Viva Justicia: Journal of Private Law
Volume 1 Nomor 2 (2025): **22–45**
ISSN: 0000-000

PELINDUNGAN DATA PRIBADI DALAM *OPEN APPLICATION PROGRAMMING INTERFACE* (OPEN API) *PAYMENT*: STUDI KOMPARATIF INGGRIS DAN INDONESIA

Pinky Eskah Prayoga* **dan R. A. Antari Inaka Turingsih**
Fakultas Hukum, Universitas Gadjah Mada,
Jl. Sosio Justicia No. 1, Bulaksumur, Kab. Sleman, D.I. Yogyakarta, 55281

Abstract
The development of Open API Payment technology enhances interoperability between banks and fintech, facilitating more efficient digital transactions. However, this technology also introduces new challenges regarding personal data breaches, as data may be shared with irresponsible third parties. Therefore, a robust legal framework for personal data protection and effective implementation measures are essential to safeguard personal data within the Open API Payment ecosystem. This research aims to review the regulation and implementation of personal data protection in Open API Payment by comparing data-sharing provisions in Indonesia and the UK. It also examines which provisions from this comparison can be adopted to improve Indonesia's regulatory framework. This research employs a normative legal methodology, using a statutory approach to analyse laws and their hierarchy, as well as a comparative approach to evaluate regulatory differences between the two countries. The findings reveal significant differences in personal data protection regulations, particularly regarding contractual agreements that define the legal relationship between data processors and regulatory oversight within the Open API Payment ecosystem. These differences highlight the need to strengthen regulatory frameworks and enhance the implementation of personal data protection measures in Indonesia. Lessons from the UK, such as more comprehensive contractual agreements and stricter regulatory supervision, can serve as a reference for improving Open API Payment regulations in Indonesia.
Keywords: *Data Protection, Open API Payment, Data Sharing, Digital Payment*

Abstrak
Pengembangan teknologi *Open* API *Payment* meningkatkan interoperabilitas antara bank dan perusahaan *fintech*, mefasilitiasi transaksi digital yang lebih efisien. Namun, teknologi ini juga mendatangkan tantangan baru terhadap kebocoran data pribadi sebagaimana dimungkinkan terjadinya pembagian data kepada pihak ketiga yang tidak bertanggung jawab. Sehingga diperlukan kerangka hukum pelindungan data pribadi dan langkah-langkah implementasinya yang memadai untuk menjamin pelindungan data pribadi dari inovasi *Open* API *Payment*. Penelitian ini bertujuan untuk mengulas pengaturan pelindungan data pribadi dan implementasinya dalam *Open* API *Payment* dengan membandingkan pengaturan mengenai ketentuan berbagi data di Indonesia dan Inggris yang aman dan mengkaji ketentuan yang dapat diadopsi dari hasil perbandingan tersebut. Penelitian ini menggunakan metode penelitian hukum yuridis-normatif dengan pendekatan perundang-undangan, yang menganalisis hukum dan hierarkinya, serta pendekatan komparatif, yang membandingkan regulasi di kedua negara. Hasil penelitian menunjukkan adanya perbedaan signifikan dalam pengaturan pelindungan

* Alamat korespondensi: pinky.eskah1403@mail.ugm.ac.id.

data pribadi, khususnya terkait perjanjian kerja sama yang menentukan hubungan hukum antara pengolah data dan ketentuan pengawasan dalam ekosistem *Open* API *Payment*. Perbedaan ini menunjukkan perlunya penguatan regulasi dan langkah penerapan perlindungan data pribadi di Indonesia. Pembelajaran dari Inggris, seperti perjanjian kerja sama yang lebih komprehensif dan pengawasan regulasi yang ketat, dapat menjadi acuan bagi peningkatan regulasi *Open* API *Payment* di Indonesia.
Kata Kunci: Pelindungan Data Pribadi, *Open* API *Payment*, Berbagi Data, Pembayaran Digital

A. PENDAHULUAN

Pertukaran data antara industri sistem pembayaran melalui teknologi API meningkatkan inklusivitas sistem pembayaran dengan melakukan *data sharing* antara beberapa industri sistem pembayaran, seperti pada *Open* API *Payment*.[1] Salah satu contoh penerapan *Open* API *Payment* adalah API *payment gateway* yang memungkinkan *e-commerce* memproses pembayaran *online* melalui bank digital pengguna tanpa bukti transfer manual.[2] Data perbankan kerap mencakup data sensitif konsumen yang apabila terjadi kebocoran data dapat menyebabkan kerugian materiil bagi konsumen dan industri, seperti kasus kebocoran data *Shopeepay* pada 2023 dan kasus Tokopedia pada 2020.[3]

Salah satu ancaman risiko yang timbul dari *Open* API *Payment* adalah kebocoran data pribadi konsumen akibat akses tidak sah dari layanan pihak ketiga sebagai Pemroses Data Pribadi Lainnya. Pemroses Data Pribadi Lainnya yang dimaksud adalah pihak yang diikutsertakan oleh Pengguna Layanan API untuk membantu pemrosesan data *(vendor service)* atau sebagai pihak penyimpan data (*clout service)*.[4] Potensi serangan siber akibat keterlibatan Pemroses Data Pribadi Lainnya meningkat karena tidak adanya jaminan bahwa Pemroses Data Pribadi Lainnya tersebut dapat memanfaatkan akses data sensitif yang diberikan sesuai prinsip pelindungan data pribadi.[5] Berdasarkan wawancara bersama Sakinah Rachmianty, Asisten Manajer Departemen Surveilans SP dan Pelindungan Konsumen di Bank Indonesia, kesadaran industri akan pentingnya kepatuhan terhadap pengaturan pelindungan data pribadi masih

---

1 Oliver Wyman, *The Appropriate Use of Customer Data in Financial Services* (Switzerland: World Economic Forum, 2018) 7.

2 Laura Brodsky dan Liz Oakes, "Data Sharing and Open Banking", *McKinsey&Company*, (March, 2017) 2.

3 Muhammad Ibrahim, "Waduh! Akun Shopee Dibobol Transaksi SPayLater Bocor Rp16,7 Juta", *Infobanknews,* 14 September 2023,https://infobanknews.com/waduh-akun-shopee-dibobol- transaksi-spaylater-bocor-rp167-juta/ lihat juga Wahyunanda Kusuma Pertiwi dan Oik Yusuf, "Data Tokopedia, Gojek, dan Bukalapak Bocor di Tengah Absennya RUU PDP", *KOMPAS.com,* 4 Mei 2020, https://tekno.kompas.com/read/2020/05/04/20170027/data-tokopedia-gojek-dan-bukalapak-bocor-di-tengah-absennya-ruu-pdp (diakses 13 Oktober 2024)

4 Ivan Stechynskyi, "The Importance of Therd-Party Vendor Risk Management for the Banking Industry", *Syteca,* 2020, https://www.syteca.com/en/blog/banks-independent-contractors-trust- verify (diakses 6 Maret 2025).

5 *Ibid.*

rendah, terutama bagi pihak non-Penyedia Jasa Pembayaran ("non-PJP") yang masih minim penerapan terhadap manajemen risiko kebocoran data.[6] Permasalahan terkait kebocoran data dalam *Open* API *Payment* memposisikan kerangka kebijakan pelindungan data pribadi, penerapan program kepatuhan hukum, dan pengawasan yang ketat terhadap pemrosesan data menjadi isu penting.

