MAS)

Singapura telah memberlakukan Undang-Undang Pelindungan Data Pribadi (PDPA) pada tahun 2012, yang berfungsi sebagai dasar hukum untuk melindungi data pribadi.[68] UU Pelindungan Data Pribadi mengakui perlunya melindungi data pribadi individu dan perlunya organisasi untuk mengumpulkan, menggunakan atau mengungkapkan data pribadi untuk tujuan yang sah dan wajar. Oleh karena itu, Organisasi diharuskan untuk mematuhi berbagai kewajiban pelindungan data jika mereka melakukan aktivitas yang berkaitan dengan pengumpulan, penggunaan, atau pengungkapan data pribadi.

MAS sebagai Bank Sentral Singapura dapat mengumpulkan dan memproses informasi pribadi dalam perannya sebagai regulator keuangan dan pengawas industri keuangan di Singapura, dan untuk pelaksanaan fungsi hukumnya berdasarkan hukum dan peraturan yang berlaku yang dikelola oleh MAS.[69] Oleh sebab itu, MAS wajib mematuhi PDPA dalam menjalankan fungsinya.

---

[64]Data Masking adalah suatu proses dalam rangka melindungi informasi pribadi atau sensitif dengan menghapus atau mengenkripsi pengidentifikasi yang menghubungkan seseorang ke data yang disimpan.

[65]European Data Protection Board, "EDPB Documenton response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", di akses pada: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf, 2 February 2021. Diakses pada: 12 Agustus 2024

[66]Bangko Sentral Ng Pilipinas, "About the Bank", 2024, https://www.bsp.gov.ph/Pages/AboutTheBank/BSPPrivacyPolicy.aspx. Diakses pada: 10 September 2024

[67]Ibid.

[68]Personal Data Protection Commission Singapore, "PDPA Overview", 2024, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act. Diakses pada: 29 Mei 2024 dan 17 September 2024

[69]Monetary Authority of Singapore, "MAS Privacy Policy Statement", 2024, https://www.mas.gov.sg/privacy-statement#:~:text=Statement%20of%20Commitment%20and%20Assurance,that%20you%20share%20with%20us. Diakses pada: 17 September 2024

Kewajiban organisasi dalam hal ini MAS berdasarkan UU Perlindungan Data Pribadi untuk melindungi data pribadi diantaranya Pertama, memastikan bahwa organisasi memenuhi kewajibannya berdasarkan UU Pelindungan Data, seperti menyediakan informasi tentang kebijakan, praktik, dan proses pengaduan pelindungan data sesuai permintaan, menunjuk petugas pelindungan data (DPO), dan menyediakan informasi kontak bisnis kepada publik. Kedua, memberitahukan individu tentang tujuan dari mengumpulkan, menggunakan, atau mengungkapkan data pribadi mereka. Ketiga, pengumpulan, penggunaan, dan pengungkapan data pribadi serta tujuan penggunaan data berdasarkan persetujuan individu/subjek data. Keempat, kewajiban dalam pembatasan tujuan dari penggunaan data pribadi. Kelima, kewajiban akurasi, dimana data pribadi yang dikumpulkan akurat. Keenam, pengaturan keamanan untuk melindungi data pribadi yang dikelola. Ketujuh, pembatasan dalam penggunaan data. Kedelapan, dalam melakukan transfer data harus sesuai dengan peraturan. Kesembilan, pemberian akses dan perubahan kepada subjek terhadap data pribadi mereka. Kesepuluh, apabila terjadi pelanggaran data, organisasi diharuskan untuk memberi tahu PDPC dan individu yang terdampak sesegera mungkin. Kesebelas, kewajiban portabilitas data dengan format khusus/sistem yang dapat terbaca.[70]

Untuk mendukung penerapan UU Pelindungan Data Pribadi Singapura/Singapore Personal Data Act 2012 dan Amandemennya 2020, MAS pada tahun 2023 mengeluarkan kebijakan internal yaitu dalam Circular No ID 03/23 tentang Data Breach Notification untuk sektor Asuransi dan selalu berkoordinasi dengan Lembaga Pengawas Data Pribadi Singapore/PDPC. Dalam surat edaran tersebut MAS meminta agar sektor industri melaporkan data breach yang terjadi, bersamaan dengan pelaporan yang disampaikan kepada PDPC. Hal ini tentunya memudahkan koordinasi antara MAS dan PDPC untuk dapat segera menyelesaikan permasalahan yang terjadi, sekaligus tetap melindungi ekosistem pada industri asuransi.[71]

4.1.4 Bank Negara Malaysia (BNM)

Negara Malaysia telah memberlakukan Undang- Undang Pelindungan Data Pribadi (PDPA) pada tahun 2010 sebagai kerangka hukum untuk pelindungan data pribadi di negara tersebut. Undang-undang ini mengatur pengumpulan, penggunaan, dan pemrosesan informasi pribadi oleh entitas swasta dan komersial, memastikan bahwa data individu ditangani secara bertanggung jawab dan aman, serta memberikan hak kepada individu untuk mengakses dan mengoreksi data mereka.[72]

Sebagaimana prinsip-prinsip yang tertuang pada undang-undang tersebut, BNM mengumpulkan dan memproses data pribadi hanya untuk tujuan yang sah dan sesuai hukum. Prinsip ini mendasari komitmen bank terhadap transparansi dalam pengelolaan data, memastikan bahwa informasi pribadi digunakan secara tepat dan sesuai dengan hukum.[73] Berdasarkan prinsip pemberitahuan, BNM menginformasikan kepada individu mengenai tujuan pengumpulan data pribadi mereka dan memberikan pilihan kepada mereka untuk memberikan data tersebut. Hal ini memastikan bahwa individu sepenuhnya menyadari bagaimana data mereka akan digunakan dan memberikan mereka kesempatan untuk menyetujui atau menolak pengumpulan informasi pribadi mereka.

BNM juga mematuhi prinsip keterbukaan dan prinsip keamanan dengan memastikan bahwa data pribadi tidak diungkapkan kepada pihak ketiga yang tidak berwenang dan dilindungi melalui langkah-langkah keamanan yang ketat. Data pribadi yang dimiliki oleh BNM hanya dibagikan kepada entitas yang berwenang untuk tujuan tertentu, sementara protokol keamanan data tingkat lanjut diterapkan untuk melindungi dari pelanggaran, penyalahgunaan, atau akses yang tidak sah. Hal ini sejalan dengan persyaratan PDPA untuk memastikan kerahasiaan dan integritas informasi pribadi.

---

[70]Personal Data Protection Commission, "Data Protection Obligations", 2024, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act/data-protection-obligations. Diakses pada: 17 September 2024

[71]Monetary Authority of Singapore, "Notification of Data Breaches to The Monetary Authority Of Singapore ("THE AUTHORITY"), 22 February 2023, https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/id/id03_23/id03_23.pdf. Diakses pada: 23 September 2024

[72]Parliament of Malaysia, "Personal Data Protection Act 2010", 2010, https://mohre.um.edu.my/img/files/Personal%20Data%20Protection%20(PDPA)%20Act%202010.pdf. Diakses pada: 23 September 2024

[73]Bank negara Malaysia, Privacy Statement"2024, https://www.bnm.gov.my/privacy-statement#:~:text=The%20Bank%20does%20not%20collect,your%20browser%20history%20(cache). Diakses pada: 23 September 2024

BNM juga mengikuti prinsip penyimpanan, integritas data, dan akses dengan menyimpan data pribadi hanya selama diperlukan, memastikan keakuratan dan kelengkapan data, serta memberikan hak kepada individu untuk mengakses dan memperbaiki data pribadi mereka. Kerangka kerja ini membantu BNM mempertahankan standar integritas data tertinggi, memastikan bahwa hak-hak individu dihormati dan data pribadi ditangani sesuai dengan ketentuan hukum PDPA Malaysia. BNM dapat mengungkapkan data pribadi Anda kepada pihak ketiga jika diijinkan atau diwajibkan oleh hukum/peraturan.[74]

4.1.5 Bank of Thailand (BOT)

Thailand memiliki Undang-Undang Pelindungan Data Pribadi (PDPA) Thailand yang diterbitkan pada tanggal 27 Mei 2019. Bank of Thailand (BOT) sebagai Bank Sentral memastikan bahwa data pribadi dikumpulkan, digunakan, dan diungkapkan secara bertanggung jawab. Prinsip-prinsip yang diatur ialah batasan pengumpulan data, pemberitahuan dan persetujuan, pemrosesan data pribadi yang sensitif, dan transfer data lintas batas yang sejalan dengan standar internasional untuk pelindungan data.[75]

Pengumpulan dan pemrosesan data oleh BOT dilakukan untuk pelaksanaan tugas sebagai bank sentral terhadap lembaga keuangan dan sistem pembayaran, dalam rangka memastikan stabilitas moneter dan ekonomi serta perlindungan bagi pengguna layanan keuangan yang dioperasikan oleh lembaga keuangan yang diatur.[76] Selanjutnya, terkait dengan pengawasan, pemeriksaan lembaga keuangan, dan pengembangan sistem pembayaran, BOT memproses data termasuk data pribadi yang diterima dari lembaga keuangan dan operator layanan keuangan untuk memastikan stabilitas ekonomi dan keuangan. Selain itu, pemrosesan bertujuan melaksanakan tugas BOT sehubungan dengan perlindungan pengguna layanan keuangan serta tugasnya sebagai penyedia infrastruktur pembayaran penting, misalnya, sistem Bank of Thailand Automated High-Value Transfer Network (BAHTNET). Oleh karena itu, pemrosesan data pribadi pengguna oleh BOT sangat penting untuk koordinasinya dengan lembaga keuangan dan untuk tindakannya terkait pemberian saran atau pelaksanaan kegiatan terkait.[77]

Dalam menjalankan perannya, BOT mengikuti peraturan dan standar internasional tentang keamanan data pribadi, dan telah menerapkan langkah-langkah berbasis risiko untuk melindungi hak, kebebasan, dan kepentingan subjek data. Pemrosesan data pribadi harus dilakukan secara sah, adil, dan transparan sesuai dengan prinsip tata kelola data. Selain itu, data pribadi harus akurat dan selalu diperbarui. Lebih lanjut, data pribadi harus disimpan hanya untuk jangka waktu yang diperlukan untuk memenuhi tujuan yang ditentukan. Selanjutnya, penggunaan atau pengungkapan data pribadi kepada pihak ketiga seperti instansi Pemerintah, rumah sakit, atau badan hukum terkait lainnya harus dilakukan sesuai dengan tujuan yang ditetapkan untuk melaksanakan tugas BOT, atau untuk tujuan melaksanakan tugasnya berdasarkan peraturan perundang-undangan lainnya, atau untuk kepentingan yang sah dari BOT atau orang lain maupun badan hukum.[78]

Penunjukkan DPO dilakukan jika memenuhi salah satu syarat diantaranya: 1)pemrosesan dilakukan oleh badan atau otoritas publik, kecuali pengadilan yang bertindak dalam kapasitas yudisialnya; 2) kegiatan inti dari pengontrol atau pemroses terdiri dari operasi pemrosesan yang, berdasarkan sifat, cakupan, dan/atau tujuannya, memerlukan pemantauan rutin dan sistematis terhadap subjek data dalam skala besar; atau 3) Aktivitas inti pengendali data pribadi atau pemroses data pribadi adalah pengumpulan, penggunaan, atau pengungkapan data pribadi yang sensitif.[79]

---

[74]Ibid.

[75]PDPA Thailand, "Section 28-PDPA Thailand", https://pdpathailand.com/pdpa/content_eng/article28_eng.php?srsltid=AfmBOorxz_vn2Y5oYEii3f7nImelNi2c3s2K-1K-x_w_9oKPIyuTJ9EM, 2019. Diakses pada: 25 September 2024

[76]Bank of Thailand, "Personal Data privacy Policy", https://www.bot.or.th/en/privacy-policy.html. Diakses pada: 25 September 2024

[77]Ibid

[78]Bank of Thailand, "Personal Data privacy Policy", https://www.bot.or.th/en/privacy-policy.html. Diakses pada: 25 September 2024

[79]Bakermckenzie, "Global Data Privacy and Cybersecurity Handbook: Thailand", 2024, https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/asia-pacific/thailand/topics/data-protection-officers. Diakses pada: 26 September 2024

4.1.6 Bank Indonesia

Di Indonesia sendiri, UU PDP telah disahkan oleh DPR dan Pemerintah dan telah diundangkan pada tanggal 17 Oktober 2022. UU PDP diperuntukkan bagi Pemerintah/sektor publik, sektor privat, dan organisasi internasional tak terkecuali Bank Indonesia. Hendri Sasmita Yuda dalam pemaparannya mengenai "Tata kelola Pelindungan Data Pribadi: UU PDP dan Arah Pengaturannya" mengatakan bahwa UU ini berlaku di wilayah hukum negara RI dan di luar wilayah hukum negara RI, yang memiliki akibat hukum (di wilayah hukum negara RI dan bagi subjek data pribadi warga negara Indonesia di luar wilayah hukum negara RI). UU PDP tidak berlaku untuk pemrosesan data pribadi oleh orang perseorangan dalam kegiatan pribadi atau rumah tangga.[80]

Substansi regulasi pada UU PDP diantaranya definisi dan ruang lingkup, asas undang-undang, jenis data pribadi, hak subjek data pribadi, pemrosesan data pribadi, prinsip dan dasar pemrosesan data pribadi, *joint controller*, kewajiban pengendali dan prosesor data pribadi, transfer data pribadi, sanksi administratif, kelembagaan, kerjasama internasional, partisipasi masyarakat, penyelesaian sengketa dan hukum acara, larangan dalam penggunaan data pribadi, ketentuan pidana, dan ketentuan peralihan serta penutup.

Di Bank Indonesia sendiri, pengaturan mengenai Pelindungan Data Pribadi (PDP) yang baru terbatas pada PDG No.11 Tahun 2024 tentang Pelindungan Data Pribadi. Pertimbangan disusunnya PDG ini, Pertama, sebagaimana mandat Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia dan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan, Bank Indonesia memiliki tujuan mencapai stabilitas nilai rupiah, memelihara stabilitas sistem pembayaran, dan turut menjaga stabilitas sistem keuangan dalam rangka mendukung pertumbuhan ekonomi yang berkelanjutan.

Dalam mencapai tujuan tersebut, Bank Indonesia memanfaatkan data dan/atau informasi untuk merumuskan dan melaksanakan kebijakan Bank Indonesia. Pemanfaatan data dan/atau informasi dalam perumusan dan pelaksanaan kebijakan Bank Indonesia sejalan dengan kewenangan Bank Indonesia dalam Pasal 14 ayat (1) dan ayat (2) Undang-Undang mengenai Bank Indonesia yang mengamanatkan pemanfaatan data dan/atau informasi di Bank Indonesia dilakukan antara lain dalam penyelenggaraan survei, pertukaran data dan/atau informasi dengan otoritas dan/atau kementerian atau lembaga terkait, serta diseminasi data dan/atau informasi terkait dengan pelaksanaan tugas Bank Indonesia.

