Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.4527

Perbandingan Mekanisme Penyelesaian Kasus Pencurian Data Pribadi Dalam Perspektif Undang–Undang No. 27 Tahun 2022 dan *General Data Protection Regulations*

Shanaya Azzahra Ariputri[1], Mohammad Wendy Trijaya[2], Elly Nurlaili[3], Dianne Eka Rusmawati[4], Dora Mustika[5]
Program Studi Ilmu Hukum, Universitas Lampung, Indoneisa[1-5]
Email Korespondensi: Shanayaazzahra@gmail.com[1], mwtrijaya@gmail.com[2], elly.nurlaili74@gmail.com[3], dianne_eka_rusmawati@fh.unila.ac.id[4], dora.mustika@fh.unila.ac.id[5]

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Februari 2026, Article published: 01 Maret 2026

ABSTRACT
The development of digital technology has made personal data an inseparable part of human life. However, the increasing volume of data processing has also been accompanied by a growing risk of misuse and theft of personal data, including in the banking sector. Indonesia has responded to the urgency of personal data theft incidents through the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which adopts the principles of the European Union's General Data Protection Regulation (GDPR). The main issues examined in this study concern how the mechanism for resolving personal data theft cases in Indonesia compares to that in Europe, as well as how the resolution of such cases in Indonesia can be evaluated from the perspective of the GDPR. This research employs a normative legal research method with a descriptive research type. The problem is approached through a comparative analysis of statutory regulations and a case study approach. The data used in this study consist of secondary data, which were collected through literature review and document study. The data were processed through stages of identification, examination, reconstruction, and systematic arrangement, and were analyzed qualitatively. The results of this study indicate that the resolution of personal data theft cases in Indonesia, particularly in the banking sector, has not yet been conducted in a manner that is as transparent and stringent as the resolution of similar cases in European banking institutions. Although the PDP Law has provided legal protection for Data Subjects by adopting the principles and foundations of the GDPR, its implementation still faces significant obstacles due to the absence of an independent supervisory authority with the competence to ensure effective protection and legal enforcement.
Keywords: *Data, GDPR, Law Number 27 Year 2022, Legal Protection, Personal Data Protection, Personal Data Breach, Banking.*

ABSTRAK
Perkembangan teknologi digital telah menjadikan data pribadi sebagai bagian yang tidak terpisahkan dari kehidupan manusia. Namun, meningkatnya pemrosesan data juga diiringi dengan meningkatnya risiko penyalahgunaan dan pencurian data pribadi, termasuk dalam sektor perbankan. Indonesia telah merespons urgensi insiden pencurian data pribadi melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang mengadopsi prinsip-prinsip dari ketentuan General Data Protection Regulation (GDPR) Uni Eropa. Permasalahan utama dalam penelitian ini dirumuskan pada bagaimana

mekanisme penyelesaian kasus pencurian data pribadi di Indonesia dibandingkan dengan di Eropa serta bagaimana penyelesaian kasus di Indonesia jika ditinjau dari perspektif hukum GDPR. Jenis penelitian ini menggunakan metode penelitian hukum normatif dengan tipe penelitian deskriptif. Dengan pendekatan masalah melalui pendekatan komparasi peraturan perundang – undangan dan studi kasus. Data yang digunakan adalah data sekunder. Metode pengumpulan data dilakukan dengan studi kepustakaan dan studi dokumen. Metode pengolahan data melalui identifikasi, pemeriksaan, rekonstruksi dan sistematika data yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa kasus pencurian Data Pribadi di Indonesia dalam sektor perbankan masih belum sepenuhnya memiliki penyelesaian yang transparan dan tegas seperti apa yang terjadi pada kasus pencurian data pada bank di Eropa. Meskipun UU PDP telah memberikan perlindungan hukum bagi Subjek Data dengan menganut asas dan prinsip pada GDPR, pada penerapannya masih terdapat kendala lantaran ketiadaan Lembaga Pengawas yang berwenang untuk memberikan perlindungan dan ketegasan hukum.
Kata Kunci: *Data, GDPR, Undang – Undang No. 27 Tahun 2022, Perlindungan Hukum, Perlindungan Data Pribadi, Pencurian Data Pribadi, Perbankan.*