Per-Oktober 2024, Indonesia telah memberlakukan UU PDP yang banyak mengandung prinsip-prinsip pelindungan data pribadi dengan menekankan pentingnya penegakan hak-hak subjek data dan kepatuhan industri terhadap peraturan terkait pelindungan data pribadi. Lebih lanjut, Bank Indonesia, sebagai badan regulator sistem pembayaran, telah menetapkan Peraturan Anggota Dewan Gubernur No. 23/15/PADG/2021 tentang Standar Nasional *Open Application Programming Interface* Pembayaran ("SNAP") yang mengatur standar mekanisme minimum pelindungan data pribadi di ekosistem *Open* API *Payment*.[7] Akan tetapi, kedua pengaturan tersebut masih memiliki kekosongan hukum, khususnya terkait pengaturan layanan pihak ketiga sebagai pengelola data.[8]

Di berbagai wilayah yurisdiksi, pendekatan manajemen risiko teknologi *Open* API *Payment* terkait regulasi dan privasi data menerapkan pendekatan yang berbeda-beda.[9] Terdapat beberapa negara yang menyusun kerangka hukum yang baru dan standar protokol untuk mendukung pembagian data yang mengikat seluruh pihak dalam proses pembagian data atau disebut dengan *regulatory-driven approach*.[10] Bagi negara- negara yang menerapkan *regulatory-driven approach,* seperti Indonesia dan Inggris[11], implementasi teknologi *Open* API *Payment* yang maksimal bergantung pada efektivitas rancanang regulasi serta mekanisme kelembagaan yang berfungsi untuk menerapkan dan menegakkan regulasi tersebut.[12]

Berdasarkan penelitian sebelumnya, perkembangan sistem *Open Banking* di Inggris merupakan sistem yang paling berkembang dan menjadi pionir standar *Open Banking* di

---

6 Berdasarkan wawancara dengan Sakinah Rachmianty, selaku Asisten Manajer Departemen Surveilans SP dan Pelindungan Konsumen pada tanggal 20 Januari 2025.

7 Bank Indonesia, "Bank Indonesia Launches National Open API Payment Standard and Sandbox Trials of QRIS and Thai QR Payment Interconnectivity." August 19, 2021. https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/sp_2321121.aspx.(Diakses 12 Oktober 2024)

8 Berdasarkan wawancara dengan Bapak Santun Gunadi, selaku *Data Protection Consultant* di PT Xynexis Internasional pada tanggal 24 Januari 2025

9 Laura Brodsky dan Liz Oakes, *Ibid*, hlm. 1

10 Charles Marshall II Wilson, "Data Sharing is Caring: Consumer Privacy and International Approaches to Open Banking" *George Washington International Law Review* 53 , No. 3, (February, 2020) 602

11 Andres Wolberg-Stok, *Open Banking Ecosystem and Infrastructure: Banking on Openness in Open Banking*, (England: Oxford University Press, 2022), 20-24.

12 Ron Babin dan Donna Smith, "Open Banking and Regulation: Please Advice the Government," *Journal of Information Technology Teaching Cases,* No. 2, (May, 2022):109

dunia.[13] Pasca-Brexit, Inggris telah mengadopsi ketentuan *The Revised Payment Service Directive* ("PSD2") dengan penyesuaian pada standardisasi API dan pengawasan melalui *Open Banking Implementation Entity* ("OBIE"), sementara *Financial Conduct Authority* ("FCA") bertanggung jawab mengatur hak akses dan privasi data konsumen serta pedoman pengelolaan data *Open Banking*[14]. Untuk melindungi kerahasiaan, integritas, menjaga data pelanggan, serta memenuhi kewajiban regulasi termasuk UK GDPR, industri diharuskan memberikan perhatian dan fokus yang memadai pada keamanan. Kasus kebocoran data Revolut[15] akibat adanya akses tidak sah pada tahun 2022, dapat dijadikan gambaran komitmen *Information Commissioner's Officer* ("ICO") sebagai badan pengawas pelindungan data pribadi Inggris dalam menginvestigasi dan memberikan sanksi kepada Revolut yang gagal melindungi kerahasiaan dan kepatuhan terhadap UK GDPR[16].

Pengembangan teknologi *Open* API *Payment* di Indonesia masih terbilang pada tahapan awal dengan belum rampunya pengaturan dan program kepatuhan terhadap pelindungan data pribadi. Semantara itu, Inggris yang terlebih dahulu mengembangkan teknologi *Open* API di sektor sistem pembayaran memiliki kerangka hukum dan program kepatuhan pelindungan data pribadi serta sistem pengawasan yang selalu disesuaikan dengan perkembangan dan ancaman teknologi yang lebih maju. Sehingga, Indonesia dan Inggris merupakan negara yang menarik untuk dibandingkan, terutama dalam hal pengaturan dan pengawasan terhadap layanan pihak ketiga, serta implementasi program kepatuhan hukum. Perlu dipahami sebelumnya, bahwa Indonesia dan Inggris memiliki sistem hukum yang berbeda, yakni Indonesia menganut sistem *civil law* sedangkan Inggris menganut sistem *common law*. Akan tetapi, dalam hal *Open* API *Payment*, kedua negara tersebut memiliki pendekatan konsep yang sama terhadap pengembangan *Open* API *Payment,* yakni pendekatan *regulatory approach.* Berdasarkan hal tersebut maka Penulis mengkaji lebih lanjut mengenai perbandingan pengaturan dan program kepatuhan terkait dengan pelindungan data pribadi dalam pelaksanaan teknologi *Open* API

---

[13] EMEA Center of Regulatory Startegy, "Open Banking Around the World",https://www.deloitte.com/global/en/Industries/financial-services/perspectives/open- banking-around-the-world.html (diakses 12 Oktober 2024)

[14] Pada dasarnya istilah *Open Banking* dan *Open* API *Payment* memiliki pengartian yang serupa, yakni layanan perbankan terbuka yang membuka jalan pihak bank untuk membangun kerja sama dengan bank atau aplikasi pembayaran digital lainnya. Namun, istilah *Open Banking* lebih sering digunakan oleh Inggris sedangkan Indonesia lebih sering menggunakan istilah *Open* API *Payment.*

[15] Revolut merupakan aplikasi sistem pembayaran digital terbesar di Inggris yang juga menyediakan layanan *Open* API *Payment.*

[16] Pasca terpisahnya dengan Uni Eropa, Inggris telah meratifikasi *General Data Protection Regulation* menjadi *Regulation* (EU) 2016/679) *of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (UK GDPR)

Payment pada sistem pembayaran ritel, khususnya pada manajemen risiko dari keterlibatan Pemroses Data Pribadi Lainnya di dalam hukum Indonesia dengan Inggris, serta pelajaran terpetik (*lesson learned)* yang dapat diambil dari hasil analisis perbandingan.

B. PEMBAHASAN

1. Perbandingan Pengaturan Pelindungan Data Pribadi Terkait Aspek Kontraktual dan Aspek Pengawasan pada Pelibatan Pemroses Data Pribadi Lainnya dalam Pelaksanaan *Open* API *Payment*

a. *Aspek Kontraktual pada Pelibatan Pemroses Data Pribadi Lainnya dalam Pelaksanaan Open API Payment*

Keberadaan Pemroses Data Pribadi Lainnya, pada dasarnya telah tercantum dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi ("UU PDP") di Indonesia dan UK GDPR di Inggris. Kedua peraturan tersebut mengatur bahwa mengikutsertaan Pemroses Data Pribadi Lainnya merupakan kewenangan Pengguna Data selama adanya persetujuan tertulis dalam bentuk kontraktual dari Pengkontrol atau Penyedia Data terlebih dahulu.[17] Kontraktual yang mengatur mekanisme keikutsertaan Pemroses Data Pribadi Lainnya menjadi penting untuk memastikan adanya penilaian uji tuntas (*due diligence)* dan pengawasan lebih lanjut terhadap Pemroses Data Pribadi Lainnya.[18] Meskipun pemprosesan data dilakukan berdasarkan persetujuan dari Subjek Data, namun hal tersebut tidak dapat menjadi satu-satunya dasar pemberian data kepada pihak Pemroses Data Pribadi Lainnya atau pihak ketiga sebagaimana kontraktual tertulis tersebut bertujuan untuk memitigasi risiko kebocoran data akibat akses tidak sah pihak ketiga.[19]

Meskipun UU PDP telah menjelaskan pada Pasal 51 ayat (4) dan (5) terkait mekanisme partisipasi Pemroses Data Pribadi Lainnya dalam pemrosesan data, PADG SNAP ataupun pedoman tata kelolanya belum mengakomodir ketentuan keikutsertaan Pemroses Data Pribadi Lainnya. Sebagaimana dalam standar kontraktual yang dirumuskan Bank Indonesia hanya mengatur peran dan mekanisme antara Penyedia Data dengan Pengguna Data dan tidak ada pengaturan klausul lebih lanjut terkait keterlibatan Pemroses Data Pribadi Lainnya. Hal ini