Pemanfaatan data dan/atau informasi dalam perumusan dan/atau pelaksanaan kebijakan Bank Indonesia mencakup pula pemanfaatan Data Pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Bank Indonesia sebagai lembaga negara yang independen berperan sebagai Pengendali Data Pribadi yang berwenang dalam menentukan tujuan dan melakukan kendali dalam Pemrosesan Data Pribadi dalam rangka mendukung pencapaian tujuan Bank Indonesia.

Untuk mendukung pencapaian tujuan Bank Indonesia tersebut, pemrosesan data dan/atau informasi, termasuk data pribadi, yang diperlukan dalam perumusan dan pelaksanaan kebijakan Bank Indonesia, diperlukan upaya pelindungan terhadap data pribadi yang dilakukan pemrosesan di Bank Indonesia yang sejalan dengan Undang-Undang Nomor 27 Tahun 2022 tentang pelindungan data pribadi. Oleh karena itu, dengan semakin meningkatnya pemanfaatan Data Pribadi di Bank Indonesia, perlu disusun suatu aturan yang menjadi acuan utama dalam pelaksanaan Pelindungan Data Pribadi di Bank Indonesia. Pelaksanaan Pelindungan Data Pribadi di Bank Indonesia dilakukan sebagai bagian dari kebijakan tata kelola data dan/atau informasi di Bank Indonesia. Untuk itu, guna memastikan pelaksanaan Pelindungan Data Pribadi sesuai dengan Undang-Undang mengenai Bank Indonesia dan Undang-Undang mengenai Pelindungan Data Pribadi, Bank Indonesia menetapkan Peraturan Dewan Gubernur tentang Pelindungan Data Pribadi di Bank Indonesia.

[80]Hendri Sasmita Yuda, "Tata kelola Pelindungan Data Pribadi: UU PDP dan Arah Pengaturannya", Webinar OJK Institute, 30 Mei 2024, https://www.ojk.go.id/ojk-institute/en/capacitybuilding/upcoming/4169/peluang-dan-tantangan-pelindungan-data-pribadi-dalam-transaksi-di-era-digital. Diakses pada: 30 Mei 2024

Menurut pandangan penulis, PDG sebagaimana diketahui, sifat pengaturannya untuk internal, sehingga tidak sepenuhnya mengakomodasi kepentingan dan kebutuhan regulasi untuk pertukaran data antara Bank Indonesia dengan eksternal atau lembaga jasa keuangan yang berada di bawah pengawasan Bank Indonesia. Oleh karena itu, Bank Indonesia sebaiknya mempertimbangkan penerbitan Peraturan Bank Indonesia (PBI) dan Peraturan Anggota Dewan Gubernur (PADG) yang khusus mengatur mekanisme pengawasan dan mekanisme pertukaran data dalam penanganan *fraud*, protokol, serta standar keamanan dalam pertukaran data lintas kementerian, lembaga, dan lembaga jasa keuangan.

Selain itu, Bank Indonesia juga perlu membuat peraturan terkait dengan *Data Protection Officer* (DPO) bagi lembaga jasa keuangan yang berada di bawah kewenangannya. Hal tersebut dilakukan mengingat dari hasil *Focus Group Discussion* (FGD) yang dilakukan Bank Indonesia bersama perwakilan industri yang terdiri dari perbankan (BCA dan Mandiri) dan perusahaan teknologi finansial (OVO) didapati bahwa sebagian besar pelaku industri telah memiliki DPO dpada lembaga mereka, namun masih belum memiliki panduan yang jelas mengenai pelaksanaan teknis dari peran tersebut. Lembaga masih meraba-raba dalam menerapkan tugas dan tanggung jawab DPO. Oleh karena itu, pelaku industri menilai bahwa diperlukan aturan lebih lanjut dan lebih spesifik dari otoritas sebagai paying hukum mereka, seperti Bank Indonesia atau otoritas terkait lainnya, untuk memberikan pedoman yang lebih rinci dan terarah mengenai peran serta tanggung jawab teknis DPO. Hal ini dianggap penting untuk memastikan bahwa setiap lembaga dapat mematuhi standar keamanan data yang konsisten dan sejalan dengan kebijakan pelindungan data.

Secara keseluruhan, penulis menilai bahwa bank-bank sentral di keenam negara ini menunjukkan komitmen yang kuat terhadap pelindungan data pribadi. Mereka semua menekankan pada prinsip-prinsip seperti transparansi, keamanan data, dan penghormatan terhadap hak-hak individu terkait data pribadi mereka. Perbedaan utama terletak pada kerangka hukum spesifik yang mereka ikuti dan beberapa detail implementasi, namun tujuan umumnya tetap sama yaitu melindungi privasi individu, memenuhi fungsi penting mereka sebagai regulator keuangan dan pengawas ekonomi. Bank sentral di keenam negara yang dibahas memiliki peran ganda yang menantang, yaitu mereka harus memenuhi fungsi regulasi dan pengawasan terkait pelindungan data pribadi, dengan tetap mematuhi undang-undang pelindungan data yang ketat. Keseimbangan ini tercermin dalam praktik mereka, dengan tetap menerapkan prinsip kehati-hatian dan memastikan kerahasiaan serta keamanan data untuk kepentingan subjek data.

4.2 Pertukaran Data di Lembaga Jasa Keuangan

Pertukaran data di lembaga jasa keuangan merupakan salah satu elemen penting yang mendukung integrasi antar lembaga keuangan, regulator, dan penyedia layanan terkait. Dalam ekosistem yang saling terhubung, aliran data yang cepat dan aman menjadi fundamental untuk memastikan operasional yang lancar, baik dalam transaksi keuangan, analisis risiko, maupun pemenuhan kepatuhan regulasi. Pertukaran data, khususnya data sharing *fraud* membuat beberapa lembaga melakukan kolaborasi dan berbagi informasi guna mencegah risiko ke depan akan terjadi lagi dari kegiatan fraudster yang mungkin dilakukan pada lembaga jasa keuangan mereka. Di sisi lain data sharing ini dapat meningkatkan efisiensi, transparansi, dan akurasi layanan Lembaga jasa keuangan, sekaligus mengurangi risiko kegiatan *fraudster* di lembaga mereka.

4.2.1 Tukar Menukar Data Pribadi dalam rangka Pencegahan dan Penanganan Fraud di Sektor Keuangan

Penggunaan data dan informasi di lembaga jasa keuangan memainkan peranan penting baik dalam rangka pengembangan usaha maupun dalam rangka pelaksanaan kepatuhan terhadap regulasi yang diterbitkan oleh otoritas, khususnya bagi keamanan data terhadap penipuan atau manipulasi (*fraud*). Demikian pula bagi Bank Indonesia, data dan informasi juga memiliki peranan yang sentral dalam rangka mendukung pelaksanaan tugas dan kewenangan Bank Indonesia serta dalam rangka perumusan dan pengembangan kebijakan Bank Indonesia. Pertukaran/berbagi data melalui *data portability* merupakan salah satu pendekatan terkait dengan *enhancement access* dan berbagi data dalam rangka kebutuhan keterbukaan data termasuk data penipuan atau manipulasi (*data fraud*). Data portability ini menggunakan bentuk khusus/tertentu yang dapat di akses oleh pihak

tertentu yang dapat dibedakan, dikategorikan, dan dianalisis lebih lanjut guna kepentingan pihak tertentu tersebut.[81]

Adapun data dan informasi yang digunakan oleh lembaga jasa keuangan dan Bank Indonesia termasuk pula data dan informasi yang merupakan data pribadi sebagaimana dimaksud dalam UU PDP. Dengan pengaturan tersebut menjadi pengecualian untuk meminta *consent* kepada subjek data, sepanjang data sharing untuk penanganan fraud ini diatur oleh Bank Indonesia, sehingga akan "dianggap" sebagai pengecualian sebagaimana Pasal 15 UU PDP. Terkait hal tersebut berdasarkan UU PDP, lembaga jasa keuangan dan Bank Indonesia memiliki kewajiban dan peran baik sebagai pengendali data pribadi maupun sebagai prosesor data pribadi sebagaimana diatur dalam Bab VI UU PDP dan dapat melakukan data sharing, dengan diaturnya hal tersebut oleh BI.

Pelindungan terhadap hak subjek data pribadi menjadi hal yang utama dalam dalam UU PDP. Hal tersebut dengan pertimbangan bahwa pelindungan data pribadi termasuk dalam pelindungan hak asasi manusia. Oleh karena itu, pengaturan menyangkut data pribadi merupakan manifestasi pengakuan dan pelindungan atas hak dasar manusia. Pelindungan data pribadi dalam UU PDP merupakan amanat dari Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa, "Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".[82] Berkenaan dengan hal tersebut, lembaga jasa keuangan dan Bank Indonesia sebagai pengendali data pribadi maupun sebagai prosesor data pribadi, memiliki berbagai kewajiban dalam UU PDP dalam rangka pemenuhan hak subjek data pribadi berupa transparansi penggunaan data pribadi dan pelindungan terhadap data pribadi.

Di sisi lain, dalam UU PDP telah diatur pula pengecualian terhadap hak-hak subjek data pribadi sebagaimana diatur dalam Pasal 15 UU PDP dan pengecualian kewajiban pengendali data pribadi sebagaimana diatur dalam Pasal 50 UU PDP untuk kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara. Berdasarkan ketentuan dalam Pasal 15 dan Pasal 50 UU PDP tersebut maka UU PDP telah memperhatikan pula kepentingan sektor keuangan terkait dengan pengelolaan data pribadi oleh pengendali data pribadi di sektor keuangan, dalam hal ini adalah Bank Indonesia.

Namun demikian, dalam UU PDP belum mengatur secara rinci dan detail terkait implementasi atau penerapan pengelolaan data pribadi di sektor keuangan dengan tetap mengedepankan pelindungan terhadap hak subjek data pribadi. Dalam UU PDP juga belum mengatur secara detail terkait implementasi atau penerapan terhadap pengecualian bagi sektor keuangan dalam Pasal 15 dan Pasal 50 UU PDP. Oleh karena itu, diharapkan terdapat *bridging* aturan yang menghubungkan norma dalam UU PDP, yaitu aturan pelaksanaan dari UU PDP yaitu Peraturan Pemerintah mengenai pelindungan data pribadi dan aturan dari masing-masing otoritas sektor keuangan sehingga dapat memperjelas pengaturan dalam UU PDP terkait pengelolaan data pribadi di sektor keuangan dengan tetap mengedepankan pelindungan terhadap hak subjek data pribadi, termasuk pengecualian bagi sektor keuangan terhadap hak-hak subjek data pribadi dan kewajiban pengendali data pribadi. Diharapkan dengan adanya aturan pelaksanaan tersebut dapat mempermudah implementasi pengelolaan data pribadi yang sejalan dengan UU PDP di sektor keuangan.

Beberapa hal yang memerlukan pengaturan lebih lanjut baik dalam Peraturan Pemerintah maupun aturan dari masing-masing otoritas sektor keuangan (dalam hal ini Bank Indonesia), yaitu antara lain terkait pertukaran data pribadi dan mekanisme koordinasi antara lembaga pengawas dan regulator yang mengatur industri di sektor keuangan, terutama dalam hal pengawasan dan pengenaan sanksi. Pertukaran data pribadi tersebut meliputi pertukaran data pribadi antar lembaga jasa keuangan maupun pertukaran data pribadi antara lembaga jasa keuangan dengan otoritas sektor keuangan dalam rangka pemenuhan kewajiban yang telah ditetapkan oleh otoritas, antara lain dalam rangka

[81]OECD, "Mapping Data Portability Initiatives, Opportunities And Challenges", OECD Digital Economy Papers, December 21 No.321 p.9, https://www.oecd.org/en/publications/mapping-data-portability-initiatives-opportunities-and-challenges_a6edfab2-en.html#:~:text=Data%20portability%20has%20become%20an,costs%20and%20lock%2Din%20effects. Diakses pada: 7 Oktober 2024

[82]Penjelasan umum Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.

pencegahan dan penanganan *fraud*[83] baik pada lembaga jasa keuangan berupa bank maupun non-bank.

Jenis kegiatan atau aktivitas yang termasuk *fraud* di sektor keuangan antara lain pencucian dan penggelapan uang dengan cara menyalahgunakan aset yang dipercayakan padanya, contohnya dalam *multi level marketing* dengan skema ponzi, pelaku akan menggelapkan aset para investor yang dipercayakan padanya.[84] Kegiatan atau aktivitas lainnya yang termasuk sebagai *fraud* yakni pencurian data melalui pengambilan data penting suatu instansi atau perusahaan untuk mendapatkan keuntungan pribadi.

Pencegahan dan penanganan *fraud* tersebut memerlukan langkah-langkah yang cepat atau seketika dengan didukung dasar hukum yang memadai. Tindakan tukar menukar data pribadi yang terindikasi atau telah terbukti terlibat dalam kegiatan atau aktivitas *fraud* merupakan salah satu tindakan yang diperlukan dalam rangka pencegahan dan penanganan fraud. Sebagaimana telah dijelaskan sebelumnya, dalam UU PDP telah mengatur pengecualian bagi sektor keuangan dalam rangka kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara sebagaimana dimaksud dalam Pasal 15 dan Pasal 50 UU PDP.

Secara implisit berdasarkan ketentuan pengecualian tersebut, lembaga jasa keuangan dan otoritas sektor keuangan memiliki kewenangan untuk melakukan berbagi data dalam rangka pencegahan dan penanganan *fraud*. Namun demikian, penafsiran secara implisit tersebut perlu ditegaskan yang lebih teknis yaitu dalam bentuk peraturan pelaksanaan. Pengaturan secara eksplisit dalam hal ini, Peraturan Pemerintah dan/atau peraturan yang dikeluarkan oleh otoritas di sector keuangan seperti Bank Indonesia dapat memberikan dasar hukum yang kuat terutama bagi lembaga jasa keuangan dalam melakukan tukar menukar data pribadi untuk pencegahan dan penanganan *fraud*.

Dasar hukum yang jelas dalam Peraturan pelaksanaannya sangat diperlukan mengingat tindakan pertukaran data pribadi mengandung risiko hukum yang tinggi terutama bagi lembaga jasa keuangan. Dalam hal tidak terdapat aturan yang eksplisit maka lembaga jasa keuangan berpotensi menerima tuntutan atau gugatan hukum bertubi-tubi dari pemilik data pribadi dapat mengajukan karena tindakan tukar menukar data pribadi tersebut dianggap tidak sejalan dengan ketentuan perundang-undangan mengenai pelindungan data pribadi. Dengan adanya aturan hukum yang eksplisit, masyarakat mengetahui bahwa tindakan tukar menukar data pribadi dalam rangka pencegahan dan penanganan *fraud* masih sejalan dengan ketentuan perundang-undangan mengenai pelindungan data pribadi. Selain itu, lembaga jasa keuangan tidak memiliki keraguan lagi dalam melakukan tukar menukar data pribadi untuk pencegahan dan penanganan *fraud* karena telah terdapat dasar hukum yang kuat baik dari aturan masing-masing otoritas sektor keuangan maupun dari peraturan perundang-undangan terkait pelindungan data pribadi.