PENDAHULUAN

Era digitalisasi menjadikan seluruh aspek di kehidupan kita bergantung pada kemajuan teknologi modern yang memerlukan Data Pribadi penggunanya. Seiring dengan meningkatnya tingkat kompleksitas pengolahan data, risiko penyalahgunaan dan pelanggaran Data Pribadi juga semakin meningkat. Data Pribadi dapat dengan mudahnya terpapar dan bocor tanpa kontrol dari pemilik data, atas aliran data (*data flow*) yang melibatkan lebih dari satu yurisdiksi menjadi perhatian pemerintah terutama dalam konsep keamanan nasional. Tercatat sebanyak 3.331 kasus kejahatan siber yang didasari bocornya data pribadi dalam catatan Kepolisian Republik Indonesia per Tahun 2024. Salah satu kasus yang menjadi fokus utama dalam penulisan kali ini yakni yang terjadi pada PT. Bank Syariah Indonesia yang mengalami pencurian data *ransomware* sebesar 1,5 *TeraByte* data pribadi nasabah per Tahun 2023. Urgensi inilah yang mendesak Undang – Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP) sebagai landasan dan kepastian hukum masyarakat Indonesia dengan mengadopsi regulasi Eropa yakni *General Data Protection Regulations* (GDPR).

fokus utama dalam pembentukan peraturan ini ialah bukan sekedar perihal ganti rugi, namun sebagai kepastian setelah terjadinya pencurian tentang apakah dan bagaimanakah data yang telah hilang atau bocor dapat diantisipasi.

Di sisi lain, GDPR telah menjadi '*golden standard*' atau standar emas dalam perancangan pembuatan UU PDP yang berangkat dari kepentingan hak asasi manusia yang merupakan peraturan perlindungan data pribadi yang mengikat bagi seluruh wilayah Eropa dan menjadi regulasi pedoman bagi Negara lain telah mengatur terkait prinsip, pertanggungjawaban, serta penyelesaian jika terjadi insiden serupa. Seperti yang terjadi pada bank UniCredit di Italia atas kelalaian keamanan pada bank sehingga dapat dengan mudah diretas dan berdampak pada ribuan hingga jutaan data nasabah. Kasus ini diselesaikan dengan menggunakan GDPR dan hukum nasional yang berlaku di Italia.

Studi komparasi yang dilakukan dengan membandingkan penyelesaian, pertanggungjawaban serta upaya hukum yang dilakukan dalam dua Negara yang berbeda dengan menggunakan dua hukum yang saling berkaitan. Melalui kasus PT. Bank Syariah Indonesia dengan bank UniCredit Italia diharapkan dapat menjadi acuan bagi Indonesia jika kembali terjadi insiden serupa terkhusus pada sektor perbankan.

METODE

Metode penelitian ini adalah penelitian hukum normatif, yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan Pustaka atau data sekunder. Disebut juga penelitian *doctrinal*, di mana hukum sering kali dikonsepkan sebagai apa yang tertulis dalam peraturan perundang-undangan *(Law in books)* atau dikonsepkan sebagai kaidah atau norma yang merupakan patokan berperilaku manusia yang dianggap pantas.

Metode Pengumpulan data yang akan digunakan dalam penelitian ini dilakukan dengan cara studi kepustakaan terhadap bahan-bahan hukum, baik dalam hukum primer, bahan sekunder, maupun bahan hukum tersier dan/atau bahan non hukum. Metode pengumpulan data yang digunakan dalam penelitian Adalah melalui studi Pustaka *(library research)* dan Studi Dokumen. Studi Pustaka dilakukan dengan mengumpulkan data dengan cara mempelajari peraturan perundang-undangan, literatur, tulisan para ahli hukum, dan leputusan hakim yang berkaitan dengan penelitian ini.