[17] Lihat Pasal 51 ayat (4) dan *Article* 28 (2) UK GDPR
[18] Camila Amalia, et al. "Legal Issues of Personal Data Protection and Consumer Protection in Open API Payments" *Journal of Central Banking Law and Institution* 1, No. 2, (Mei 2022) 339.
[19] *Ibid.*

berpotensi menimbulkan situasi tidak adanya kontraktual SNAP yang mengatur hubungan hukum antara Penyedia Data, Pengguna Data, dan Pemroses Data Pribadi Lainnya sebagai pihak ketiga sehingga sulit untuk memastikan standar yang diterapkan oleh Pemroses Data Pribadi Lainnya telah sesuai standar minimum SNAP dan pengawasan lebih lanjut terhadap aktivitas Pemroses Data Pribadi Lainnya.[20] Kekosongan pengaturan dalam standar kontraktual SNAP disebabkan oleh pengaturan SNAP yang belum disesuaikan dengan pengaturan UU PDP secara menyeluruh. Ditambah lagi dengan belum diberlakukannya Rancangan Peraturan Pemerintah tentang Peraturan Pelaksanaan UU PDP ("RPP PDP"), yang juga telah mengatur standar teknis pendelegasian tugas kepada Pemroses Data Pribadi Lainnya, atau disebut juga dengan Prosesor Data Lainnya dalam RPP PDP, menyebabkan pemahaman industri akan kepatuhan terhadap UU PDP masih rendah.[21]

Di sisi lain, Inggris telah mengatur lebih jelas mengenai hal tersebut dengan menstandarkan *data sharing agreement* untuk pelibatan Pemroses Data Pribadi Lainnya. Standar kontrak yang mengacu pada *Article* 28 (3) UK GDPR, mengatur klausul bentuk persetujuan *controller* terhadap keterlibatan Pemroses Data Pribadi Lainnya. Dalam klausul tersebut diatur bahwa bentuk persetujuan yang akan diberikan dapat berbentuk persetujuan secara khusus (*specific authorisation)* ataupun persetujuan secara umum (*general aurhotisation)*.[22] Penentuan jenis persetujuan tersebut akan berpengaruh pada tenggat waktu yang diberikan kepada Pengkontrol atau Penyedia Data *(controller)* untuk memberikan persetujuannya.[23] Dalam hal *controller* menyatakan pemberian persetujuan kepada Pemroses Data Pribadi Lainnya secara umum, meskipun *controller* tidak memberikan penjelasan apapun hingga tenggat waktu, maka *controller* akan dianggap telah memberikan persetujuan atas pelibatan Pemroses Data Pribadi Lainnya. Dengan demikian, Pemroses Data Pribadi Lainnya juga terikat pada perjanjian kontrak yang

---

[20] *Ibid.*

[21] Berdasarkan wawancara dengan Santun Gunandi, selaku *Data Protection Consultant* di PT Xynesis International, pada tanggal 24 Januari 2025

[22] UK Information Commissioner's Office (ICO). "What Does it Mean If You Are a Processor?" https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and- processors/controllers-and-processors/what-does-it-mean-if-you-are-a-processor/#:~:text=Specific%20authorisation%20means%20the%20controller,of%20potential%20sub%2Dprocessors%3B%20or (Diakses 30 Januari 2025)

[23] *Ibid.*

mengharuskannya mematuhi pengaturan pelindungan data pribadi. Terlepas dari kriteria yang disarankan oleh *controller* untuk memilih Pemroses Data Pribadi Lainnya, Pengguna Data tetap bertanggung jawab penuh atas aktivitas pemrosesan data dan kepatuhan hukum Pemroses Data Pribadi Lainnya.[24] Oleh karena itu, Pengguna Data harus melaksanakan uji tuntas yang membuktikan bahwa Pemroses Data Pribadi Lainnya yang memberikan jaminan keamanan yang cukup.

b. Aspek Pengawasan pada Pelibatan Pemroses Data Pribadi Lainnya dalam Pelaksanaan Open API Payment

Pengawasan atau melakukan *audit* secara berkala merupakan aspek penting dalam memastikan aktivitas Pemroses Data Pribadi Lainnya dalam ekosistem *Open* API *Payment* dilakukan sesuai dengan standar minimum dan pengaturan yang berlaku. Pengaturan hukum terkait badan pengawasan untuk melakukan *audit* di lingkup internal dan eksternal untuk memastikan aktivitas pemrosesan data yang mengedepankan pelindungan data pribadi. Di lingkup internal organisasi, pengawasan *Open* API *Payment* dilakukan oleh pejabat perusahaan yang bertanggung jawab untuk memastikan pemenuhan kepatuhan atas prinsip pelindungan data pribadi dan mitigasi risiko pelanggaran pelindungan data pribadi tersebut sebagai *Data Protection Officer* ("DPO"). Dalam Pedoman Tata Kelola SNAP, sebagai bentuk pemenuhan standar mekansime menjaga kerahasiaan dan keamanan data, PJP Penyedia Layanan dan PJP Pengguna Layanan diperlukan untuk penunjukan DPO.[25] Akan tetapi, dalam mekanisme tersebut hanya mengatur sebatas peran dan tanggung jawab DPO dan tidak secara lengkap menjelaskan terkait pengaturan pada aspek structural dan kriteria DPO sebagaimana dijelaskan dalam UU PDP.

Inggris melalui DPA 2018[26] dan Indonesia melalui UU PDP[27] sama-sama telah mengadopsi pengaturan GDPR terkait DPO. pengaturan pelindungan data pribadi terkait penunjukan DPO antara Inggris dan Indonesia memiliki keserupaan pada aspek tugas DPO yang mencakup:

[24] *Article* 28 (4) UK GDPR
[25] Indonesian Payment System Assosiaion, *Op.cit.* hlm. 11
[26] Lihat *Part 3 Chapter* 4 *Article* 69 *Data Protection Act 2018*
[27] Pasal 53 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

(a) menginformasikan dan memberikan saran kepada Pengendali Data Pribadi atau Prosesor Data Pribadi agar mematuhi ketentuan dalam pengaturan pelindungan data pribadi;
(b) memantau dan memastikan kepatuhan terhadap UU PDP dan kebijakan Pengendali Data Pribadi dan memantau kinerja Pengendali Data Pribadi dan Prosesor data Pribadi;
(c) memberikan saran mengenai penilaian dampak pelindungan data pribadi dan memantau kinerja Pengendali Data Pribadi dan Prosesor Data Pribadi; dan
(d) berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan Data Pribadi.

Kedua pengaturan tersebut juga sama-sama mengatur bahwa penugasan DPO dapat ditunjukan kepada pihak eksternal secara kontraktual ataupun kepada badan pengurus yang telah ada di organisasi tersebut dengan memastikan tidak adanya *conflict of interest*.[28]Akan tetapi, pengaturan dalam UU PDP dapat terbilang belum rampung sebagaimana dalam Peraturan Pemerintah tersebut juga menyatakan bahwa ketentuan mengenai penunjukan, profesionalitas dan kompetensi DPO akan diatur lebih lanjut dalam Peraturan Lembaga PDP.[29]

Perbedaan signifikan lainnya antara kedua pengaturan tersebut antara lain terkait pengaturan karakteristik organisasi yang diwajibkan untuk melakukan penunjukan DPO. Dalam Pasal 54 ayat (1), pengaturan terkait karakteristik perusahaan yang diwajibkan untuk menunjuk DPO adalah:

(a) pemrosesan data pribadi untuk kepentingan pelayanan publik;
(b) kegiatan ini Pengendali Data Pribadi memiliki sifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas Data Pribadi dengan skala besar; dan
(c) kegiatan inti pengendali Data Pribadi terdiri dari pemrosesan Data Pribadi yang bersifat spesifik dan/atau Data Pribadi yang berkaitan dengan tindak pidana.