Di sisi lain diperlukan pula pengaturan mengenai mekanisme koordinasi antara lembaga pengawas PDP dengan regulator dan pengawas di sektor keuangan, mengingat industri di sektor keuangan sudah sangat maju dan advance sehingga akan sangat membantu lembaga pengawas PDP dalam melakukan pengawasan terhadap industri di sektor keuangan. Hal ini tentunya diperlukan koordinasi yang baik antara Kominfo dan Regulator dari K/L di sektor keuangan seperti Kementerian Keuangan, Bank Indonesia, OJK, dan LPS untuk dapat duduk bersama memformulasikan aturan pelaksanaannya dalam Peraturan Pemerintah sehingga masing-masing K/L di sektor keuangan dapat menyesuaikan/menyempurnakan peraturan-peraturan pelaksanaannya yang sudah berlaku saat ini dengan pengaturan terkait mengenai PDP sehingga implementasi di lapangan dapat berjalan dengan efisien dan efektif. Di sisi lain dengan adanya koordinasi tentunya tidak akan ada peraturan yang tumpang tindih, bahkan sekaligus melakukan

[83]Berdasarkan Pasal 1 angka 2 Peraturan Otoritas Jasa Keuangan Nomor 39/POJK.03/2019 tentang Penerapan Strategi Anti Fraud bagi Bank Umum, *fraud* adalah tindakan penyimpangan atau pembiaran yang sengaja dilakukan untuk mengelabui, menipu, atau memanipulasi Bank, nasabah, atau pihak lain, yang terjadi di lingkungan Bank dan/atau menggunakan sarana Bank sehingga mengakibatkan Bank, nasabah, atau pihak lain menderita kerugian dan/atau pelaku *fraud* memperoleh keuntungan keuangan baik secara langsung maupun tidak langsung. Oleh karena itu, diperlukan pertukaran data guna pencegahan *fraud* lebih lanjut.

[84]Indonesia Securities Investor Protection Fund (Indonesia SIPF), "Skema Ponzi, Ancaman Bagi Perkembangan Industri Jasa Keuangan", Maret 2024, https://www.indonesiasipf.co.id/uploads/media/bulletin/bulletin-sipf_q1_2024.pdf. Diakses pada: 23 Juli 2024

harmonisasi peraturan yang ada ke depannya. Kominfo dapat berkoordinasi dengan lembaga KSSK atau dengan masing-masing anggota KSSK untuk membangun kerjasama dalam menyusun Peraturan Pemerintah ini.

Dalam UU PDP pertukaran data pribadi dikenal sebagai transfer data pribadi. Berkenaan dengan transfer data pribadi di sektor keuangan telah dilaksanakan diskusi dengan pejabat dari Kementerian Komunikasi dan Digital (Komdigi) yaitu Bapak Hendri Sasmita Yuda pada tanggal 8 November 2024. Beberapa masukan yang diperoleh dari diskusi dimaksud yaitu sebagai berikut:

Transfer data pribadi prinsipnya tidak dilarang dan bahkan harus dilakukan untuk dapat memberikan nilai tambah terhadap data pribadi.

Dalam pelaksanaan transfer data pribadi terdapat beberapa skema yaitu sebagai berikut **(Lampiran 2)**.

Penjelasan atas masing-masing skema transfer data pribadi dan beberapa hal yang perlu diperhatikan dalam melakukan transfer data pribadi **(Lampiran 3)**.

Pemetaan para pihak dalam pelaksanaan transfer data pribadi berdasarkan UU PDP yaitu sebagai berikut **(Lampiran 4)**.

Sebelum melakukan transfer data pribadi perlu dilakukan asesmen terkait dengan transfer data pribadi tersebut, termasuk menentukan dasar pemrosesan, identifikasi tujuan transfer/sharing data, rincian jenis data pribadi, jangka waktu, serta mekanisme penghapusan/pemusnahan data pribadi. Selain itu, perlu ditentukan instrumen untuk memastikan pembagian peran dan tanggung jawab yang jelas antar para serta bagaimana mekanisme otorisasi dan pelaksanaan dari transfer tersebut dalam regulasi/MoU/PKS/perjanjian/juknis. Pelaksanaan transfer dituangkan dalam dokumen tertentu sebagai bentuk akuntabilitas. Selain itu perlu dilakukan penilaian (*assessment/ due diligence*) secara bersama terhadap rencana transfer termasuk tingkat maturitas masing-masing sebelum transfer dilaksanakan. Penilaian terhadap rencana transfer dituangkan dalam bentuk tertulis secara elektronik dan/atau nonelektronik.

Perlunya suatu lembaga yang berfungsi sebagai "wasit" dalam menentukan dapat atau tidaknya suatu transfer data pribadi di [illegible] ini bukan merupakan Lembaga PDP sebagaimana dimaksud dalam UU PDP. Lembaga ini memiliki personil yang berpengalaman dan merupakan praktisi di masing-masing sektor sehingga dapat memahami karakteristik pertukaran data di setiap sektor.

Hal yang perlu diperhatikan

4.2.2 Penerapan Prinsip Transparansi Pelindungan Data Pribadi di Sektor Keuangan

Pentingnya menjaga kepercayaan masyarakat dalam sektor keuangan merupakan salah satu hal yang mendasar atau fundamental. Lembaga jasa keuangan yang tidak lagi memiliki kepercayaan dari nasabah atau konsumen dapat mengganggu kelangsungan usaha dari lembaga jasa keuangan tersebut. Oleh karena itu, lembaga jasa keuangan selalu berupaya untuk menjaga kepercayaan nasabah atau konsumennya, antara lain melalui pengelolaan risiko reputasi. Risiko reputasi bagi lembaga jasa keuangan dapat dijaga salah satunya melalui pengelolaan informasi kepada nasabah/konsumen dan masyarakat. Pemberitahuan atau penyampaian informasi kepada nasabah/konsumen dan masyarakat harus dikelola sedemikian rupa sehingga meminimalisir timbulnya persepsi negatif terhadap lembaga jasa keuangan dimaksud.

Lembaga jasa keuangan yang mengelola dan memproses data pribadi memberikan peningkatan keamanan dalam menjaga data pribadi seperti menerapkan standar enkripsi yang ditingkatkan dan memberitahukan kepada pemilik data pribadi terhadap pembaruan. Lembaga jasa keuangan berkewajiban untuk memberitahu pemilik data pribadi mengenai potensi ancaman keamanan, dan bersikap proaktif dalam mengatasi potensi ancaman tersebut dengan langkah berupa aspek teknologi dan kebijakan. [85]

Di sisi lain, prinsip transparansi dalam UU PDP menjadi salah satu fokus dalam pengelolaan pelindungan data pribadi. Salah satu penerapan prinsip transparansi yaitu subjek data pribadi memiliki hak untuk mengetahui tujuan dan dasar pemrosesan data

[85] Zlatan Moric, Vedran Dakic, Daniela Djekic, dan Damir Regvart. 2024. *Protection of Personal Data in the Context of E-Commerce*. J. Cybersecur. Priv., 4, 731–761.

pribadi. Dalam setiap pertukaran data pribadi dalam rangka pencegahan dan penanganan *fraud*, pengendali data pribadi wajib terlebih dahulu memberitahukan pertukaran data dimaksud kepada pemilik data pribadi yang diduga merupakan *fraudster*. Kewajiban pemberitahuan tersebut kontraproduktif dengan upaya lembaga jasa keuangan dan otoritas sektor keuangan untuk mencegah dan menangani *fraud*. Dengan adanya pemberitahuan bahwa akan dilakukan perpindahan data pribadi karena terdapat dugaan *fraud* maka *fraudster* dapat segera melakukan upaya berupa pemindahan/penarikan dana atau penutupan rekening bank/akun pada lembaga jasa keuangan. Hal tersebut dapat menghambat dan bahkan dapat menghentikan upaya pencegahan dan penanganan *fraud* karena pelaku diberikan kesempatan untuk menghilangkan jejak kejahatan yang dilakukan.

Terkait hal tersebut, dalam Peraturan Pemerintah mengenai pelindungan data pribadi perlu ditegaskan bahwa implementasi atau penerapan prinsip transparansi penggunaan data pribadi berupa pemberitahuan kepada *fraudster* dapat dikecualikan untuk tukar menukar data pribadi dalam rangka pencegahan dan penanganan *fraud*.

4.2.3 Koordinasi Pengawasan dan Pemberian Sanksi Pelanggaran Pelindungan Data Pribadi di Sektor Keuangan

Dalam UU PDP diatur mengenai keberadaan Lembaga Pelindungan Data Pribadi (Lembaga PDP). Dalam Pasal 58 UU PDP diatur bahwa penyelenggaraan Pelindungan Data Pribadi sesuai dengan ketentuan UU PDP dilaksanakan oleh lembaga yang akan ditetapkan oleh Presiden. Lebih lanjut, dalam Pasal 58 juga diatur bahwa Lembaga PDP bertanggung jawab kepada Presiden dan terkait dengan kelembagaan, peran, dan tugas Lembaga PDP akan diatur dengan Peraturan Presiden. Saat ini Peraturan Presiden yang menjadi dasar pembentukan Lembaga PDP belum terbit, namun dalam konteks ini, struktur dan kedudukan Lembaga Pengawas PDP ini mengerucut menjadi 3 (tiga) pilihan. Pertama, lembaga pengawas PDP berupa institusi independen yang bertanggung jawab dan melaporkan pekerjaannya langsung kepada presiden. Kedua, status lembaga tersebut dilekatkan pada lembaga yang sudah ada. Maka bisa saja ada unit tertentu yang sudah ada diberi tugas tambahan untuk melakukan pengawasan berkenaan dengan pelindungan data pribadi. Ketiga, lembaga pengawas PDP berada di bawah naungan presiden, tapi bekerja dan berkoordinasi dengan kementerian atau lembaga terkait, termasuk dengan Bank Indonesia.[86]

Dalam Pasal 59 UU PDP diatur tugas Lembaga PDP yaitu melaksanakan perumusan dan penetapan kebijakan dan strategi Pelindungan Data Pribadi yang menjadi panduan bagi Subjek Data Pribadi, Pengendali Data Pribadi, dan Prosesor Data Pribadi, melakukan pengawasan terhadap penyelenggaraan Pelindungan Data Pribadi, melaksanakan penegakan hukum administratif terhadap pelanggaran UU PDP, dan menberikan fasilitasi penyelesaian sengketa di luar pengadilan.

Selain itu, dalam Pasal 60 UU PDP diatur mengenai kewenangan Lembaga PDP yaitu merumuskan dan menetapkan kebijakan di bidang Pelindungan Data Pribadi, melakukan pengawasan terhadap kepatuhan Pengendali Data Pribadi, menjatuhkan sanksi administratif atas pelanggaran Pelindungan Data Pribadi yang dilakukan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi, membantu aparat penegak hukum dalam penanganan dugaan tindak pidana Data Pribadi sebagaimana dimaksud dalam UU PDP. Selain itu kewenangan lainnya antara lain bekerja sama dengan Lembaga PDP negara lain dalam rangka penyelesaian dugaan pelanggaran Pelindungan Data Pribadi lintas negara, melakukan penilaian terhadap pemenuhan persyaratan transfer Data Pribadi ke luar wilayah hukum Negara Republik Indonesia, memberikan perintah dalam rangka tindak lanjut hasil pengawasan kepada Pengendali Data Pribadi dan/atau Prosesor Data Pribadi, melakukan publikasi hasil pelaksanaan pengawasan Pelindungan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.

Terkait dengan pengawasan dan pemeriksaan, kewenangan Lembaga PDP meliputi antara lain menerima aduan dan/atau laporan tentang dugaan terjadinya pelanggaran Pelindungan Data Pribadi, melakukan pemeriksaan dan penelusuran atas pengaduan, laporan, dan/atau hasil pengawasan terhadap dugaan terjadinya pelanggaran Pelindungan

[86]Portal Informasi Indonesia, "Era Baru Pelindungan Data Pribadi", https://indonesia.go.id/kategori/editorial/8725/ era-baru-pelindungan-data-pribadi?lang=1. Di akses 27 Juli 2024

Data Pribadi, memanggil dan menghadirkan Setiap Orang dan/ atau Badan Publik yang terkait dengan dugaan pelanggaran Pelindungan Data Pribadi, meminta keterangan, data, Informasi, dan dokumen dari Setiap Orang dan/ atau Badan Publik terkait dugaan pelanggaran Pelindungan Data Pribadi, memanggil dan menghadirkan ahli yang diperlukan dalam pemeriksaan dan penelusuran terkait dugaan pelanggaran Pelindungan Data Pribadi, melakukan pemeriksaan dan penelusuran terhadap sistem elektronik, sarana, ruang, dan/atau tempat yang digunakan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi, termasuk memperoleh akses terhadap data dan/atau menunjuk pihak ketiga, dan meminta bantuan hukum kepada kejaksaan dalam penyelesaian sengketa Pelindungan Data Pribadi.

Sebagaimana telah dijelaskan sebelumnya, tugas dan kewenangan Lembaga PDP akan memiliki dampak yang luas bagi semua pihak yang memiliki peran sebagai pengendali data pribadi dan prosesor data pribadi. Terkait hal tersebut, otoritas sektor keuangan dan lembaga jasa keuangan selaku pengendali data pribadi dan prosesor data pribadi juga memiliki kepentingan terhadap tugas dan kewenangan Lembaga PDP. Koordinasi yang baik antara otoritas sektor keuangan dengan Lembaga PDP sangat diperlukan agar tidak menghambat di industri keuangan yang memiliki kontribusi yang signifikan terhadap pengembangan perekonomian Indonesia.

Berdasarkan hal tersebut diperlukan bentuk atau mekanisme koordinasi yang tepat antara otoritas sektor keuangan dengan Lembaga PDP terkait dengan pengaturan dan pengawasan pelaksanaan pelindungan data pribadi di sektor keuangan. Hal tersebut antara lain untuk mencegah adanya tumpang tindih, dalam pengaturan dan pengawasan pelaksanaan pelindungan data pribadi oleh industri sektor keuangan. Dalam hal otoritas sektor keuangan akan melakukan pengaturan mengenai implementasi pelindungan data pribadi maka perlu dikoordinasikan terlebih dahulu dengan Lembaga PDP sehingga ketentuan atau peraturan yang terbit dapat harmonis. Selain itu, dalam melakukan pengawasan dan pemeriksaan terhadap lembaga jasa keuangan maka Lembaga PDP perlu melakukan koordinasi atau pemeriksaaan bersama dengan otoritas sektor keuangan sehingga hasil temuan tidak bias dan tepat sasaran.