HASIL DAN PEMBAHASAN

Perbandingan Mekanisme Penyelesaian Kasus Pencurian Data Pribadi di Indonesia dan Eropa

Latar Belakang dan Tujuan Regulasi Perlindungan Data Pribadi

Di Indonesia, sebelum disahkannya Undang – Undang Perlindungan Data Pribadi pada tahun 2022 (UU PDP), perlindungan hukum terhadap kasus yang berkaitan dengan data pribadi masih bersifat sektoral, parsial serta tidak secara khusus dan komprehensif mengatur hak Subjek Data dan kewajiban Pengendali Data. Regulasi atau hukum yang digunakan juga berkembang mengikuti kebutuhan masyarakat. Beberapa dasar hukum kerap digunakan sebelum kehadiran UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi, antara lain UU No. 39 Tahun 1999 Tentang Hak Asasi Manusia yang menjamin hak atas perlindungan diri pribadi dan rasa aman sebagaimana diatur dalam Pasal 29 dan 30 UU HAM. Selain itu, UU Nomor 23 Tahun 2006 jo. UU No. 24 Tahun 2013 tentang Administrasi Kependudukan memberikan perlindungan terbatas terhadap data kependudukan, termasuk sanksi bagi pihak yang menyalahgunakannya sebagaimana tercantum dalam Pasal 95A. Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik mengatur kewajiban penyelenggara sistem elektronik untuk menjaga kerahasiaan data pengguna serta kewajiban melapor jika adanya kegagalan perlindungan data. Di samping itu, PP No. 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik memuat sanksi administratif bagi penyelenggara

yang melanggar ketentuan perlindungan data. Demikian pula, UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) pada Pasal 26 Ayat (1) menegaskan bahwa penggunaan data pribadi harus dilakukan dengan persetujuan pemilik data. Namun sayangnya, penyelesaian pada regulasi – regulasi ini masih bersifat rancu dan belum memliki penyelesaian yang konkrit.

Di lain sisi, regulasi perlindungan data di Eropa, GDPR, disahkan pada tahun 2018 atas suatu bentuk kepastian hukum yang melindungi hak – hak, prinsip, dan kewajiban yang berkaitan dengan data pribadi seseorang. Regulasi ini bersifat directly applicable yang artinya memiliki daya mengikat yang penuh bagi seluruh Negara Anggota Uni Eropa. Pada kedudukannya di Hukum Internasional, GDPR telah menjadi pedoman global bagi banyak Negara di Dunia, selain Indonesia, banyak Negara lain yang mengadopsi GDPR bagi hukum nasionalnya seperti Brazil, Jepang, hingga Korea Selatan. GDPR memperlihatkan sistehm hukum yang kuat dan memberikan efek jera bagi pelanggar serta penyelesaian yang dapat menjadi inspirasi bagi penyelesaian hukum di Indonesia.

Penyelesaian Kasus Pencurian Data Pribadi di Indonesia dengan UU PDP

Pasca UU PDP disahkan pada tahun 2022 dan melalui masa transisi selama dua tahun hingga akhirnya secara penuh diberlakukan pada tahun 2024. Meskipun begitu, hingga pertengahan 2025, belum ditemukan kasus pencurian data yang secara definitif diselesaikan melalui mekanisme UU ini. Mengambil kasus pencurian data PT. Bank Syariah Indonesia (BSI) pada tahun 2023 yang mengalami serangan *ransomware* sebanyak lebih dari 1,5 *Terabyte* data hanya melalui penyelesaian internal dan tidak transparan serta konkrit. Hal ini dikarenakan pada masa tersebut, UU PDP masih dalam masa transisi dan belum terbentuknya lembaga pengawas independen yang secara khusus diamanatkan untuk mengawasi dan memberikan sanksi atas pelanggaran maupun insiden serupa. BSI mengaku telah melakukan penyelesaian internal dengan bekerja sama dengan Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), serta Kominfo berupa asesmen terhadap serangan, audit hingga mitigasi agar gangguan serupa tidak terulang. Jika melihat pada ketentuan UU PDP, atas konsep *das sollen* dan *das sein*-nya langkah penyelesaian ideal yang dapat diambil oleh BSI yakni;