[28] UK Information Commissioner's Office (ICO). *Ibid.* Lihat juga Pasal 168 ayat (2) Rancangan Peraturan Pemerintah tentang Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
[29] Pasal 165 ayat (3) dan Pasal 166 ayat (3) Rancangan Peraturan Pemerintah tentang Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Karakteristik tersebut bersifat kumulatif dengan penggunaan frasa "dan".[30] Sehingga, karakteristik tersebut harus dipenuhi secara keseluruhan oleh perusahaan untuk diwajibkan penunjukan DPO. Hal tersebut menimbulkan celah hukum, sebab karakteristik tersebut tidak mencakup secara keseluruhan perusahaan perbankan ataupun Industri Keuangan Non-Bank yang melakukan pemrosesan data pribadi. Santun Gunandi, sebagai *Data Protection Consultant* di PT *Xynexis International,* berpendapat bahwa hal tersebut merupakan hal yang mendasar tetapi berakibat fatal dan saat ini sedang diajukan *judicial review* ke Mahkamah Konstitusi.[31]

Dari lingkup eksternal terdapat dua pihak lembaga. Pertama, lembaga yang bertugas untuk menetapkan standar *Open* API *Payment* dan verifikasi PJP Penyedia Layanan dan PJP ataupun non-PJP Pengguna Layanan. Di Indonesia, berdasarkan Pasal 8 ayat (2) UU P2SK, Bank Indonesia memiliki tugas untuk mengatur dan menjaga kelancaran sistem pembayaran. Melalui Surat Bank Indonesia Nomor 14/17/DASP tanggal 19 Oktober 2012, Asosiasi Sistem Pembayaran Indonsesia ("ASPI") merupakan SRO yang telah mendapatkan persetujuan Bank Indonesia dengan tujuan untuk meningkatkan peran pelaku sistem pembayaran di Indonesia dalam mewujudkan industri sistem pembayaran yang lebih efisien, aman, dan andal. Sedangkan Inggris sebagai pionir *Open Banking* telah membentuk sebuah entitas privat yang dibiayai dan diorganisir oleh CMA9 dengan sebutan *Open Banking Limited* (OBL) pada tahun 2017.[32] OBL memiliki kewajiban untuk menyediakan layanan *Open Banking* dengan struktur data dan standar keamanan yang tinggi agar nasabah dapat dengan aman dan mudah membagikan data keuangannya.[33] Baik ASPI dan OBL melaksanakan fungsinya sebagai perwakilan industri dengan merepresentasikan suara dari industri dan melindungi kepentingan anggota dalam dialog bersama regulator dan pembuat

[30] Lihat Bab III tentang Ragam Bahasa Peraturan Perundang-undangan angka 262 Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan

[31] Berdasarkan wawancara dengan Santun Gunadi, selaku *Data Protection Consultant* di PT Xynexis Internasional pada tanggal 24 Januari 2025

[32] Gov.UK, "Update on Open Banking", 1 Oktober 2021 https://www.gov.uk/government/news/update-on-open-banking (Diakses 30 Januari 2025)

[33] Open Banking Limited, "CMA Publishes Approved Roadmap for The Final Stages of Open Banking Implementation", 15 Mei 2020 https://www.openbanking.org.uk/news/cma-publishes- approved-roadmap-for-the-final-stages-of-open-banking-implementation/ (Diakses 30 Januari 2025)

kebijakan.[34] Sehingga, ASPI dan OBL berperan penting dalam mempromosikan teknologi *Open* API di sektor keuangan, khususnya pada sistem pembayaran, untuk mendukung inovasi sistem pembayaran digital dengan memperhatikan keamanan data konsumen.

Akan tetapi, peran OBL di Inggris menunjukkan bahwa fungsinya tidak akan berjalan secara efektif apabila tidak adanya harmonisasi antar otoritas sebagai pengawas dan regulator. Dalam menjalankan OBL, Inggris mengedepankan pendekatan *cross-functional* dengan beberapa lembaga pemerintah lainnya untuk meningkatkan efektifitas dan kestabilan implementasi *Open Banking* dalam sebuah entitas dengan sebutan *Joint Regulatory Oversight Committee* ("JROC"). JROC yang menguraikan pekerjaan lintas otoritas, seperti HM *Treasury,* CMA, FCA, Payment Service Regulator ("PSR") untuk bekerja sama untuk memberikan arahan dan menentukan operasional yang strategis untuk membangun ekosistem berkelanjutan dan kompetitif yang akan membuka potensi penuh *Open Banking* serta mengembangkan model *data sharing* yang terkendali secara independent.[35]

Kedua, lembaga otoritas independen yang memiliki tugas untuk mengawasi dan memastikan prinsip pelindungan data pribadi berdasarkan peraturan perundang-perundangan telah terpenuhi oleh industri. Keberadaan Lembaga PDP diharapkan dapat memastikan kepatuhan perusahaan kepada prinsip pemrosesan data pribadi dan menekankan hak-hak Subjek Data sebagaimana dijelaskan dalam UU PDP. Pasal 59 UU PDP menjelaskan bahwa tugas Lembaga PDP, yakni:

(a) perumusan dan penetapan kebijakan dan strategi PDP yang menjadi panduan bagi Subjek Data Pribadi, Pengendali Data Pribadi, dan Prosesor Data Pribadi;
(b) pengawasan terhadap penyelenggaraan PDP;
(c) penegakan hukum administratif terhadap pelanggaran UU PDP; dan
(d) fasilitasi penyelesaian sengketa di luar pengadilan.

[34] ASPI, "Peran dan Komitmen ASPI" https://www.aspi-indonesia.or.id/tentang-kami/peran-dan- komitmen-aspi/, lihat juga Open Banking Limited, "Events Archive" https://www.openbanking.org.uk/events/ (Diakses 30 Januari 2025)

[35] Gov.UK, "Policy Paper: Joint Statement by HM Treasury, the CMA, the FCA, and the PSR on the future of Open Banking", 25 Maret 2022 https://www.gov.uk/government/publications/joint- statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking/joint- statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking (Diakses 6 Maret 2025)

Sejak berlakunya UU PDP hingga saat ini, Lembaga PDP belum terbentuk. Saat ini, tugas menyelenggarakan perumusan dan pelaksanaan kebijakan di bidang pengawasan ruang digital dan pelindungan data pribadi saat ini berada pada Direktorat Jendral Pengawasan Ruang Digitial dibawah Kementrian Komunikasi dan Digital.[36] Santun Gunandi berpendapat bahwa meskipun pengaturan saat ini memberikan solusi sementara, hal ini menimbulkan pertanyaan tentang ketidakberpihakan dan efektivitas penegakan di bawah kerangka kementerian.[37] Nantinya, apabila Lembaga PDP sudah terbentuk, maka diperlukannya harmonisasi kembali terkait kewenangan Lembaga PDP dan Bank Indonesia terkait pengawasan pelindungan data pribadi di ekosistem API.

Jika berkaca pada Inggris, tugas pengawasan dalam implementasi pelindungan data pribadi berdasarkan UK GDPR dibebankan kepada ICO. ICO memiliki kewenangan untuk melakukan investigasi kepada perusahaan dalam memastikan kepatuhan pelindungan data pribadi melalui *data protection audits* secara berkala serta memberikan notifikasi kepada perusahaan apabila perusahaan tersebut diduga melanggar ketentuan pelindungan data pribadi yang terkait.[38] Selain itu, ICO juga memiliki wewenang untuk pencegahan ataupun pemulihan keadaan dari potensi adanya kebocoran data ataupun kegagalan kepatuhan terhadap regulasi, seperti memberi peringatan kepada Pengkontrol atau Penyedia Data ataupun Pengguna atau Pemroses Data apabila dalam upaya pemrosesan datanya terdapat potensi pelanggaran terhadap pengaturan dan memerintahkan Pengkontrol Data untuk mengkomunikasikan kebocoran data pribadi kepada Subjek Data. Dalam menjalankan tugas dan wewenangnya tersebut, ICO bertindak secara *independent* dan terbebas dari pengaruh eksternal baik langsung ataupun tidak langsung.[39]

2. Perbandingan Program Kepatuhan Pelindungan Data Pribadi Terkait Aspek Penunjukan DPO dan Aspek Penilaian Dampak Risiko dalam Pelaksanaan *Open* API *Payment*

a. Aspek Penunjukan DPO dalam Pelaksanaan Open API Payment

Dalam praktiknya, lembaga jasa perbankan ataupun non-perbankan sudah

[36] Pasal 21 Peraturan Presiden Nomor 174 Tahun 2024 tentang Kementrian Komunikasi dan Digital
[37] Berdasarkan wawancara dengan Santun Gunadi, selaku *Data Protection Consultant* di PT Xynexis Internasional pada tanggal 24 Januari 2025
[38] *Article* 58 (1) UK GDPR
[39] *Article* 58 (2) UK GDPR

banyak yang melakukan penunjukan DPO di struktur organisasinya masing-masing. Sakinah Rachmianty menyatakan bahwa sudah banyak lembaga jasa perbankan ataupun non-perbankan telah mengimplementasikan mandat UU PDP dan SNAP dengan penunjukan DPO, meskipun terdapat beberapa yang menunjuk DPO di dalam bagian *cybersecurity* dan bukan menjadi suatu badan organisasi baru.[111] Di lain sisi, Santun Gunadi, sebagai *Data Protection Consultant* di PT *Xynexis International,* menyatakan bahwa penempatan DPO diharuskan *independent* sebagaimana DPO akan mengawasi dan memastikan perusahaan menerapkan prinsip pelindungan data pribadi sesuai ketentuan yang berlaku, khususnya bagi perusahaan berskala besar.[40] Sebagai ilustrasi, DPO di suatu perusahaan dapat diposisikan sebagai divisi mandiri yang dibawah pengawasan langsung oleh direktur perusahaan untuk menilai risiko kebocoran data dan memberikan analisis pelindungan data pribadinya secara independent.