Seperti halnya terjadi di Singapura, terdapat kesamaan tugas dan kewenangan dalam pengaturan dan pengawasan pelaksanaan pelindungan data pribadi untuk industri sektor keuangan. Dalam hal ini Monetary Authority of Singapore (MAS) yang merupakan otoritas sektor keuangan, Personal Data Protection Commission Singapore (PDPC) yang merupakan Lembaga PDP, dan Cyber Security Agency of Singapore (CSA) yang merupakan badan pengamanan siber, masing-masing memiliki kewenangan terkait pengaturan dan pengawasan pelaksanaan pelindungan data pribadi. Namun demikian, pengaturan dan pengawasan oleh PDPC dan CSA dilakukan untuk hal tertentu. PDPC melakukan pengaturan dan pengawasan untuk industri sektor keuangan yang memiliki dampak atau berpotensi berisiko bagi lebih dari 500 (lima ratus) individu. Sementara itu, CSA melakukan pengaturan dan pengawasan untuk industri yang memiliki potensi risiko siber yang signifikan. Adapun MAS melakukan pengaturan dan pengawasan untuk semua aspek terkait dengan implementasi keamanan siber dan pelindungan data pribadi. Hal tersebut sebagaimana terlihat pada gambar berikut **(Lampiran 5)**.[87]

Selanjutnya, terdapat usulan agar pengaturan dan pengawasan terkait keamanan siber untuk industri sektor keuangan dapat dilakukan oleh MAS berkoordinasi dengan CSA, sehingga tidak terjadi tumpang tindih dalam kewenangan pengaturan dan pengawasan terhadap keamanan siber. Namun demikian, untuk pengaturan dan pengawasan terkait pelaksanaan pelindungan data pribadi dapat dilakukan bersama antara MAS dengan PDPC mengingat terdapat mandat khusus dalam peraturan perundang-undangan. Dengan adanya pemangkasan alur kewenangan pengaturan dan pengawasan antara MAS dengan CSA maka dapat meningkatkan efektivitas rezim pengaturan dan pengawasan terkait pelindungan data pribadi bagi sektor keuangan. Hal tersebut terlihat pada gambar berikut **(Lampiran 6)**.[88]

Mengacu pada mekanisme koordinasi yang ada di Singapura, perlu terdapat pengaturan kembali terkait kriteria lembaga keuangan yang dapat diatur dan diawasi oleh Lembaga PDP. Hal tersebut untuk mencegah terjadinya tumpang tindih tugas dan

[87] A Report by OC Queen Street LLC, Regulations at a Glance for Financial Institutions: Reconciling the Draft Cybersecurity Bill, the Monetary Authority of Singapore Regulations and the Public Consultation for Approaches to Managing Personal Data in the Digital Economy.
[88] Ibid

kewenangan dengan otoritas sektor keuangan seperti Bank Indonesia. Kriteria tersebut antara lain dapat terkait dengan besarnya data pribadi yang diproses oleh lembaga jasa keuangan atau besarnya dampak kepada subjek data pribadi dalam hal terjadi pelanggaran data pribadi.

Selain itu, dalam rangka pengenaan sanksi terhadap industri sektor keuangan juga diperlukan koordinasi yang baik sehingga pengenaan sanksi terkait dengan pelanggaran pelindungan data pribadi tidak berdampak negatif terhadap industri sektor keuangan. Sebagaimana diketahui, sektor keuangan sangat sensitif terhadap isu kepercayaan. Oleh karena itu pengenaan sanksi juga perlu memperhatikan dampaknya terhadap keseluruhan industri keuangan. Jangan sampai, pengenaan sanksi menimbulkan risiko sistemik yang pada akhirnya dapat berdampak negatif terhadap perekonomian. Ketika Lembaga PDP akan mengenakan sanksi kepada lembaga jasa keuangan maka perlu dikoordinasikan terlebih dahulu dengan otoritas sektor keuangan untuk mendapatkan gambaran jenis dan besaran sanksi yang tepat bagi lembaga jasa keuangan tersebut.

4.3 Peraturan Bank Indonesia yang berlaku saat ini terkait Pelindungan Data Pribadi

Bank Indonesia (BI) bertanggung jawab dan berkepentingan untuk menjaga keamanan data, khususnya pelindungan data pribadi dengan mengatur baik secara eksternal (sektor keuangan yang berada di bawah kewenangannya), dan secara internal antara lain terkait layanan Sistem Pembayaran (a.l. RTGS, BI-SSSS, BI-Fast, dan SKN), data pribadi lain yang dikelolanya seperti data pegawai, data kesehatan pegawai, dan data layanan publik lainnya yang dikelola Bank Indonesia. Saat ini, Bank Indonesia belum memiliki peraturan yang secara khusus mengatur pelindungan data pribadi kepada pihak eksternal yang berhubungan dengan BI, akan tetapi di dalam beberapa Peraturan baik Peraturan Bank Indonesia (PBI) dan Peraturan Anggota Dewan Gubernur (PADG) yang telah ada, terdapat pasal-pasal yang mengatur mengenai keamanan data dan sistem informasi, baik mengatur keluar, yang ditujukan kepada lembaga jasa keuangan maupun mengatur ke dalam, kepada internal Bank Indonesia. Peraturan-peraturan tersebut saat ini dikaitkan dengan perlindungan konsumen. Beberapa peraturan tersebut di rangkum pada gambar berikut **(Lampiran 7)**.

Dari skema di atas, Bank Indonesia telah memiliki beberapa peraturan yang di dalamnya mengatur mengenai keamanan data dan informasi seperti Peraturan Bank Indonesia Nomor 22/23/PBI/2020 Tentang Sistem Pembayaran, Peraturan Bank Indonesia Nomor 21/8/PBI/2019 tentang Perubahan Ketiga Atas Peraturan Bank Indonesia Nomor 17/9/PBI/2015 tentang Penyelenggaraan Transfer Dana Dan Kliring Berjadwal Oleh Bank Indonesia, Peraturan Bank Indonesia Nomor 23/7/PBI/2021 Tentang Penyelenggara Infrastruktur Sistem Pembayaran, Peraturan Bank Indonesia Nomor 23/6/PBI/2021 Tentang Penyedia Jasa Pembayaran. Peraturan Bank Indonesia Nomor 2 Tahun 2024 Tentang Keamanan Sistem Informasi Dan Ketahanan Siber Bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang Dan Pasar Valuta Asing, serta Pihak Lain Yang Diatur Dan Diawasi Bank Indonesia. Peraturan Bank Indonesia Nomor 3 Tahun 2023 Tentang Pelindungan Konsumen Bank Indonesia, Peraturan Anggota Dewan Gubernur Nomor 23/24/PADG/2021 Tentang Kepesertaan Dalam Penyelenggaraan Transfer Dana, Kliring Berjadwal, Transaksi, Penatausahaan Surat Berharga, Dan Setelmen Dana Seketika, Peraturan Anggota Dewan Gubernur Nomor 21/12/PADG/2019 Tentang Penyelenggaraan Transfer Dana Dan Kliring Berjadwal Oleh Bank Indonesia, Peraturan Anggota Dewan Gubernur Nomor 23/23/PADG/2021 Tentang Perubahan Ketiga Atas Peraturan Anggota Dewan Gubernur Nomor 20/4/PADG/2018 Tentang Penyelenggaraan Penatausahaan Surat Berharga Melalui Bank Indonesia-Scripless Securities Settlement System. Selanjutnya telah terbit pada tanggal 17 Oktober 2024 Peraturan Dewan Gubernur No 11Tahun 2024 tentang Pelindungan Data Pribadi (PDG PDP) yang mengatur mengenai pemrosesan data pribadi dalam lingkup internal Bank Indonesia.

Berdasarkan beberapa peraturan di atas, Bank Indonesia sudah *concern* terhadap pentingnya menjaga keamanan data termasuk data pribadi yang terdiri dari beberapa aspek, yaitu diwajibkan penerapan SOP mengenai pengelolaan risiko, memiliki audit internal, kepatuhan dan manajemen risiko, memiliki DRP (*disaster recovery plan*), pengelolaan *fraud*, *penetration test*, audit TI independen, audit keuangan, melakukan evaluasi secara berkala,

dan sertifikasi/ISO serta melakukan simulasi keamanan siber dan non-siber. Aspek-aspek tersebut juga diberlakukan untuk aspek keamanan data *cross border.*

Beberapa sertifikasi ISO yang sudah didapatkan oleh Bank Indonesia diantaranya **ISO 9001:2015** *Quality Management System* terhadap fungsi layanan nasabah dan perizinan, layanan nasabah perbankan dan pemerintah, layanan operasional sistem tresuri dan perbankan, dan layanan tresuri dan non tresuri, **ISO 27001:2013** yang merupakan standar internasional yang menetapkan persyaratan untuk Sistem Manajemen Keamanan Informasi (*Information Security Management System*/ISMS), **ISO 22301:2019** mengenai manajemen risiko dan manajemen keberlangsungan tugas BI serta **ISO 15489: 2016** mengenai pencapaian standar manajemen arsip di BI.[89]

Peneliti memandang bahwa sertifikasi ini merupakan salah satu upaya Bank Indonesia dalam rangka menjalankan mandat UU Perlindungan Data Pribadi guna meningkatkan kredibilitas sekaligus menjaga standar kualitas layanan kebanksentralan Bank Indonesia. Saat ini Bank Indonesia sedang mempersiapkan peraturan terkait dengan *collecting data* yang di susun oleh Departemen Statistik. Penyusunan peraturan ini diharapkan dapat menjadi bagian dari peraturan yang mengatur mengenai PDP secara keseluruhan, dan tidak mengatur sendiri-sendiri. Oleh karena itu, perlu dilakukan Komunikasi dan koordinasi dengan satker-satker terkait antara lain Departemen Kebijakan Sistem Pembayaran, Departemen Inovasi dan Digitalisasi Data, Departemen Penyelenggaraan Sistem Pembayaran, Departemen Sumber Daya Manusia, Departemen Pengelolaan dan Kepatuhan Laporan, Departemen Pengelolaan Logistik dan Fasilitas serta Departemen Layanan Digital dan Keamanan Siber.

Terkait dengan rencana pengaturan tersebut, berdasarkan hasil *mapping* ketentuan yang diterbitkan oleh BI, terdapat *gap* terkait pengaturan pelindungan data pribadi yaitu sebagai berikut:

1. Ketentuan/peraturan di bidang SP yang mengatur mengenai pelindungan data pribadi (PBI SP, PBI PJP, dan PBI PIP) terbit sebelum berlakunya UU PDP sehingga tidak secara spesifik mencantumkan kepatuhan terhadap cakupan ketentuan perundang-undangan mengenai pelindungan data pribadi, seperti mematuhi asas dan prinsip pelindungan data pribadi.
2. Belum terdapat pengaturan terhadap lembaga jasa keuangan yang mengatur implementasi pelindungan data pribadi secara komprehensif, antara lain seperti:
    a. pengaturan mengenai kewajiban yang diatur dalam UU PDP a.l. menyusun ROPA, DPIA, transparansi penggunaan data pribadi (*privacy notice*), mekanisme pengajuan ganti rugi, penunjukkan DPO.
    b. Pengaturan yang dibuat dari kalangan industri atau dikenal dengan *Self Regulation Organization* (SRO) yang tertuang dalam *bye laws*/SK asosiasi. Aturan spesifik pelindungan data pribadi untuk LJK yang diawasi BI, memedomani ketentuan yang diatur oleh Bank Indonesia, yang masih tersebar di berbagai peraturan (tidak terintegrasi dalam 1 peraturan mengenai implementasi pelindungan data pribadi untuk lembaga jasa keuangan yang diawasi oleh BI).
3. Belum terdapat pengaturan mengenai penyelesaian sengketa terkait PDP apabila terjadi perselisihan atau kebocoran data yang diadukan oleh subjek data. LAPS Sektor Keuangan dapat menjadi alternatif lembaga untuk penyelesaian sengketa terkait pelindungan data pribadi sambil menunggu pengaturan dalam RPP PDP.
4. Belum terdapat pengaturan perihal tukar menukar data terkait *fraud* (antara lain APUPPT), antar lembaga jasa keuangan.

Dari gap tersebut di atas dapat terlihat bahwa Bank Indonesia memerlukan regulasi secara komprehensif yang dapat mengakomodasi berbagai kepentingan, baik kepentingan *stakeholders*, maupun kepentingan BI sendiri. BI saat ini baru memiliki PDG PDP yang hanya mengatur mengenai internal BI, dan belum mengatur eksternal BI. Pengaturan eksternal tentunya tidak kalah penting mengingat BI selaku otoritas dan regulator memiliki tanggung jawab terhadap *stakeholders*/industri yang berada di bawah kewenangannya yang juga membutuhkan pengaturan dari otoritas guna menjaga kelancaran usaha dan

[89] Siaran Pers Bank Indonesia, "BI Kembali Pertahankan Kualitas Layanan Kebanksentralan dan Manajemen Dokumen", 2023, https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_2531223.aspx. Di akses pada: 20 November 2024

pengembangan industri di sektor keuangan yang memiliki perubahan teknologi yang sangat cepat. Kehadiran peraturan eksternal BI terkait PDP, tentunya akan memberikan mandat kepada industri untuk mematuhi pengaturan mengenai PDP yang pada akhirnya diharapkan dapat melindungi dan menjaga subjek data pribadi dan lembaga jasa keuangan itu sendiri.

5. Rekomendasi

Berdasarkan hasil penelitian di atas Bank Indonesia telah memiliki peraturan yang terkait dengan keamanan data pribadi seperti yang dimandatkankan UU PDP, namun belum ada peraturan secara spesifik yang lebih komprehensif dan terfokus mengenai pelindungan data pribadi, seperti mematuhi asas dan prinsip pelindungan data pribadi termasuk penunjukkan DPO dan koordinasi dengan lembaga pengawas PDP serta alternatif penyelesaian sengketa. Oleh karena itu, untuk menegaskan wewenang BI selaku otoritas/regulator terhadap lembaga jasa keuangan terkait PDP, penulis memberikan usulan rekomendasi terhadap beberapa hal terkait dengan rekomendasi kebijakan dan rekomendasi teknis yang perlu dilakukan oleh Bank Indonesia, sebagai berikut.

5.1. Rekomendasi Kebijakan

Dalam rekomendasi kebijakan ini, penulis mengusulkan pokok-pokok rekomendasi kebijakan yang akan dimuat dalam kerangka hukum atau peraturan-peraturan yang lebih spesifik untuk mengakomodasi kompleksitas pelindungan data pribadi. Peraturan ini akan menjadi payung hukum bagi industri untuk memastikan kepatuhan lembaga jasa keuangan terkait dengan PDP. Berikut pokok-pokok rekomendasi kebijakan:

1. Perumusan prinsip-prinsip umum pelindungan data pribadi

Bank Indonesia selaku otoritas/regulator memiliki kepentingan dan kewenangan membuat peraturan untuk memberikan pedoman bagi lembaga jasa keuangan dalam menjalankan mandat UU sehingga Bank Indonesia perlu merancang prinsip-prinsip umum mengenai pelindungan data pribadi yang dituangkan dalam Peraturan.

Prinsip-prinsip tersebut terbagi menjadi tiga bagian. Pertama, pengumpulan data pribadi yang memiliki 3 prinsip, yaitu pemberitahuan, persetujuan, dan pembatasan tujuan. Pada prinsip **pemberitahuan**, lembaga harus transparan dengan memberi tahu individu tentang tujuan pengumpulan, penggunaan, atau pengungkapan data pribadi mereka. Prinsip **persetujuan**, data pribadi hanya boleh dikumpulkan, digunakan, atau diungkapkan sesuai dengan persetujuan individu. Individu juga berhak menarik persetujuan mereka kapan saja, dan lembaga harus menghentikan penggunaan data tersebut setelah penarikan. Prinsip **pembatasan tujuan**, penggunaan data pribadi harus terbatas sesuai dengan persetujuan individu, tanpa memaksa persetujuan lebih dari yang diperlukan untuk menyediakan produk atau layanan.

Kedua, mengenai pelindungan data pribadi yang terbagi menjadi 4 prinsip, yaitu akurasi, pelindungan, pembatasan retensi, dan pembatasan transfer. Prinsip **Akurasi**, lembaga harus memastikan bahwa data pribadi yang dikumpulkan akurat dan lengkap, terutama jika data tersebut akan digunakan untuk membuat keputusan penting atau dibagikan dengan pihak lain. Prinsip **Perlindungan**, lembaga wajib menerapkan langkah-langkah keamanan untuk melindungi data pribadi dari akses, penggunaan, atau pengungkapan yang tidak sah. Prinsip **Pembatasan Retensi**, data pribadi harus dihapus atau dimusnahkan ketika tidak lagi dibutuhkan. Prinsip **Pembatasan Transfer,** data pribadi hanya boleh ditransfer apabila sesuai dengan persyaratan yang berlaku serta memastikan sesuai dengan standar perlindungan yang berlaku. Hal ini termasuk *cross border transfer.*

Ketiga, otonomi individu atas data pribadi terbagi menjadi 3 prinsip, yaitu akses dan koreksi, pemberitahuan pelanggaran data, dan portabilitas data. Prinsip **Akses dan Koreksi**, lembaga harus menyediakan akses kepada individu untuk melihat data pribadi mereka dan mengoreksi kesalahan data atas permintaan mereka. Prinsip **Pemberitahuan Pelanggaran Data**, jika terjadi pelanggaran data yang signifikan atau berdampak besar, lembaga harus segera melaporkan kejadian tersebut kepada lembaga pengawas (Bank Indonesia dan Lembaga Pengawas PDP) dan individu yang terkena dampak. Prinsip **Portabilitas Data**, lembaga harus memfasilitasi transfer data pribadi ke lembaga lain dalam format khusus yang terbaca oleh sistem jika diminta oleh individua atau dimungkinkan pula dapat

dilakukan jika ada kebutuhan lembaga dalam menjaga pelindungan data pribadi di ekosistem keuangan digital.

2. Keseimbangan Antara Hak Subjek Data Pribadi dan Kepentingan Industri.

Bank Indonesia perlu mengatur ketentuan dimana hak subjek data pribadi lebih diutamakan daripada kepentingan industri. Hal ini mencerminkan pentingnya melindungi privasi individu sebagai hak asasi manusia dalam era digital, di mana data pribadi rentan disalahgunakan oleh pengendali data dan prosesor. Namun demikian, penting pula untuk menciptakan keseimbangan antara hak-hak subjek data pribadi dan kepentingan industri dalam mengelola data tersebut. Oleh karena itu, diperlukan regulasi yang mempertimbangkan pelindungan subjek data tanpa menghambat kemampuan industri untuk beroperasi. Regulasi yang diharapkan diatur dalam peraturan di Bank Indonesia ini agar kepentingan kedua belah pihak terakomodasi dengan baik.

3. Koordinasi Pengawasan antara Bank Indonesia dan Lembaga Pengawas PDP terhadap Lembaga Jasa Keuangan

Koordinasi antara Bank Indonesia (BI) dan lembaga pengawas PDP menjadi kunci penting dalam menjaga pelindungan data pribadi di ekosistem keuangan digital. Koordinasi ini bertujuan agar pengawasan terhadap lembaga Jasa keuangan dapat berjalan lebih efisien dan tidak menghambat ekosistem, pengembangan, dan inovasi teknologi. Sehingga perlu di atur mekanisme koordinasi pengawasan antar BI dan lembaga pengawas PDP sehingga menghindari aturan yang tumpeng tindih mengenai pengawasan dan pengenaan sanksi terhadap lembaga jasa keuangan

4. Koordinasi antara Bank Indonesia dan DPO

BI, sebagai otoritas moneter, sistem pembayaran, dan stabilitas sistem keuangan yang mengawasi sektor keuangan, perlu bekerja sama dengan DPO di lembaga jasa keuangan untuk memastikan bahwa pengelolaan data pribadi sesuai dengan standar dan regulasi yang berlaku. BI dapat mengatur atau memberikan panduan yang harus diikuti oleh DPO untuk memastikan bahwa pelindungan data pribadi menjadi prioritas dalam setiap operasi keuangan. Selain itu, BI dan DPO bekerja sama dalam pengembangan kebijakan privasi yang lebih adaptif terhadap perubahan teknologi.

5. Koordinasi antar Satuan kerja di Bank Indonesia

BI perlu memperkuat koordinasi antar Satuan Kerja terkait untuk menyusun suatu peraturan yang terintegrasi dalam rangka pengumpulan, pengelolaan, dan pemrosesan data pribadi yang dilakukan oleh beberapa Satker, antara lain Departemen Statistik, Departemen Sumber Daya Manusia, dan Satker yang melaksanakan tugas pemrosesan data milik lembaga lain (misalnya: perbankan) atas amanat Undang-Undang, sebagai contoh DPSP dalam infrastruktur sistem pembayaran (RTGS, SKNBI dan BI-FAST). Dengan koordinasi ini diharapkan terciptanya harmonisasi peraturan sehingga tidak terjadi tumpang tindih dalam menjalankan tugas dan kewenangan masing-masing.

6. Pengaturan Transfer Data *Fraud* antar Industri

Bank Indonesia selaku otoritas/regulator perlu mengeluarkan kebijakan yang mengatur mengenai transfer data antar industri termasuk pula transfer data *fraud* (antara lain terkait dengan Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme/APUPPT, termasuk *social engineering*) dengan mekanisme pengamanan data yang ketat, seperti enkripsi, data masking atau data anonim, sehingga memastikan privasi data nasabah tetap aman dan terjaga. Untuk kepentingan nasional wide, BI dapat menginisiasi dengan membentuk pusat cepat tanggap scam nasional. Hal ini dengan berkaca pada negara Malaysia yang telah membentuk the National Scam Response Center (NSRC) yang diumumkan oleh Departemen Perdana Menteri pada tanggal 14 Oktober 2022. NSRC ini merupakan sebuah pusat operasional untuk mengoordinasikan respons secara cepat terhadap penipuan/*fraud* keuangan. Respons ini mencakup deteksi lebih cepat atas dana curian dan tindakan penegakan hukum terhadap pelanggaran kejahatan. Hal ini bisa dijadikan contoh untuk membuat penyelesaian risiko timbulnya *fraud* tidak hanya di sektor keuangan di Bank Indonesia, namun keseluruhan otoritas keuangan, seperti OJK, LPS dan Kemenkeu. BI dapat menginisiasi dengan memfasilitasi untuk membuat aplikasi/*data warehouse* berupa daftar *fraudster* nasional (DFN), yang dapat di akses oleh OJK, LPS, dan Kementerian Keuangan.

Di sisi lain, BI sedang mengembangkan *Fraud Detection System* dalam Aplikasi BI-Payment Info yang salah satunya menyediakan *data exhchange platform* dan Fitur BI-Payment Clear yang antara lain menyediakan *data base fraudsters.*[90]

7. Pengaturan *Self Regulation Organization* (SRO)

BI perlu mengatur LJK untuk membuat aturan main yang dibuat oleh dan untuk kalangan industri atau dikenal dengan *Self Regulation Organization* (SRO) yang tertuang dalam *bye laws*/SK asosiasi. Aturan spesifik pelindungan data pribadi untuk LJK yang diawasi BI, memedomani ketentuan yang diatur oleh Bank Indonesia, yang sampai saat ini masih tersebar di berbagai peraturan (tidak terintegrasi dalam 1 peraturan mengenai implementasi pelindungan data pribadi untuk lembaga jasa keuangan yang diawasi oleh BI).

8. Edukasi dan Meningkatkan Literasi

Diperlukan kebijakan untuk meningkatkan literasi dan kesadaran terhadap *stakeholders* terkait pentingnya menjaga data pribadi, baik sebagai pemilik, pengelola, maupun pengendali data. BI dan berbagai pihak terkait diharapkan meningkatkan literasi melalui kampanye edukasi, seminar, dan pelatihan yang bertujuan untuk memberikan pemahaman yang lebih mendalam tentang pentingnya menjaga keamanan data pribadi.

5.2. Rekomendasi Teknis

1. Pengembangan Standar Operasional untuk Pelindungan Data Pribadi

Bank Indonesia perlu mengatur mengenai spesifikasi teknis dan operasional yang detil untuk memastikan keamanan data umum dan spesifik pegawai serta *stakeholders* terkait. Pengaturan juga mengatur mengenai penggunaan teknologi enkripsi, firewall, serta audit keamanan sistem yang teratur guna memastikan data tetap aman dari ancaman. Hal tersebut termasuk pedoman implementasi mengenai bagaimana data dikelola, disimpan, dan dilindungi dalam sistem BI maupun industri. Seperti penyusunan ROPA, DPIA, transparansi penggunaan data pribadi (*privacy notice*), mekanisme pengajuan ganti rugi, penunjukkan DPO.

2. Penerapan Prosedur Transfer Data Fraud dengan Pengamanan Data

Proses transfer data *fraud* antar industri keuangan harus dilaksanakan dengan penggunaan enkripsi kuat atau teknik anonimisasi dan data masking. Protokol transfer ini harus diatur secara ketat, sehingga data fraud yang dipertukarkan hanya dapat diakses oleh pihak-pihak yang berwenang dan dilindungi dari penyalahgunaan.

3. Survei Pegawai yang Memperhatikan Pelindungan Data Pribadi

Survei yang dilakukan pada pegawai harus mematuhi regulasi pelindungan data pribadi. Bank Indonesia perlu menetapkan pedoman teknis dalam pelaksanaan survei agar data pribadi dan data kesehatan yang dikumpulkan tetap mengacu pada peraturan Pelindungan Data Pribadi.

4. Standar Keamanan di Lembaga Jasa Keuangan

DPO di lembaga jasa keuangan harus memastikan bahwa setiap penggunaan data pribadi dalam operasional sehari-hari sesuai dengan standar keamanan yang diatur oleh BI, seperti menggunakan enkripsi untuk penyimpanan data, melakukan audit berkala terhadap sistem (internal dan independen), dan memastikan data disimpan dengan cara yang aman.

5. Monitoring dan Pelaporan Keamanan Data Secara Berkala

BI perlu mengatur dan mengimplementasikan sistem monitoring dan pelaporan berkala terkait keamanan data pribadi, termasuk kemungkinan penggunaan *suptech* dan *regtech.* Hal ini dapat mencakup pelaporan rutin mengenai kebocoran data, serangan siber, serta kepatuhan terhadap standar operasional dan regulasi yang ada maupun berkala, seperti ketika diminta laporan kebocoran data oleh Lembaga Pengawas PDP, secara bersamaan melaporkan pula kepada Bank Indonesia.

Rekomendasi kebijakan dan teknis ini perlu dituangkan dalam suatu peraturan yang mengikat para pihak untuk dipatuhi dan dilaksanakan. Berdasarkan PBI tentang

[90]Pengembangan yang dilakukan oleh DKSP terkait ***BI-Payment Clear,*** *merupakan* ***skema untuk memperkuat kapasitas industri dalam manajemen risiko*** *dan memperkuat integritas transaksi. Pelaku industri akan melakukan* ***flagging dan penolakan atas transaksi fraudsters / mencurigakan (suspicious transactions).***

Pembentukan Peraturan di Bank Indonesia, Bank Indonesia memerlukan pengaturan ke luar (eksternal) dan ke dalam (internal) yang dituangkan dalam penyusunan PBI, PDG dan PADG/PADGI. Penulis memandang BI perlu untuk mengatur Pelindungan Data Pribadi secara khusus sebagai pelaksanaan mandat yang diberikan oleh UU PDP.

Di samping itu, Bank Indonesia telah mengatur mengenai PDP namun masih tersebar di berbagai peraturan sebagaimana yang telah diuraikan pada Bab 4.3. BI baru-baru ini telah menerbitkan PDG khusus mengenai PDP **(Lampiran 8)**.

Dalam penyusunan PBI/PDG dan PADG/PADGI, penulis mencoba menyusun substansi yang perlu diatur dalam peraturan dimaksud yaitu sebagai berikut **(lampiran 9)**.

1. Peraturan Bank Indonesia (PBI) tentang PDP. Hal-hal yang perlu diatur dalam PBI ini a.l. yaitu:

   Jenis data pribadi, hak-hak data pribadi, kepatuhan terhadap prinsip-prinsip pelindungan data pribadi, keamanan data domestik dan *cross border*, kewajiban pengendali data pribadi dan prosesor data pribadi dalam pemrosesan data pribadi (*Data protection officer, Record of Processing Activities (ROPA), Data Protection Impact Assessment (DPIA),* kepatuhan dan manajemen risiko (audit internal, audit TI independen, audit keuangan, DRP (*disaster recovery plan*) pengelolaan *fraud*, *penetration test,* melakukan evaluasi secara berkala, sertifikasi/ISO, melakukan simulasi keamanan siber dan non-siber), transfer data pribadi baik antar otoritas maupun pertukaran data fraud, koordinasi dengan lembaga pengawas serta sanksi serta penyelesaian sengketa
2. Peraturan Anggota Dewan Gubernur (PADG) tentang PDP. Hal-hal yang perlu diatur dalam PADG ini a.l. yaitu:

   Jenis data pribadi, pengelolaan dan pemrosesan data pribadi, prinsip-prinsip dan dasar pemrosesan data pribadi, transfer data pribadi antar otoritas, lembaga pengawas, koordinasi dengan lembaga pengawas maupun otoritas terkait, tugas dan wewenang *Data Protection Officer* (DPO) serta aturan teknis mengenai *Record of Processing Activities* (ROPA), *Data Protection Impact Assessment* (DPIA), *Self-Regulatory Organization* (SRO) serta sanksi.
3. Peraturan Anggota Dewan Gubernur Intern (PADGI) tentang PDP. Hal-hal yang perlu diatur dalam PADGI ini a.l. yaitu:

   Bank Indonesia saat ini memiliki PADG Intern Pelindungan Data Pribadi yang mengatur mengenai kerangka pengelolaan yang terdiri dari identifikasi, penatakelolaan, pengendalian, komunikasi, serta proteksi. Selanjutnya, pemrosesan data pribadi yang terdiri dari pemerolehan, pengolahan dan penganalisisan, penyimpanan, perbaikan dan pembaruan, penampilan, pengumuman, transfer, penyebarluasan atau pengungkapan serta pemusnahan data. Ketiga, hubungan dengan eksternal. Keempat, tindakan atas pelanggaran/sanksi.