Implementasi penunjukan DPO di Inggris merupakan sebuah bentuk kepatuhan terhadap *Article* 37 UK GDPR. Terlepas dari karakteristik organisasi yang diwajibkan penunjukan DPO, ICO menekankan bahwa setiap organisasi diharuskan untuk memiliki tenaga kerja yang memadai untuk menjalankan fungsi DPO sebagaimana dijelaskan dalam UK GDPR.[41] Dalam menentukan apakah suatu organisasi diwajibkan untuk menunjuk DPO secara khusus, ICO telah memiliki panduan teknis untuk menilai aktivitas pemrosesan data organisasi tersebut.[42] Lebih lanjut, untuk memastikan fungsi DPO sebagai narahubung dengan otoritas terkait, UK GDPR menyatakan bahwa informasi terkait kontak detil DPO diharuskan dipublikasikan dan dilaporkan kepada ICO.[43] Hal tersebut tentunya bertujuan untuk mempermudah terjalinnya komunikasi ICO kepada organisasi dalam hal melakukan penilaian dampak pelindungan data pribadi dan investigasi saat adanya insiden kebocoran data.[44] Lebih lanjut, meskipun dalam peraturan UK GDPR ataupun UU PDP tidak

---

[40] Berdasarkan wawancara dengan Santun Gunadi, selaku *Data Protection Consultant* di PT Xynexis Internasional pada tanggal 24 Januari 2025

[41] UK's Information Commissioner's Office (ICO), "Data Protection Officer" https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/accountability-and-governance/data-protection-officers/#ib4, (Diakses 6 Maret 2025)

[42] UK's Information Commissioner's Office (ICO), "Data Protection Officer for Organisations" https://ico.org.uk/for-organisations/data-protection-fee/does-my-organisation-need-a-data- protection-officer-dpo/ (Diakses 3 Maret 2025)

[43] *Ibid.*

[44] *Ibid.*

mengatur secara eksplisit terkait sertifikasi DPO, sertifikasi DPO merupakan hal yang cukup patut dikonsiderasikan oleh perusahaan dalam melakukan penunjukan DPO yang profesional. Berdasarkan rekomendasi dari ICO, DPO sangat direkomendasikan untuk memiliki pelatihan dan sertifikasi terlebih dahulu untuk memahami tanggung jawab dan tugas dari fungsi DPO.[45]

Meskipun RUU PDP yang belum berlaku dan dalam pengaturnnya hanya memberikan sedikit klarifikasi mengenai opsi yang akan diadopsi untuk mendukung kualitas DPO, tim Tata Kelola PDP Asosiasi Pengusaha Teknologi Informasi dan Komunikasi ("APTIK") dan Kepala Badan Litbang Kementerian Komunikasi dan Digital telah menetapkan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan yang Berhubungan Dengan Itu (YBDI) Bidang Keahlian Pelindungan Data Pribadi ("SKKNI PDP") sesuai Keputusan Menteri Ketenagakerjaan Nomor 103 Tahun 2023. SKKNI PDP merupakan amanat UU PDP Pasal 53 ayat (2) yang mewajibkan pejabat DPO ditunjuk berdasarkan profesionalitas, pengetahuan mengenai hukum, praktrik PDP, dan kemampuan untuk memenuhi tugas-tugasnya. Dengan mengacu kepada Pasal 4 Peraturan Pemerintahan Nomor 31 Tahun 2006 tentang Sistem Pelatihan Kerja Nasional, maka seluruh pelatihan pejabat pelindungan data pribadi harus disusun berdasarkan SKKNI PDP tersebut. Lebih lanjut, Pasal 14 PP SPKN juga mensyaratkan bahwa sertifikasi dilaksanakan oleh lembaga terpisah yang telah terakreditasi oleh Badan Standardisasi Nasional ("BSN") atau Komite Akreditas Nasional ("KAN"), seperti Asosiasi Profesional Privasi Data Indonesia ataupun asosiasi sertifikasi lainnya.

Akan tetapi, sertifikasi DPO juga diperlukan strategi untuk menghindari hambatan dan memaksimalkan pelindungan data pribadi di seluruh cakupan industri sistem pembayaran. Salah satu hambatannya antara lain adalah minimnya Sumber Daya Manusia di sebuah perusahaan. Selain minimnya kesadaran akan kepatuhan terhadap UU PDP, Sakinah Rachmianty menyatakan bahwa kendala terbesar dari kepatuhan terhadap penunjukan DPO, khususnya di industri non-PJP, adalah keterbatasannya Sumber Daya Manusia yang memadai

[45] UK's Information Commissioner's Office (ICO), "Specialised Training" https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/training-and-awareness/specialised-training/ (Diakses 6 Maret 2025)

untuk membentuk DPO yang independen dan tersertifikasi.[46] Oleh karena itu, pemerintah perlu melakukan pendefinisian skala badan usaha dan persyaratan mengenai penunjukan DPO, mengingat banyaknya badan usaha dengan skala mikro di ekosistem sistem pembayaran, agar program kepatuhan pelindungan data pribadi dapat terimplementasi dengan baik.[47]

b. Aspek Penilaian Dampak Risiko dalam Pelaksanaan *Open* API *Payment*

Dengan mengacu pada *Article* 25 UK GDPR, Inggris menerapkan konsep pendekatan berbasis risiko (*risk based approach)* sehingga pelindungan data pribadi diharuskan dilaksanakan *by design and by default*.[48] *Data protection by design* memiliki arti bahwa perusahaan dalam pemrosesan data diharuskan untuk mementingkan privasi dan pelindungan data di setiap tahap pengembangan sistem, pelayanan, produk, atau proses secara keseluruhan.[49] Sedangkan, *data protection by default* adalah kewajiban perusahaan untuk memastikan pemrosesan data hanya dilakukan sesuai kebutuhan untuk mencapai tujuan tertentu dengan menentukan spesifikasi data yang diperlukan dan memberitahukan kepada Subjek Data atas pemrosesan data tersebut.[50] Dalam memastikan perusahaan menerapkan pelindungan data *by design and by default*, Inggris memandatkan perusahaan untuk melakukan *Data Protection Impact Assessments* (DPIA).

Inggris, dibawah naungan ICO, mewajibkan penyusunan DPIA dalam beberapa skenario. Bagi perusahaan yang melakukan pemrosesan data dengan teknologi baru, maka DPIA dapat dirumuskan oleh pengembang produk dan diimplementasikan oleh perusahaan.[51] Hal terpenting adalah dimana perusahaan yang baru memiliki inisiasi pemrosesan data dalam suatu produk baru, maka DPIA harus dijadikan acuan dalam penyusunan rancangan produk tersebut.[52]

---

[46] Berdasarkan wawancara dengan Sakinah Rachminty, selaku Asisten Manajer Departemen Surveilans SP dan Pelindungan Konsumen, pada tanggal 20 Januari 2025.

[47] Dewa Ayu D. A. dan Sri Handayani N., *Tantangan Implementasi dan Penguatan Kerjasama Lintas Sektor Pelindungan Data Pribadi,* (Yogyakarta: Central For Digital Society, 2021) 5.