   Dalam hal ini penulis memberikan rekomendasi terkait dengan tambahan pengaturan dalam PADG Intern antara lain mengenai pertukaran data pribadi, koordinasi dengan lembaga pengawas maupun otoritas terkait, pengawasan, *Data Protection Officer* (DPO) serta mekanisme *Record of Processing Activities* (ROPA), *Data Protection Impact Assessment* (DPIA), *Self-Regulatory Organization* (SRO)

Rekomendasi peraturan BI di atas perlu mempertimbangkan RPP yang masih digodog oleh Pemerintah. Hal ini diperlukan guna harmonisasi peraturan antara Pemerintah dengan BI.

Dalam hal diperlukan, industri dapat membuat aturan main sendiri yang dikeluarkan oleh asosiasi yang ditunjuk/disetujui oleh BI dan pengaturannya dimandatkan oleh Bank Indonesia sebagaimana usulan rekomendasi teknis dari penulis, khususnya terkait dengan pertukaran data *fraud*. Untuk tetap terjaga keamanan data yang dipertukarkan, data tersebut dapat dibuat anonym atau dilakukan enkripsi maupun dilakukan *masking* sehingga memitigasi risiko timbulnya kebocoran data dalam kegiatan pertukaran data tersebut. Aturan main, atau yang biasanya dikenal dengan nama *byelaws* ini memberikan keleluasaan bagi industri untuk menentukan mekanisme yang akan digunakan dengan tetap melaksanakan prinsip kehati-hatian sehingga keamanan data tetap terjamin dan terjaga.

Penulis menegaskan kembali mengenai pentingya pengaturan BI, baik eksternal maupun internal. Saat ini, BI baru memiliki Peraturan Dewan Gubernur No 11 Tahun 2024 tentang Pelindungan Data Pribadi di Bank Indonesia. Berdasarkan PBI tentang Pembentukan Peraturan di Bank Indonesia (18/42/PBI/2016), penerbitan PDG ini menurut hemat penulis perlu juga mengatur secara eksternal sehingga perlu dilakukan penyusunan PBI yang akan menjadi payung hukum bagi lembaga jasa keuangan terkait dengan PDP. Dengan demikian, penulis merekomendasikan untuk menyusun peraturan sesuai dengan hierarki tata urutan pembentukan peraturan, dalam hal ini perlu disusun PBI tentang PDP untuk eksternal dan kemudian didelegasikan ke PADG dan PADGI. Di samping perangkat aturan yang memadai, perlu juga mempertimbangkan substansi yang perlu diatur terkait dengan pelindungan data pribadi.

Daftar Pustaka

Antara News, “Pakar sebut kebocoran data BI perlu segera dihentikan”, https://www.antaranews.com/berita/2674793/pakar-sebut-kebocoran-data-bi-perlu-segera-dihentikan, 31 Januari 2022. Diakses pada: 25 April 2024

A Report by OC Queen Street LLC, Regulations at a Glance for Financial Institutions: Reconciling the Draft Cybersecurity Bill, the Monetary Authority of Singapore Regulations and the Public Consultation for Approaches to Managing Personal Data in the Digital Economy.

ASEAN Digital Senior Officials’ Meeting, “ASEAN Data Management Framework: Data Governance and Protection throughout the data lifecycle”, 2021, https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf

Astfalk, S., & Schunck, C. H, "Balancing Privacy and Value Creation in the Platform Economy: The Role of Transparency and Intervenability”, Balancing Privacy and Value Creation in the Platform Economy. 10.18420/OID2023_12, 2023. Diakses pada: 23 April 2024

Australian Government, “Privacy Act 1988”, Dec 2019. https://www.legislation.gov.au/C2004A03712/2019-08-13/text

Bakermckenzie, “Global Data Privacy and Cybersecurity Handbook: Thailand”, 2024, https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/asia-pacific/thailand/topics/data-protection-officers. Diakses pada: 26 September 2024

Bangko Sentral Ng Pilipinas, “About the Bank”, 2024, https://www.bsp.gov.ph/Pages/AboutTheBank/BSPPrivacyPolicy.aspx. Diakses pada: 10 September 2024

Bank Indonesia, Siaran Pers Bank Indonesia, “BI 7-Day Reverse Repo Rate Tetap 5,75%: Sinergi Menjaga Stabilitas Dan Mendorong Pertumbuhan”, https://www.bi.go.id/id/publikasi/ruang-media/newsrelease/Pages/sp_2525923.aspx

Bank negara Malaysia, Privacy Statement”2024, https://www.bnm.gov.my/privacy-statement#:~:text=The%20Bank%20does%20not%20collect,your%20browser%20history%20(cache). Diakses pada: 23 September 2024

Bank of England, “Privacy and the Bank of England”, 2024, https://www.bankofengland.co.uk/legal/privacy. Diakses pada: 7 Agustus 2024

Bank of Thailand, “Personal Data privacy Policy”, https://www.bot.or.th/en/privacy-policy.html. Diakses pada: 25 September 2024

California Department of Justice, “California Consumer Privacy Act (CCPA)”, 2024, https://oag.ca.gov/privacy/ccpa. Diakses pada: 21 Maret 2024

CNBC Indonesia, “BFI Finance Diserang Hacker, Nasabah Takut Tagihan Menggunung”, 25 Mei 2023, https://www.cnbcindonesia.com/market/20230525151416-17-440614/bfi-finance-diserang-hacker-nasabah-takut-tagihan-menggunung

CNBC Indonesia, “Heboh Nasabah BCA Kebobolan Rp68,5 Juta, Begini Kronologinya”, 13 November 2023, https://www.cnbcindonesia.com/market/20231113141815-17-488611/heboh-nasabah-bca-kebobolan-rp685-juta-begini-kronologinya. Diakses pada: 25 April 2024

CNBC Indonesia, “BPD Bali Kebobolan, Rp21,59 M Dana Nasabah Raib”, 15 November 2023, https://www.cnbcindonesia.com/market/20231115063713-17-489065/bpd-bali-kebobolan-rp2159-m-dana-nasabah-raib

Djafar, W dan Santoso, M.J “Perlindungan Data Pribadi: Konsep, Instrumen, dan Prinsipnya”, Lembaga Studi dan Advokasi Masyarakat, 2019. https://elsam.or.id/storage/files/2/Policy%20Brief%20Perlindungan%20Data%20Pribadi%20KOnsep,%20instrumen%20dan%20prinsipnya%20oke.pdf. Di akses pada: 1 Agustus 2024

DLA PIPER, “Data Protection Officer in Thailand”, 2024. Diakses pada: 29 Mei 2024

Duggal, N “What Is Data Processing: Cycle, Types, Methods, Steps and Examples”, 24 Juli 2023, https://www.simplilearn.com/what-is-data-processing-article#examples_of_data_processing. Diakses pada: 20 Agustus 2024

Dwi Tjahja K. Wardhono, Retno Muhardini, Dian Puji Nugraha Simatupang, Nadhia Shalehanti, “Crisis, Hazard, and Disaster Management: A Study of Regulatory Formulation and Institutional Coordination”, *Journal of Central Banking Law and Institutions Vol 2 No 3,* 2023, ttps://doi.org/10.21098/jcli.v2i3.193. Di akses pada: 20 November 2024

European Commission, “Data protection in the EU”, 2016, https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en. Diakses pada: 3 Juni 2024

European Data Protection Board, “task and duties”, https://www.edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en. Diakses pada: 3 Juni 2024

European Data Protection Board, “EDPB Documenton response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research”, di akses pada: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf, 2 February 2021. Diakses pada: 12 Agustus 2024

European Union Law, “Directive (EU) 2016/680 of the European Parliament and of the Council”, 27 April 2016 https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC. Diakses pada: 13 Mei 2024

European Union Law, “Regulation (EU) 2016/679 of the European Parliament and of the Council”, https://eur-lex.europa.eu/eli/reg/2016/679/oj. Diakses pada: 20 Maret 2024

Federal Reserve, “Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices”, https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf. Diakses pada: 5 Juni 2024

Federal Trade Commission: Protecting America’s Consumers, “Protecting Consumer Privacy and Security”, 2024, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security. Diakses pada: 4 Juni 2024

Fintech Indonesia, “AFTECH Annual Members Survey 2022/2023, Industri Fintech Indonesia Semakin Mantap Melangkah Menuju Arah Keberlanjutan dan Inklusi”, https://fintech.id/id/dokumen/siaran-pers-aftech-annual-members-survey-20222023-industri-fintech-indonesia-mantap-melangkah-menuju-arah-keberlanjutan-dan-inklusi

Fullstory, “What is data processing? Definition, steps & methods”, 14 Maret 2024, https://www.fullstory.com/blog/what-is-data-processing/. Diakses pada: 15 Mei 2024

GDPR. Art. 17 GDPR Right to erasure (‘right to be forgotten’), https://gdpr-info.eu/art-17-gdpr/. Diakses pada: 13 Mei 2024

Government of Canada, “Personal Information Protection and Electronic Documents Act”, 2000. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html#h-416889. Diakses pada: 20 Maret 2024

Government of Canada, “Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96”, https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-7.html#h-417659.

Hall Booth Smith, “Understanding Malaysia’s 2024 Data Privacy Reform: Essential Insights for Business Leaders”, 1 Oktober 2024. Diakses pada: 20 Mei 2024

Hendri Sasmita Yuda, “Tata kelola Pelindungan Data Pribadi: UU PDP dan Arah Pengaturannya”, Webinar OJK Institute, 30 Mei 2024, https://www.ojk.go.id/ojk-institute/en/capacitybuilding/upcoming/4169/peluang-dan-tantangan-pelindungan-data-pribadi-dalam-transaksi-di-era-digital. Diakses pada: 30 Mei 2024

Hui, K. L., & Png, I. P, “Economics of privacy. Handbooks in Information Systems”, Vol. 1. Elsevier. https://www.comp.nus.edu.sg/~ipng/research/privacy_HISE.pdf, 2005. Diakses pada: 24 April 2024

Indonesia Securities Investor Protection Fund (Indonesia SIPF), “Skema Ponzi, Ancaman Bagi Perkembangan Industri Jasa Keuangan”, Maret 2024, https://www.indonesiasipf.co.id/uploads/media/bulletin/bulletin-sipf_q1_2024.pdf. Diakses pada: 23 Juli 2024

Information Commissioner’s Office, “The benefits of data protection laws”, https://ico.org.uk/for-organisations/advice-for-small-organisations/the-benefits-of-data-protection-laws/#:~:text=And%20you%20have%20to%20 protectdiscrimination%20or%20even%20physical%20harm. Diakses pada: 31 Mei 2024

Intersoft Consulting, “Art. 17 GDPR Right to erasure (‘right to be forgotten’)”, https://gdpr-info.eu/art-17-gdpr/.

Intersoft Consulting, “General Data Protection Regulation (GDPR)”, 2018, https://gdpr-info.eu/. Diakses pada: 13 Mei 2024

Intersoft Consulting, “GDPR: Data Protection Officer”, 2024, https://gdpr-info.eu/issues/data-protection-officer/. Diakses pada: 13 Mei 2024

ISO, “ISO/IEC 27001:2022”, 2022, https://www.iso.org/standard/27001. Di akses pada 15 November 2024

Jamal Wiwoho, Dona Budi Kharisma, Dwi Tjahja K. Wardhono, “Financial Crime in Digital Payments”, *Journal of Central Banking Law and Institutions Vol 1 No 1*, 2022, DOI: 10.21098/jcli.v1i1.7. Diakses pada: 24 April 2024

Jaringan Dokumentasi dan Informasi HukumBPK (JDIH BPK), “Undang-Undang Pelindungan Data Pribadi”, https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

JDIH BPK, “Undang-Undang Perlindungan Data Pribadi”, 2022, https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022. Diakses pada: 18 Maret 2024

Joanna Kulesza, “Privacy”, In: Schintler, L., McNeely, C. (eds) Encyclopedia of Big Data. Springer, Cham. 2019, https://doi.org/10.1007/978-3-319-32001-4_314-1. Diakses pada: 11 Juli 2024

Kominfo, Siaran Pers No.138/HM/KOMINFO/07/23, “Perkembangan Penanganan Dugaan Kebocoran Data Paspor 34,9 Juta Warga Indonesia”, https://www.kominfo.go.id/content/detail/50065/siaran-pers-no-138 hmkominfo072023-tentang-perkembangan-penanganan-dugaan-kebocoran-data-paspor-349-juta-warga-indonesia/0/siaran_pers

Kominfo, “5 Alasan Mengapa Data Pribadi Perlu Dilindungi”, 16 Juli 2019, https://www.kominfo.go.id/content/detail/19991/5-alasan-mengapa-data-pribadi-perlu-dilindungi/0/sorotan _media. Diakses pada: 18 Maret 2024

Lu Sudirman, Hari Sutra Disemadi, dan Arwa Meida Aninda, 2023, *Comparative Analysis of Personal Data Protection Laws in Indonesia and Thailand: A Legal Framework Perspective*, Journal of Etika Demokrasi, Vol. 8 No. 4.

Malaysia Government, “Personal Data protection Actt 2010”, 2010, https://www.pdp.gov.my/jpdpv2/assets/2019/09/Personal-Data-Protection-Act-2010.pdf. Diakses pada: 20 Mei 2024

Monetary Authority of Singapore, “Notification of Data Breaches to The Monetary Authority Of Singapore (“THE AUTHORITY”), 22 February 2023, https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/id/id03_23/id03_23.pdf. Diakses pada: 23 September 2024

Monetary Authority of Singapore, “MAS Privacy Policy Statement”, 2024, https://www.mas.gov.sg/privacy-statement#:~:text=Statement%20of%20Commitment%20and%20Assurance,that%20you%20share%20with%20us. Diakses pada: 17 September 2024

Nisaputra, R “Permasalahan Fintech yang harus diwaspadai di 2024”. https://infobanknews.com/ini-dia-7-permasalahan-fintech-yang-harus-diwaspadai-di-2024/, 29 Desember 2023. Diakses pada: 19 April 2024

OECD Legal Instrument, “Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data”, 2013, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Diakses pada: 10 Juni 2024

OECD, “Mapping Data Portability Initiatives, Opportunities And Challenges”, OECD Digital Economy Papers, December 21 No.321 p.9, https://www.oecd.org/en/publications/mapping-data-portability-initiatives-opportunities-and-challenges_a6edfab2-en.html#:~:text=Data%20portability%20has%20become%20an,costs%20and%20lock%2Din%20effects. Diakses pada: 7 Oktober 2024

Official Journal of the European Union, “Regulations”, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Diakses pada: 13 Mei 2024

Opderbeck, D. W, “Cybersecurity, data breaches, and the economic loss doctrine in the payment card industry”, Maryland Law Review Vol.75, 2016 Diakses pada: 23 April 2024

Otoritas Jasa Keuangan, “Roadmap Perusahaan Pembiayaan 2023-2027”, https://ojk.go.id/id/regulasi/otoritas-jasa-keuangan/rancangan-regulasi/Documents/Draft%20Roadmap%20Pengembangan%20Perusahaan%20Pembiayaan%20Indonesia.pdf. Diakses pada: 16 April 2024

Parliament of Malaysia, “Personal Data Protection Act 2010”, 2010, https://mohre.um.edu.my/img/files/Personal%20Data%20Protection%20(PDPA)%20Act%202010.pdf. Diakses pada: 23 September 2024