[48] *Article* 25 UK GDPR

[49] *Article* 25 (1) UK GDPR

[50] *Article* 25 (2) UK GDPR

[51] *Ibid.*

[52] *Article* 86 UK GDPR

ICO menekankan bahwa DPIA bukanlah suatu dokumen yang hanya disusun untuk kepentingan kepatuhan saja, akan tetapi DPIA merupakan penilaian yang akan terus berkembang sejalan dengan pengembangan produk perusahaan dan perluasan aktivitas pemrosesan data. Sehingga, DPIA harus dilakukan penilaian kembali dalam kurun waktu tertentu untuk menentukan potensi risiko yang relevan, seperti adanya kegagalan keamanan data yang baru, penggunaan teknologi baru, atau permasalahan publik lainnya yang timbul dari pemrosesan data.[53] Berdasarkan UK GDPR, perusahaan yang gagal untuk menyusun dan menerapkan DPIA dapat dikenakan sanksi sebesar 8.7 juta *poundsterling* (delapan koma tujuh juta poundsterling) atau 2% (dua persen) dari omzet tahunan global jika lebih tinggi.[54]

Sedangkan di Indonesia, kewajiban melakukan penilaian dampak risiko atau DPIA pada dasarnya telah diatur dalam Pasal 34 UU PDP yang kemudian dijabarkan lebih lanjut dalam RPP PDP. Akan tetapi, implementasi DPIA di Indonesia masih belum maksimal sebagaimana UU PDP masih terbilang baru sehingga kesadaran atas kewajiban dokumen penilaian tersebut di banyak perusahaan masih renah. Hal tersebut dinyatakan oleh Santun Gunandi bahwa dari enam perusahaan baru satu perusahaan di enam bulan terakhir yang sudah dalam masa transisi ke arah kepatuhan terhadap UU PDP, akan tetapi karena RPP PDP yang belum disahkan membuat banyak perusahaan tidak memprioritaskan penilaian tersebut.[55]

Adapun tujuan dari DPIA, selain sebagai bentuk pemenuhan kepatuhan terhadap *Article* 25 UK GDPR ataupun UU PDP, yaitu untuk menilai risiko apa saja dan mitigasi risiko yang diambil perusahaan dalam pemrosesan data sebelum aktivitas pemrosesan data dilakukan.[56] Dengan demikian, perusahaan dapat mengidentifikasi dan memperbaiki permasalahan di tahapan awal.[57] Hal tersebut tentunya akan meningkatkan kepercayaan konsumen yang dapat

---

53 UK Information Commissioner's Office (ICO), *Op.cit*

54 *Ibid.*

55 Berdasarkan wawancara dengan Bapak Santun Gunandi, selaku *Data Protection Consultant* di PT Xynexis Internasional pada tanggal 24 Januari 2025

56 UK Information Commissioner's Office (ICO). "What Is A DPIA?" https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection- impact-assessments-dpias/what-is-a-dpia/#what1 (Diakses 1 Februari 2025)

57 *Ibid.*

memberikan reputasi yang baik bagi perusahaan.[58] Dari segi finansial, identifikasi permasalahan lebih dahulu dan menentukan data apa saja yang digunakan akan menghemat biaya operasional pemrosesan data.[59] Sehingga, dengan menjadikan DPIA acuan dalam melakukan audit, hasil audit akan lebih efektif dan objektif.

3. Konsep yang Dapat Diadopsi dan Diintegrasikan dari Pengaturan Program Kepatuhan Pelindungan Data Pribadi di Inggris, Serta Manfaatnya dalam Mendukung Implementasi *Open* API *Payment* di Indonesia

Berdasarkan pemaparan dan perbandingan ketentuan pengaturan pelindungan data pribadi dan program kepatuhan yang terdapat di kedua belah negara, terdapat beberapa pelajaran terpenting yang dapat diadopsi dan diintegrasikan di kerangka hukum Indonesia untuk membenahi dan mengembangkan peraturan serta kebijakan pelindungan data pribadi di Indonesia dalam ekosistem *Open* API *Payment*, terutama dalam hal mencegah adanya akses tidak sah dari pihak ketiga yang berperan sebagai Pemroses Data Pribadi Lainnya. Khususnya, ada tiga aspek utama yang dapat dijadikan fokus utama untuk memperbaiki pengaturan dan meningkatkan penerapan program kepatuhan pelindungan data pribadi *Open* API *Payment* di Indonesia. Aspek tersebut antara lain mencakup aspek harmonisasi kewenangan antara otoritas, aspek penyesuaian standar *Open* API *Payment* kepada pengaturan pelindungan data pribadi, dan aspek penilaian dampak pelindungan data pribadi.

a. Konsep Harmonisasi Kewenangan antara Otoritas (cross-function)

Indonesia dapat membuat suatu kebijakan untuk mengharmonisasikan berbagai lembaga yang berwenang dalam meregulasi dan mengawasi implementasi *Open* API *Payment* di Indonesia seperti di Inggris yang melibatkan CMA, JROC, FCA, dan ICO dengan pendekatan *cross-function*. Inggris selalu menjaga keselarasan standar dengan persyaratan peraturan dan hukum, sehingga UK GDPR, DPA 2018, hingga PSR 2017 juga teradopsi pada pembuatan standar tersebut. Meskipun dalam pemrosesan data pribadi di ekosistem *Open Banking* terdapat pihak Pemroses Data Pribadi Lainnya yang tidak berada di bawah pengawasan OBL, Pemroses Data Pribadi Lainnya tersebut masih terikat kewajiban untuk mematuhi UK GDPR.

---

[58] *Ibid.*
[59] *Ibid.*

Sedangkan, fenomena yang terjadi di Indonesia dalam menangani kasus kebocoran data masih termasuk koridor pelindungan konsumen.[60] Terlebih lagi, saat ini Indonesia memiliki 30 peraturan sektoral terkait pelindungan data pribadi.[61] Peraturan yang tersebar ini menjadi hambatan dalam implementasi karena diperlukannya sinkronisasi dalam hal definisi dan tata elola antar sektor. Sehingga, dalam menyelesaikan permasalahan pelindungan data pribadi dalam ekosistem *Open* API *Payment* di Indonesia masih bersifat sektoral dan menyertakan berbagai macam otoritas lainnya.[62] Hal tersebut tentunya berdampak pada pengawasan Bank Indonesia karena keterbatasannya dalam pemberian sanksi kepada pihak seperti penyelenggara penunjang, karena terdapat kemungkinan penyelenggara penunjang tersebut berada di kewenangan otoritas lain.[63] Sehingga, Bank Indonesia, ASPI, Indonesia E-commerce Association (idea), dan Penyedia Jasa Sistem Pembayaran dapat bekerja sama untuk merumuskan peraturan yang memperjelas lingkup penyelesaian sengketa pada sistem pembayaran untuk mengatasi permasalahan data pribadi konsumen secara efektif.[64]

Perlu dipahami bahwa perbedaan yang cukup signifikan antara pengaturan di Inggris dan Indonesia adalah bagaimana Indonesia belum memiliki suatu lembaga PDP dan belum adanya kebijakan yang mengharmonisasi kewenangan antara otoritas. Selain banyaknya kepentingan dari kementerian atau lembaga pemerintah non kementrerian yang terkait, hambatan harmonisasi kewenangan terjadi dikarenakan tingginya *ego* sektoral dan adanya irisan kewenangan terkait tugas dan fungsi masing-masing.[65] Sakinah Rachmianty menerangkan bahwa dalam kehadiran beberapa forum antara otoritas terkait, otoritas yang mewakili forum tersebut sering bergantian perwakilan, sehingga pemahaman otoritas dan proses harmonisasi kewenangan masih terhambat.[66] Lembaga PDP yang nantinya akan disahkan tentunya diperlukan harmonisasi kembali terkait kewenangan

---

60 Camila Amalia, *et.al, Op.cit,* hlm. 350

61 Dewa Ayu D. A. dan Sri Handayani N., *Op.cit,* hlm. 1

62 *Ibid.*

63 Berdasarkan wawancara dengan Sakinah Rachminty, selaku Asisten Manajer Departemen Surveilans SP dan Pelindungan Konsumen, pada tanggal 20 Januari 2025.

64 Iwan Setiawan, "Risiko Theft, Fraud, dan Peningkatan Keamanan Sistem Pembayaran Melalui Penguatan Perlindungan Konsumen", Sesmabi 3 Bank Indonesia Institute Presentation, 10 Mei 2020.