Pauletto, C “Options towards a global standard for the protection of individuals with regard to the processing of personal data”, Computer Law & Security Review, 2020, https://doi.org/10.1016/j.clsr.2020.105433. Diakses pada: 23 April 2024

PDPA Thailand, “Section 28-PDPA Thailand”, https://pdpathailand.com/pdpa/content_eng/article28_eng.php?srsltid=AfmBOorxz_vn2Y5oYEii3f7nImelNi2c3s2K-1K-x_w_9oKPIyuTJ9EM, 2019. Diakses pada: 25 September 2024

Purnama, T.D. & Alhakim, A, “Pentingnya UU Pelindungan Data Pribadi sebagai bentuk Pelindungan Hukum terhadap Privasi di Indonesia”, e-Journal Komunitas Yustisia Universitas Pendidikan Ganesha. Diakses pada: 19 April 2024

Personal Data Protection Commission Singapore, “PDPA Overview”, 2024, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act. Diakses pada: 29 Mei 2024 dan 17 September 2024

Personal Data Protection Commission, “Data Protection Obligations”, 2024, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act/data-protection-obligations. Diakses pada: 17 September 2024

Rekiana Nisaputra, “Permasalahan Fintech yang harus diwaspadai di 2024”, 29 Desember 2023, https://infobanknews.com/ini-dia-7-permasalahan-fintech-yang-harus-diwaspadai-di-2024/

Secure Privacy, “What Is a Data Protection Officer and Do You Need One?”, 19 Januari 2024, https://secureprivacy.ai/blog/data-protection-officer-guide#:~:text=The%20CCPA%20does%20not%20require,or%20a%20third%2Dparty%20vendor. Diakses pada: 20 Mei 2024

Siaran Pers AFTECH AMS 2022/2023, “Industri Fintech Indonesia Mantap Melangkah Menuju Arah Keberlanjutan dan Inklusi”, 27 Juli 2023. https://fintech.id/id/dokumen/siaran-pers-aftech-annual-members-survey-20222023-industri-fintech-indonesia-mantap-melangkah-menuju-arah-keberlanjutan-dan-inklusi. Diakses pada: 17 April 2024

Siaran Pers Bank Indonesia, “BI 7-Day Reverse Repo Rate Tetap 5,75%: Sinergi Menjaga Stabilitas Dan Mendorong Pertumbuhan”. Diakses pada: 16 April 2024

Siaran Pers No.138/HM/KOMINFO/07/23, “Perkembangan Penanganan Dugaan Kebocoran Data Paspor 34,9 Juta Warga Indonesia”, https://www.kominfo.go.id/content/detail/50065/siaran-pers-no-138hmkominfo072023-tentang-perkembangan-penanganan-dugaan-kebocoran-data-paspor-349-juta-warga-indonesia/0/siaran_pers. Diakses pada: 18 April 2024

Smith, H.B, “Understanding Malaysia’s 2024 Data Privacy Reform: Essential Insights for Business Leaders”, 1 Oktober 2024, https://hallboothsmith.com/malaysia-2024-data-privacy-reform/#:~:text=Introduction, compliance%20and%20maintain%20stakeholder%20trust. Diakses pada: 20 Mei 2024

Thailand Government, “Personal Data Protection Act, B.E. 2562”, 2019, https://www.dataguidance.com/sites/default/files/entranslation_of_the_personal_data_protection_act_0.pdf. Diakses pada: 29 Mei 2024

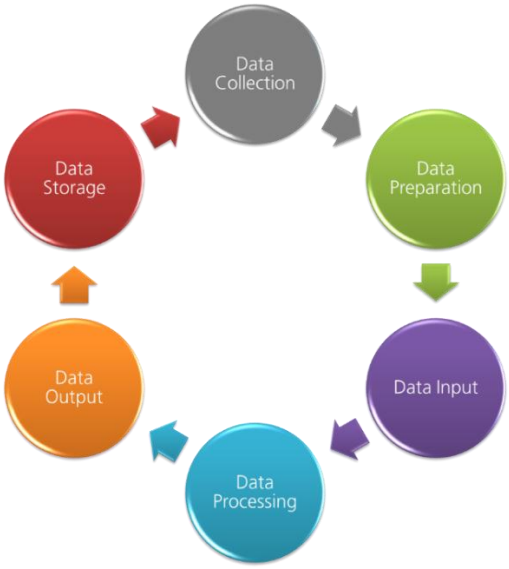
Tempo.co,” Data Bank Indonesia diretas Geng Ramsomware, Kaspersky sebut Conti sangat Aktif” https://tekno.tempo.co/read/1552218/data-bank-indonesia-diretas-geng-ransomware-kaspersky-sebut-conti-sangat-aktif, 20 Januari 2022. Diakses pada: 25 April 2024

Valentin Rupp dan Max von Grafenstein, “Clarifying “personal data” and the role of anonymisation in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection”,Computer Law & Security Review Vol. 52, April 2024, https://doi.org/10.1016/j.clsr.2023.105932. Diakses pada: 5 Juni 2024

VeraSafe, “Singapore Data Protection Officers: Everything You Need to Know”, 4 oktober 2024, https://verasafe.com/blog/singapore-data-protection-officers-everything-you-need-to-know/#:~:text=What%20law%20regulates%20data%20protection,data%20and%20bolster%20individuals'%20rights. Diakses pada: 29 Mei 2024

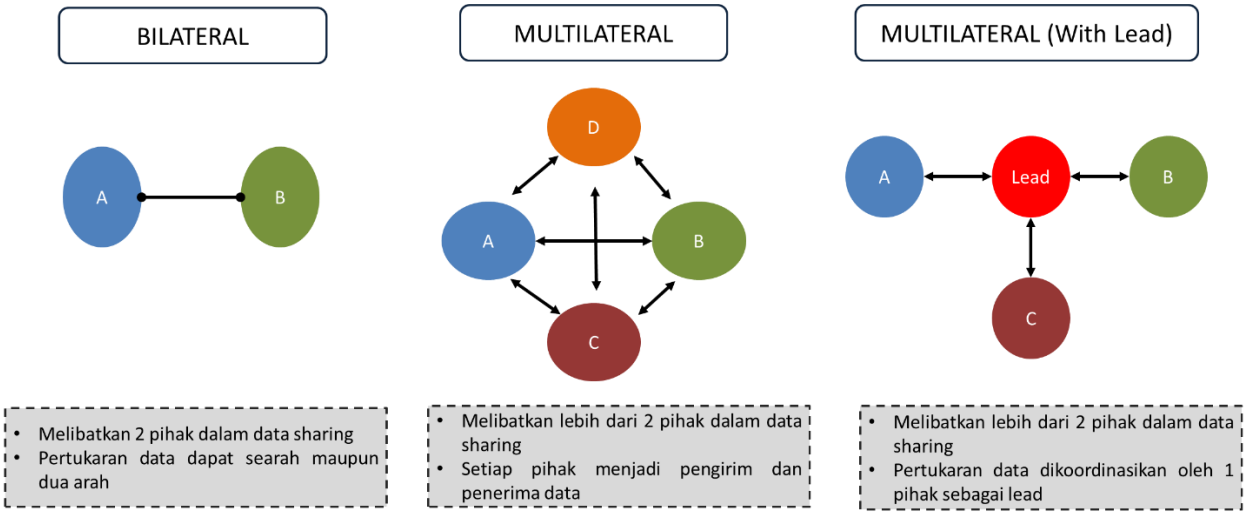
Lampiran

Lampiran 1. Proses Data



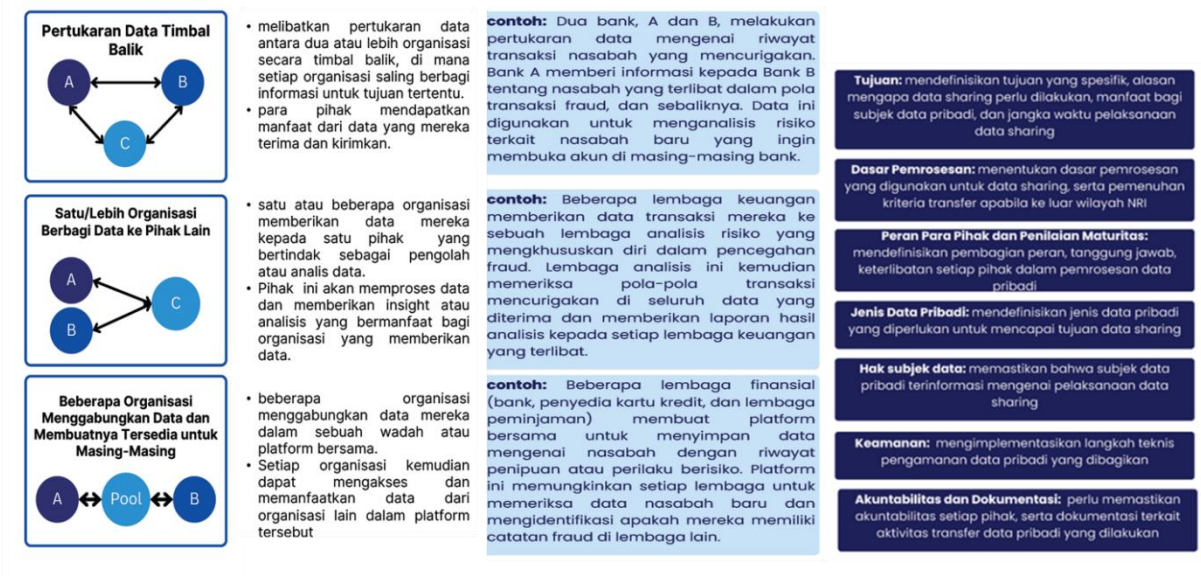
Gambar 1. Proses Data
Sumber: Nikita Duggal (2023)

Lampiran 2. Skema Model Transfer Data



Gambar 2. Skema Model Transfer Data

Lampiran 3. Penjelasan atas masing-masing skema transfer data pribadi



Lampiran 4. Pemetaan para Pihak dalam pelaksanaan transfer data pribadi berdasarkan UU PDP

Gambar 4. Pemetaan para Pihak berdasarkan Aturan PDP

Lampiran 5. Current Investigation and Reporting Structure for FIs

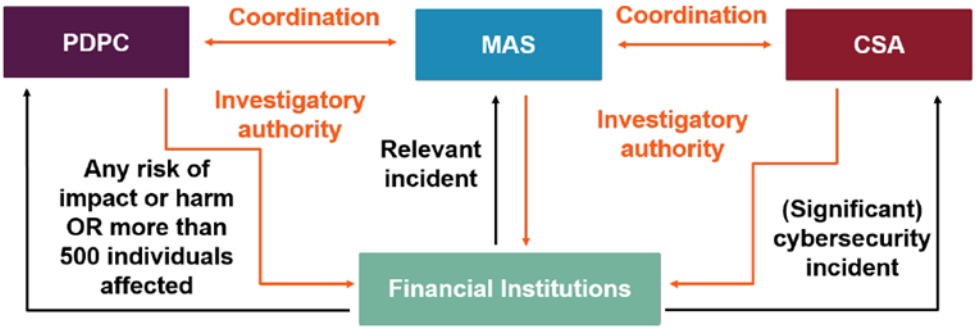


Fig 1: Current investigation and reporting structure for FIs (taking into account the Draft Bill and Consultation Paper)

Lampiran 6. Proposed Investigation and Reporting Structure for FIs

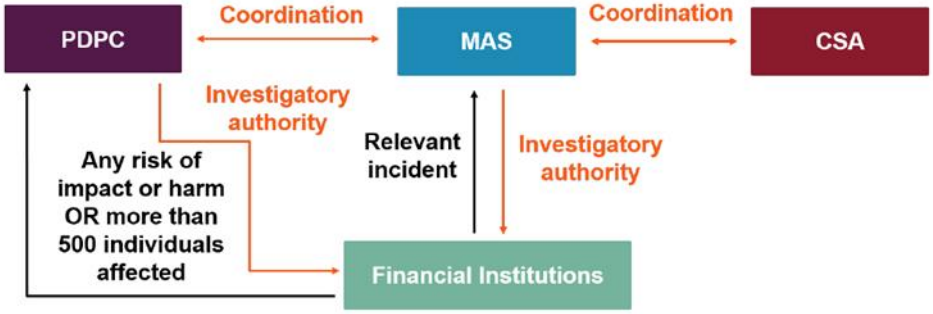
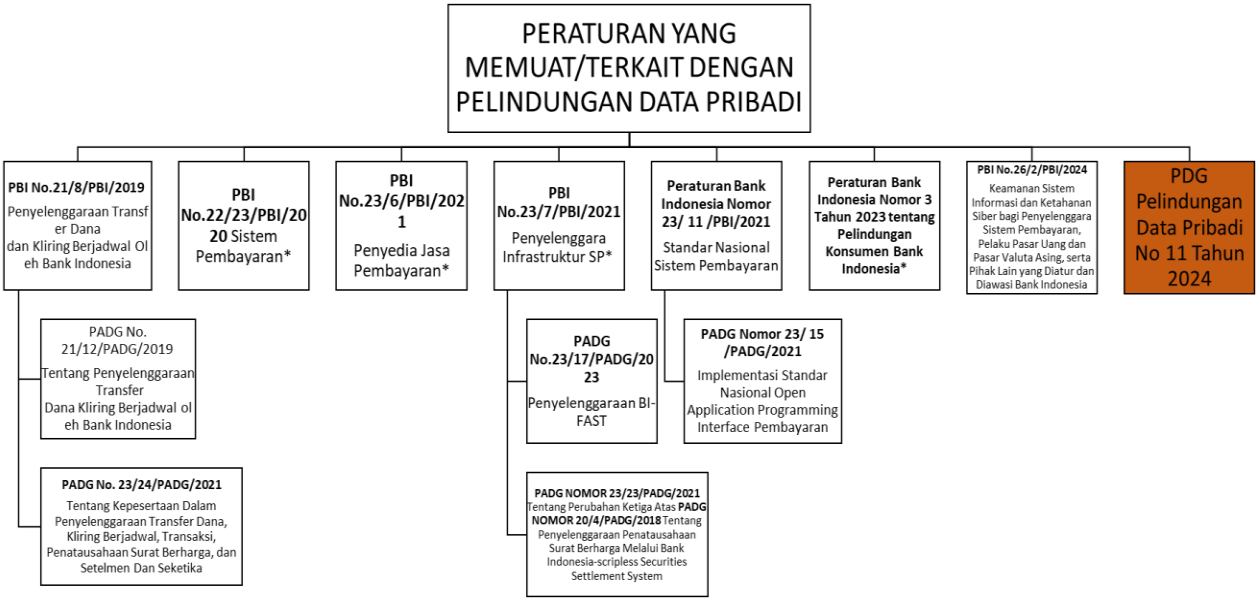