65 Padma Widyantari dan Adi Sulistiyono, "Pelaksanaan Harmonisasi Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP)" *Jurnal Privat Law* VIII, No. 1 (April: 2020) 122

66 Berdasarkan wawancara dengan Sakinah Rachmianty, selaku Asisten Manajer di Departemen Surveilans SP dan Pelindungan Konsumen pada tanggal 20 Januari 2025

pengaturan terkait pelindungan data pribadi. Dengan demikian, implementasi program kepatuhan pelindungan data pribadi sesuai dengan ketentuan UU PDP dan RPP PDP dapat terlaksanakan dan diterapkan oleh seluruh industri secara maksimal.

b. Konsep Penyesuaian Standar Open API Payment dengan Pengaturan Pelindungan Data Pribadi

Indonesia dapat menyesuaikan standar kontrak kerjasama SNAP dengan peraturan perundang-undangan yang berlaku. Perlu dipahami pula bahwa kepatuhan terhadap pengelolaan SNAP tidak secara keseluruhan sudah meliputi kepatuhan kepada UU PDP. Sebagaimana pengaturan tentang pelibatan Pemroses Data Pribadi Lainnya belum diatur secara jelas standar kontraktual dan pembagian tanggung jawabnnya dalam PADG SNAP ataupun Pedoman Tata Kelola SNAP.[67] Ditambah lagi, implementasi yang dilakukan oleh non-PJP dalam hal manajemen risiko tidak sekuat dengan yang diterapkan oleh PJP atau bank karena tidak semua non-PJP memahami secara detil pengaturan, prosedur, pengkontrolan internal dan eksternal.[68] Sebagaimana dinyatakan oleh Sakinah Rachmianty bahwa *awareness* pada non-PJP masih sangat kurang dalam hal pemenuhan prinsip pelindungan data pribadi ataupun UU PDP yang baru diberlakukan.[69]

Kendati demikian, Bank Indonesia dapat mengadopsi konsep Inggris yang merumuskan standar kontraktual antara Penyedia Layanan API dengan Pengguna Layanan API serta Pemroses Data Pribadi Lainnya agar kepastian hukum Pemroses Data Pribadi Lainnya dapat lebih terjamin dan meningkatkan kepatuhan terhadap UU PDP. Indonesia dapat berkaca kepada Inggris yang mengutamakan kepatuhan terhadap UK GDPR dalam hal pemrosesan data di lingkup *Open Banking.* Apabila terdapat kebocoran data, OBL dapat mengajukan laporan kepada ICO dan pelaku industri yang terbukti lalai dapat dikenakan denda sebagai tindakan penegakan hukum akibat pelanggaran data. Berdasarkan UK GDPR, pelanggaran perlindungan data dapat dikenakan denda hingga 4% dari total pendapatan tahunan global atau 20 juta poundsterling, tergantung mana yang lebih besar.

c. Konsep Penilaian Dampak Pelindungan Data Pribadi

---

67 Camila Amalia, et.al, *Op.cit,* hlm. 341

68 *Ibid.*

69 Berdasarkan wawancara dengan Sakinah Rachminty, selaku Asisten Manajer Departemen Surveilans SP dan Pelindungan Konsumen, pada tanggal 20 Januari 2025.

Penilaian dampak pelindungan data pribadi berfungsi untuk menentukan risiko awal dan mengatasi risiko secara perventif dan solutif. Indonesia dapat mempersyaratkan DPIA sebagai salah satu syarat dokumen pengajuan persetujuan pengembangan aktivitas atau layanan produk *Open* API *Payment.* Setelah adanya *regulatory reform* yang dilakukan oleh Bank Indonesia sebagai upaya menyederhanakan regulasi terkait sistem pembayaran nasional, efektivitas pengaturan sistem pembayaran ditingkatkan melalui penerapan pendekatan pengaturan yang mengedepankan *principle-based regulation* dan optimalisasi peran SRO.[70] Optimalisasi peran SRO digambarkan dengan adanya ASPI sebagai SRO yang memberikan surat rekomendasi kepada PJP yang ingin mengembangkan teknologi *Open* API setelah dilakukannya verifikasi berdasarkan Pedoman Tata Kelola SNAP.

Lebih lanjut, PJP yang ingin mengembangkan aktivitas dan/atau kerja sama dengan pihak lain diharuskan memberikan perizinan, persetujuan, ataupun pelaporan yang persyaratannya terklasifikasi berdasarkan kategori risiko (*risk based)*.[71] Kategori risiko bagi PJP yang ingin mengimplementasikan *Open* API terkategori sebagai risiko medium dan harus memenuhi berbagai aspek dalam persyaratan dokumen. Dokumen yang dibutuhkan PJP dalam pemenuhan syarat apabila ingin mengajukan pemanfaatan teknologi *Open* API berbasis SNAP, khususnya pada aspek pelindungan konsumen, yakni:

(a) Dokumen yang menunjukkan transparansi aktivitas atau produk yang dikembankan kepada penggunanya. Paling kurang mencakup bukti bahwa PJP/PIP telah menyediakan informasi yang lengkap mengenai aktivitas/produk yang diselenggarakan kepada penggunanya. Informasi paling kurang mencakup jenis layanan yang disediakan, biaya, mekanisme penyelesaian gangguan, manfaat dan risiko;

(b) Dokumen yang menunjukkan kewajiban PJP/PIP untuk menjaga keamanan dan kerahasiaan data nasabahnya;

(c) Hasil penilaian PJP/PIP mengenai dampak pengembangan aktivitas dan/atau pengembangan produk terhadap perubahan kebijakan dan prosedur operasional dalam rangka pelindungan konsumen, serta

[70] Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran

[71] Pasal 79 Peraturan Bank Indonesia Nomor 23/6/PBI/2021tentang Penyedia Jasa Pembayaran

perubahan prosedur dan mekanisme penanganan dan penyelesaian pengaduan konsumen; dan

(d) Hasil penyesuaian prosedur dan mekanisme berdasarkan hasil penilaian sebagaimana dimaksud dalam poin sebelumnya.

Kategori risiko dalam pengajuan penambahan layanan API diperbolehkan untuk mengajukan persetujuan dengan kategori risiko rendah dan hanya diwajibkan untuk mengajukan pelaporan kepada Bank Indonesia setelah adanya surat rekomendasi dari ASPI.[72]

Serangkaian persyaratan dokumen tersebut telah memastikan adanya mekanisme minimum yang dipenuhi oleh perusahaan secara internal dalam mengatasi pelindungan konsumen. Sebagaimana dijelaskan sebelumnya, Pedoman Tata Kelola SNAP juga mensyaratkan mekanisme pengelolaan API terproses di perusahaannya sesuai dengan prinsip pelindungan konsumen. Akan tetapi, dengan hadirnya UU PDP maka ada pergeseran fokus dengan manajemen risiko di perusahaan menjadi manajemen risiko untuk pemenuhan hak-hak Subjek Data Pribadi. Dengan demikian, ASPI sebagai SRO yang melakukan verifikasi Penyedia Layanan API, dapat mewajibkan perusahaan untuk melakukan DPIA yang sesuai dengan UU PDP untuk menilai *maturity* dari perusahaan tersebut dalam pemenuhan hak Subjek Data Pribadi.

Bank Indonesia dan ASPI diharuskan melakukan *regulatory reform* lebih terkini terkait pelindungan data pribadi yang sesuai dengan UU PDP. Hal ini tentunya akan membantu para perusahaan untuk patuh kepada peraturan perundang-undangan yang berlaku serta mewujudkan sistem pembayaran dengan teknologi *Open* API yang aman bagi masyarakat. Sebagai ilustrasi, Bank A yang hendak bekerja sama dengan *fintech* B diharuskan melakukan DPIA terlebih dahulu untuk menentukan risiko apa saja yang berpotensi timbul dari penggunaan teknologi API dengan menjadikan UU PDP standar minimum pelindungan data pribadi, termasuk apabila adanya keterlibatan Pemroses Data Pribadi Lainnya.

Kerangka pelindungan data yang kuat tidak hanya akan memungkinkan

---

[72] Pasal 10 Peraturan Anggota Dewan Gubernur Nomor 23/15/PADG/2021 tentang Implementasi Standar Nasional *Open Application Programming Interface* Pembayaran

adanya mekanisme untuk melawan akses tidak sah dan pelaku kejahatan siber lainnya, tetapi juga memasang sistem pertanggungjawaban hukum bagi para industri untuk memastikan bahwa mereka mengambil tindakan-tindakan yang tepat, yakni mengidentifikasi apakah industri bertangungjawab atas suatu kebocoran data atau menerapkan langkah-langkah preventif untuk mencegah pelanggaran serupa terjadi di masa mendatang.[73] Konsep atau langkah-langkah tersebut yang nantinya akan diadopsi di pengaturan pelindungan dan program kepatuhan pelindungan data pribadi di Indonesia, keefektivitasnya tentunya akan bergantung pada bagaimana tingkat *awareness* industri atas pentingnya kepatuhan terhadap pengaturan pelindungan data pribadi. Kepatuhan terhadap UU PDP tidak hanya kewajiban hukum, tetapi juga strategi etis dan bisnis yang penting untuk menjaga kepercayaan dan kepuasan pelanggan.

Peningkatan *awareness* industri atas pentingnya kepatuhan terhadap pengaturan pelindungan data pribadi dapat dilakukan dengan menyediakan forum *policy dialogue* secara berkala antara industri dengan Bank Indonesia dan juga ASPI untuk menyesuaikan dengan kesiapan industri terhadap pelindungan data pribadi di ekosistem *Open* API *Payment* yang dinamis dan terus berkembang. Lebih lanjut, peningkatan *awareness* industri dapat dilakukan dengan melaksanakan program-program pelatihan profesi privasi dan sertifikasi DPO dengan para pelaku industri sistem pembayaran *Open* API *Payment*.

C. PENUTUP

Perbandingan regulasi pelindungan data pribadi antara Indonesia dan Inggris menunjukkan bahwa Indonesia masih menghadapi tantangan dalam harmonisasi regulasi, kelembagaan pengawasan, dan implementasi program kepatuhan dalam ekosistem *Open* API *Payment*. Inggris memiliki standar yang lebih komprehensif dalam pendelegasian Pemroses Data Pribadi Lainnya, pengawasan kelembagaan dengan pendekatan *cross-function*, serta kewajiban DPIA untuk menilai risiko kebocoran data, sementara Indonesia masih mengalami ketidaksinkronan regulasi dan belum mengatur kewajiban tersebut pada pengaturan yang lebih khusus, seperti Peraturan Bank Indonesia. Untuk memperkuat

[73] Ajisatria Suleiman, *et.al, Makalah Kebijakan No. 50 Pengaturan Bersama dalam Pelindungan Data Pribadi: Potensi peran Asosiasi Industri sebagai Organisasi Regulator Mandiri* (Jakarta: Center for Indonesian Policy Studies, 2022) 13

perlindungan data pribadi, Indonesia dapat mengadopsi pendekatan *cross-function* dalam pengawasan, menerapkan konsep *data protection by design and by default* dengan mewajibkan DPIA dalam pengembangan teknologi *Open* API, serta menyelaraskan standar SNAP dengan regulasi perlindungan data pribadi guna memastikan kepatuhan industri terhadap prinsip perlindungan data yang lebih ketat.

D. DAFTAR PUSTAKA

Andres Wolberg-Stok. *Open Banking Ecosystem and Infrastructure: Banking on Openness in Open Banking.* England: Oxford University Press, 2022.

Ayu, D. A., Dewa, dan Sri Handayani N. *Tantangan Implementasi dan Penguatan Kerjasama Lintas Sektor Pelindungan Data Pribadi.* Yogyakarta: Central For Digital Society, 2021.

Bank Indonesia. *Blueprint Sistem Pembayaran Indonesia 2025 BI: Menavigasi, Sistem Pembayaran Nasional di Era Digital.* Jakarta: Bank Indonesia, 2019.

Basel Committee on Banking Supervision. *Report on Open Banking and Application Programming Interfaces.* England: Bank for International Settlement, 2019.

Indonesian Payment System Association (ASPI). *SNAP – Standar National Open API Pembayaran (Pedoman Tata Kelola).* Ver. 1.0, 2021.

Wyman, Oliver. *The Appropriate Use of Customer Data in Financial Services.* Switzerland: World Economic Forum, 2018.

Amalia, Camila, et al. "Legal Issues of Personal Data Protection and Consumer Protection in Open API Payments." *Journal of Central Banking Law and Institution* 1, no. 2 (Mei 2022): 339.

Babin, Ron, dan Donna Smith. "Open Banking and Regulation: Please Advice the Government." *Journal of Information Technology Teaching Cases* no. 2 (Mei 2022): 109.

Sugarda, Paripurna P., dan Muhammad Rifky Wicaksono. "Enhancing the Competitiveness of Indonesia's Financial Service Sector in the Digital Era Through Open Banking: Lessons Learned From the UK's Experienced." *Journal of Central Banking Law and Institution* no. 1 (Januari 2023): 156.

Widyantari, Padma, dan Adi Sulistiyono. "Pelaksanaan Harmonisasi Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP)." *Jurnal Privat Law* VIII, no. 1 (April 2020): 122.

ASPI. "Peran dan Komitmen ASPI." Diakses 30 Januari 2025. https://www.aspi-indonesia.or.id/tentang-kami/peran-dan-komitmen-aspi/.

Bank Indonesia. "Bank Indonesia Launches National Open API Payment Standard and Sandbox Trials of QRIS and Thai QR Payment Interconnectivity." 19 Agustus 2021. Diakses 12 Oktober 2024. https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/sp_2321121.aspx.

Brodsky, Laura, dan Liz Oakes. "Data Sharing and Open Banking." *McKinsey & Company*, Maret 2017. https://www.mckinsey.com.

EMEA Center of Regulatory Strategy. "Open Banking Around the World." Diakses 12 Oktober 2024. https://www.deloitte.com/global/en/Industries/financial-services/perspectives/open-banking-around-the-world.html.

Gov.UK. "Policy Paper: Joint Statement by HM Treasury, the CMA, the FCA, and the PSR on the Future of Open Banking." 25 Maret 2022. Diakses 6 Maret 2025. https://www.gov.uk/government/publications/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking.

———. "Update on Open Banking." 1 Oktober 2021. Diakses 30 Januari 2025. https://www.gov.uk/government/news/update-on-open-banking.

Ibrahim, Muhammad. "Waduh! Akun Shopee Dibobol Transaksi SPayLater Bocor Rp16,7 Juta." *Infobanknews*, 14 September 2023. Diakses 30 Januari 2025. https://infobanknews.com/waduh-akun-shopee-dibobol-transaksi-spaylater-bocor-rp167-juta/.

Makarin, Edmon. "Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi." *Hukumonline.com*, 9 Juli 2020. Diakses 6 Maret 2025. https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef/.

Open Banking Limited. "CMA Publishes Approved Roadmap for The Final Stages of Open Banking Implementation." 15 Mei 2020. Diakses 30 Januari 2025. https://www.openbanking.org.uk/news/cma-publishes-approved-roadmap-for-the-final-stages-of-open-banking-implementation/.

Pertiwi, Wahyunanda Kusuma, dan Oik Yusuf. "Data Tokopedia, Gojek, dan Bukalapak Bocor di Tengah Absennya RUU PDP." *KOMPAS.com*, 4 Mei 2020. Diakses 13 Oktober 2024. https://tekno.kompas.com/read/2020/05/04/20170027/data-tokopedia-gojek-dan-bukalapak-bocor-di-tengah-absennya-ruu-pdp.

Setiawan, Iwan. "Risiko Theft, Fraud, dan Peningkatan Keamanan Sistem Pembayaran Melalui Penguatan Perlindungan Konsumen." *Sesmabi 3 Bank Indonesia Institute Presentation*, 10 Mei 2020.

Stechynskyi, Ivan. "The Importance of Therd-Party Vendor Risk Management for the Banking Industry." *Syteca*, 2020. Diakses 6 Maret 2025. https://www.syteca.com/en/blog/banks-independent-contractors-trust-verify.

UK Information Commissioner's Office (ICO). "Data Protection Officer." Diakses 3 Maret 2025. https://ico.org.uk/for-organisations/law-enforcement/guide-to-le.

———. "Data Protection Officer for Organisations." Diakses 3 Maret 2025. https://ico.org.uk/for-organisations/data-protection-fee/does-my-organisation-need-a-data-protection-officer-dpo/.

Wawancara dengan Sakinah Rachmianty, Asisten Manajer Departemen Surveilans SP dan Pelindungan Konsumen, 20 Januari 2025.

Wawancara dengan Santun Gunadi, Data Protection Consultant di PT Xynexis Internasional, 24 Januari 2025.