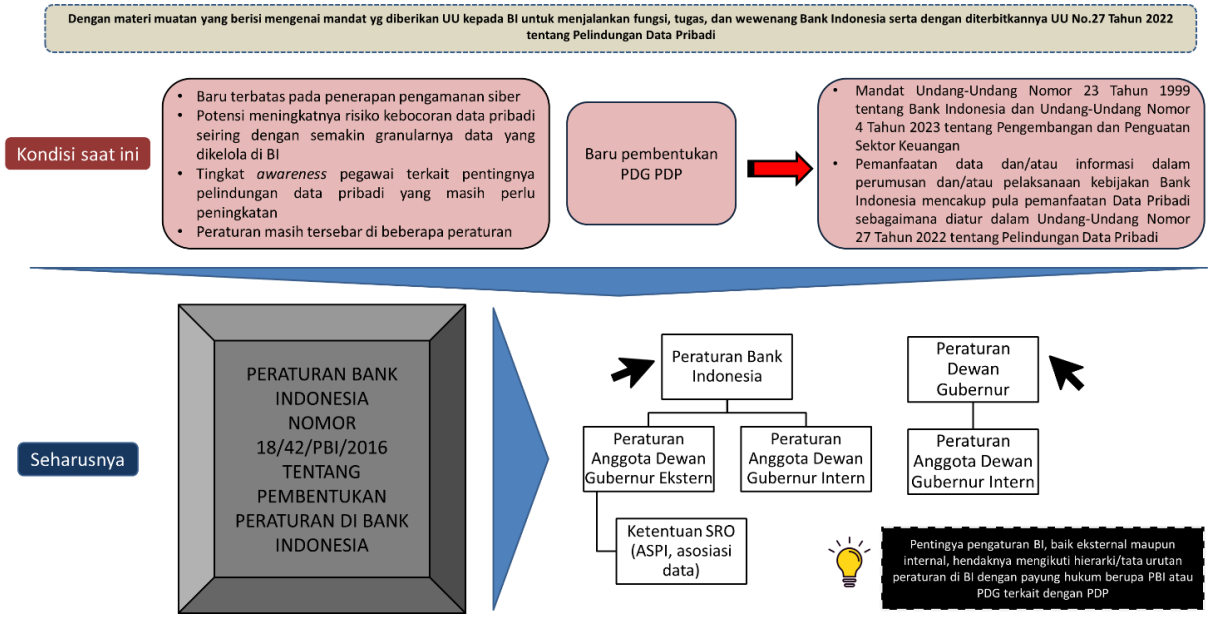
Figure 2: Proposed investigation and reporting structure for FIs (taking into account the Draft Bill and Consultation Paper)

Lampiran 7. Peraturan Bank Indonesia yang berlaku saat ini terkait Pelindungan Data Pribadi



*terdapat peraturan mengenai data pribadi, namun tidak bersifat komprehensif dan terpisah di beberapa peraturan.

Lampiran 8.



Lampiran 9. Rancangan Peraturan di Bank Indonesia

Tabel 1. Peraturan Bank Indonesia (PBI) PDP

BAB	Judul Bab	Ket
I	**Ketentuan Umum**	
II	**Jenis data pribadi**	
	Data Pribadi Umum	
	Data Pribadi Spesifik	
III	**Prinsip-prinsip Pelindungan data pribadi**	Pasal prinsip-prinsip umum 1. Menyebutkan prinsip-prinsip apa saja 2. LJK wajib memenuhi prinsip-prinsip umum (LJK wajib memenuhi prinsip umum dalam penyelenggaraan Sistem Pembayaran yang yaitu kewajiban penyelenggaraan yang meliputi aspek pemenuhan ketentuan peraturan perundang-undangan) 3. Penerapan prinsip pelindungan data pribadi dilakukan dengan mempertimbangkan aspek kepentingan publik dan/atau persyaratan lain yang ditetapkan oleh otoritas
IV	**Hak subjek data pribadi**	
	Hak untuk Diberitahu	
	Hak Akses	
	Hak untuk Perbaikan	
	Hak untuk Dihapus / Hak untuk Dilupakan	
	Hak untuk Menarik Persetujuan	
	Hak untuk Menolak Pengambilan Keputusan Otomatis dan Profiling	
	Hak untuk Membatasi Pemrosesan	
	Hak atas Portabilitas Data	
	Hak untuk Mengajukan Klaim	
V	**Keamanan data**	
	penerapan SOP mengenai pengelolaan risiko	➢ Aspek-aspek standar keamanan sistem informasi mencakup: a. ketersediaan kebijakan dan prosedur tertulis sistem informasi; b. penggunaan sistem yang aman dan andal paling sedikit: • pengamanan dan pelindungan kerahasiaan data; • pengelolaan *fraud*; • pemenuhan sertifikasi dan/atau standar keamanan dan keandalan sistem; dan
	memiliki audit internal	
	kepatuhan dan manajemen risiko	
	memiliki DRP (*disaster recovery plan*)	
	pengelolaan fraud	
	penetration test	
	audit TI independen	
	audit keuangan	
	melakukan evaluasi secara berkala	
	sertifikasi/ISO	
	melakukan simulasi keamanan siber dan non-siber	
	aspek keamanan data cross border	

BAB	Judul Bab	Ket
		• pemeliharaan dan peningkatan keamanan teknologi; c. penerapan standar keamanan siber; d. pengamanan data dan/atau informasi; dan e. pelaksanaan audit sistem informasi secara berkala. ➢ LJK bertanggung jawab atas keamanan dan kelancaran pemrosesan transaksi pembayaran yang dilakukan oleh Penyelenggara Penunjang
VI	**Kewajiban Pengendali Data Pribadi Dan Prosesor Data Pribadi dalam Pemrosesan Data Pribadi**	➢ Mekanisme pemrosesan data dan/atau informasi terkait Sistem mencakup: a. akses dan tata cara pemrosesan; b. standardisasi data, standardisasi teknis, standardisasi keamanan, dan standardisasi tata kelola; dan/atau c. mekanisme lainnya yang ditetapkan Bank Indonesia ➢ Terkait pemrosesan dan pengumpulan data pribadi, LJK dan/atau pihak yang bekerja sama dengan LJK wajib melakukan: • menerapkan prinsip pelindungan data pribadi termasuk memenuhi aspek persetujuan Pengguna Jasa atas penggunaan data pribadinya yang meliputi: • pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, patut, dan transparan; • pemrosesan data pribadi dilakukan sesuai dengan tujuannya; • pemrosesan data pribadi dilakukan dengan menjamin hak pemilik data pribadi; • pemrosesan data pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tujuan pemrosesan data pribadi;

BAB	Judul Bab	Ket
		• pemrosesan data pribadi dilakukan dengan melindungi keamanan data pribadi dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan data pribadi; • pemrosesan data pribadi dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan pelindungan data pribadi; dan • pemrosesan data pribadi dimusnahkan dan/atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan. • memenuhi mekanisme pemrosesan data dan/atau informasi terkait Sistem Pembayaran yang ditetapkan oleh Bank Indonesia, termasuk mekanisme pemrosesan melalui infrastruktur data dan infrastruktur Sistem Pembayaran Bank Indonesia; • memenuhi mekanisme pemanfaatan infrastruktur data pihak ketiga yang ditetapkan oleh Bank Indonesia; • menerapkan manajemen risiko siber dalam penyelenggaraan Sistem Pembayaran, termasuk standar keamanan sistem informasi; • memperhatikan integritas data yang merepresentasikan fakta atau keadaan yang sebenarnya dan konsisten dengan menggunakan metode yang transparan; dan • memenuhi ketentuan peraturan perundang-undangan. ➢ *Data protection officer* ➢ *Record of ProcessingActivities (ROPA)* ➢ *Data Protection Impact Assessment (DPIA)*

BAB	Judul Bab	Ket
VII	**Transfer data pribadi**	
	Pertukaran data antar otoritas, lembaga jasa keuangan (domestik maupun *cross border*)	Bank Indonesia memberikan persetujuan sepanjang terdapat jaminan dari LJK bahwa pemrosesan di luar wilayah Negara Kesatuan Republik Indonesia tidak mengurangi efektivitas pengawasan, perolehan data, dan pelindungan data pribadi SRO menyusun aturan main antar LJK Tambahan APUPPT
	Pertukaran data fraud yg dianonim dan encryption (data masking)	
VIII	**Kelembagaan**	
	Lembaga Pengawas	
IX	**Koordinasi**	Dalam melaksanakan kewenangan dan fungsi di bidang Sistem Pembayaran, Bank Indonesia dapat berkoordinasi dengan otoritas, lembaga, dan/atau pihak lain
	Pelaporan	➢ LJK dan pihak yang bekerja sama wajib menyampaikan kepada Bank Indonesia atau pihak lain yang ditugaskan oleh Bank Indonesia terkait dokumen, data, informasi, dan/atau laporan dan bertanggung jawab atas keabsahan, kebenaran, kelengkapan, dan ketepatan waktu atas setiap penyampaian dokumen, data, informasi, laporan, keterangan, dan/atau penjelasan kepada Bank Indonesia. ➢ LJK menyampaikan data dan/atau informasi terkait Sistem Pembayaran kepada Bank Indonesia sesuai dengan tata cara dan mekanisme yang ditetapkan Bank Indonesia. Begitupun pihak lain yang bekerja sama dengan LJK wajib menyampaikan data dan/atau informasi terkait Sistem Pembayaran kepada Bank Indonesia sesuai dengan tata cara dan mekanisme yang ditetapkan Bank Indonesia ➢ LJK wajib menyampaikan kepada Bank Indonesia atau pihak lain yang ditugaskan oleh Bank Indonesia antara lain: Dokumen, data, informasi, laporan, keterangan, dan/atau penjelasan disampaikan melalui: a. pelaporan; b. pertemuan langsung; dan/atau c. media lain

BAB	Judul Bab	Ket
		yang ditetapkan oleh Bank Indonesia
	Pengawasan	Pengawasan terdiri dari pengawasan langsung dan tidak langsung. Pengawasan tidak langsung dilakukan melalui monitoring, identifikasi, dan/atau asesmen melalui analisis laporan, data, dan informasi yang diperoleh Bank Indonesia
X	**Penyelesaian Sengketa (LAPSI)**	perselisihan atau kebocoran data yang diadukan oleh subjek data
XI	**Sanksi**	
	Sanksi Administratif	
XII	**Ketentuan Peralihan**	
	Akan dibuat tahapan-tahapan	
XIII	Ketentuan penutup	

Peraturan Dewan Gubernur (PDG) PDP (*Existing*)

BAB	Judul Bab	Isi
I	Ketentuan Umum	Ketentuan Umum
II	Kerangka PDP	1. Kewenangan BI terkait PDP 2. Tujuan, Objek, Sasaran, dan Prinsip PDP di Bank Indonesia 3. Ruang Lingkup Pengaturan PDP
III	Perolehan Data Pribadi	1. Cakupan Data pribadi 2. Kewenangan Bank Indonesia dalam Perolehan Data Pribadi 3. Hak Subjek Data Pribadi dalam Perolehan Data Pribadi 4. Kewajiban Bank Indonesia dalam Perolehan Data Pribadi
IV	Penanganan data Pribadi	1. Kewajiban Bank Indonesia Dalam Penanganan Data Pribadi 2. Dukungan Sistem Pengamanan Fisik dan/atau Elektronik 3. Kewenangan dan Proses Pengambilan Keputusan dalam Penanganan Data Pribadi
V	Pemanfataan Data Pribadi	Pemanfaatan dan penyebarluasan data pribadi
VI	PPDP	Tugas, struktur, dan kewajiban PPDP
VII	Kewajiban, larangan, dan sanksi atas pelanggaran PDP serta Mekanisme Penanganan ganti rugi	1. Kewajiban, Larangan, dan Sanksi atas Pelanggaran PDP 2. Mekanisme Penanganan Ganti Rugi
VIII	Ketentuan Peralihan	Ketentuan Peralihan
IX	Ketentuan Penutup	Ketentuan Penutup

Draf Peraturan Anggota Dewan Gubernur (PADG) PDP

I	Ketentuan Umum	Ketentuan Umum
II	Jenis data pribadi	Data pribadi umum dan data pribadi spesifik
III	Prinsip-prinsip pelindungan data pribadi	1. Menyebutkan prinsip-prinsip 2. LJK wajib memenuhi prinsip-prinsip umum
IV	Kewajiban Pengendali Data Pribadi Dan Prosesor Data Pribadi dalam Pemrosesan Data Pribadi	1. Mekanisme pemrosesan data dan/atau informasi 2. Kewajiban pemrosesan dan pengumpulan data pribadi, LJK dan/atau pihak yang bekerja sama dengan LJK
V	Keamanan data	Penerapan SOP mengenai pengelolaan risiko, memiliki audit internal, kepatuhan dan manajemen risiko, memiliki DRP (*disaster recovery plan*), pengelolaan fraud, penetration test, audit TI independen, audit keuangan, melakukan evaluasi secara berkala, dan sertifikasi/ISO serta melakukan simulasi keamanan siber dan non-siber. Aspek-aspek tersebut juga diberlakukan untuk aspek keamanan data *cross border.*
VI	Transfer data pribadi dan pertukaran data fraud	1. Pertukaran data antar otoritas, lembaga jasa keuangan (domestik maupun *cross border*) 2. Pertukaran data fraud yg dianonim dan encryption (data masking)
VII	Koordinasi Kelembagaan	1. Lembaga Pengawas PDP 2. Koordinasi Pengawasan
VIII	Pengawasan	1. Pengawasan langsung (pemeriksaan) dan tidak langsung (pelaporan) A. Bank Indonesia sebagai otoritas pengawas B. Bank Indonesia dapat bersama-sama melakukan pengawasan langsung dan tidak langsung dengan lembaga pengawas
IX	Tugas dan Wewenang DPO	Tugas dan wewenang DPO
X	Penyelesaian Sengketa	Penyelesaian Sengketa
XI	Sanksi	Sanksi
XII	Ketentuan Peralihan	Ketentuan Peralihan
XIII	Ketentuan Penutup	Ketentuan Penutup

Draf Peraturan Anggota Dewang Gubernur Intern (PADGI)

I	Ketentuan Umum	1. Ketentuan Umum 2. *Consent*
II	Kerangka PDP	1. ROPA dan DPIA 2. Penatakelolaan 3. Pengendalian 4. Komunikasi 5. Proteksi
III	Pemrosesan Data Pribadi	1. Pemrosesan data (pemerolehan, pengolahan dan penganalisisan, penyimpanan, perbaikan dan pembaruan, penampilan, pengumuman, transfer, penyebarluasan/pengungkapan) 2. Hubungan dengan pihak eksternal
IV	Tindakan atas pelanggaran	1. Sanksi Personel 2. Permintaan atas ganti rugi dari subjek data pribadi
V	Pejabat PDP	1. Tujuan pembentukan PPDP 2. Tugas dan Kewajiban PPDP 3. Pembentukan spesifikasi teknis dan operasional 4. Pembuatan *Privacy Notice* 5. Koordinasi dengan Lembaga Pengawas PDP
VI	Edukasi dan Literasi	1. Sosialisasi inventarisasi data pribadi 2. Penyusunan program sosialisasi dan training
VII	Ketentuan Peralihan	Ketentuan Penutup
VIII	Ketentuan Penutup	Ketentuan Peralihan