1. Notifikasi Wajib oleh BSI

Pada Pasal 46 Ayat (1) UU PDP, jika terjadi kegagalan perlindungan data, pihak pengendali data wajib menyampaikan notifikasi pemberitahuan secara tertulis paling lambat 3x24 jam kepada pihak pemilik data dan lembaga terkait setelah insiden terjadi. Pada penerapannya, dua hari setelah insiden BSI melakukan siaran pers namun bukan atas alasan pencurian data melainkan pemeliharaan system, sehingga BSI dianggap tidak menyampaikan pemberitahuan secara tertulis kepada nasabah terkait serangan siber.

2. Melakukan Pemulihan

BSI dengan sigap melakukan pemulihan layanan elektronik secara bertahap setelah satu pekan layanan perbankan terganggu, termasuk proteksi data.

2. Investigasi oleh Lembaga Pengawas Data Pribadi

Hingga saat ini, belum ada Lembaga Pengawas Independen di Indonesia yang dibentuk sesuai dengan ketetapan UU PDP. Lembaga Pengawas masih bersifat sektoral sehingga penyelesaian belum konkrit sampai pada akarnya. Dalam kasus ini, Kominfo dibantu oleh BSSN dan OJK menjadi lembaga yang mengawasi dan memberikan pemulihan atas insiden yang terjadi. Namun tidak ada sanksi yang tegas, hanya berupa teguran dan perbaikan layanan.

3. Sanksi Administrasi

Pihak penyelenggara dapat dikenai sanksi atas kelalaian berupa teguran tertulis, penghentian sementara aktivitas pemrosesan data, penghapusan data, hingga denda administratif dengan maksimal 2%dari pendapatan tahunan perusahaan yang diatur dalam Pasal 57 UU PDP.

4. Sanksi Pidana

Jika ditemukan adanya unsur kesengajaan maka dapat dikenakan hukum pidana yang tertera pada Pasal 67-69 UU PDP dengan denda pidana penjara paling lama 5 tahun dan denda 5 miliar rupiah.

5. Hak Ganti Rugi

Nasabah yang dirugikan berhak mengajukan Ganti rugi melalui jalur litigasi sebagaimana diatur dalam Pasal 12 Ayat (1) UU PDP baik melalui gugatan individu atau non litigasi seperti mediasi melalui lembaga pengawas sektoral.

6. Penyelesaian yang Transparan

Penyelesaian yang transparan diperlukan agar dapat menimbulkan kepastian hukum dan menjawab keresahan Masyarakat terutama pihak nasabah.

Mekanisme Penyelesaian Kasus Pencurian Data Pribadi di Eropa dengan GDPR

Di Eropa, mekanisme penyelesaian kasus pencurian data pribadi atau *data privacy breach* dijalankan oleh Otoritas Perlindungan Data berdasarkan kerangka yang diatur pada GDPR. Lembaga ini memberi kewenangan untuk mengeluarkan perintah korektif, perintah administratif, serta denda administratif sesuai Pasal 58 dan Pasal 83 GDPR. . Setelah melalui masa 2 tahun transisi, GDPR berlaku penuh pada 25 Mei 2018 yang pada akhirnya menjadi kerangka hukum utama perlindungan data pribadi di Uni Eropa dengan membawa standar baru seperti hak – hak Subjek Data Pribadi, prinsip – prinsip yang dianut, hak portabilitas data, kewajiban notifikasi pencurian data dalam 72 jam, hingga denda administratif hingga 20 Juta Euro atau 4% dari omzet global perusahaan.

Walaupun demikian, Eropa tidak lepas dari kasus pencurian data pribadi dari para peretas. Seperti insiden yang dialami oleh Bank UniCredit pada tahun 2016. Kasus ini merupakan salah satu kasus besar yang menguji penerapan GDPR di Eropa. Peretas berhasil menyusup ke dalam sistem keamanan UniCredit dan mengakses data pribadi nasabah. Akibatnya, lebih dari 400.000 (empat ratus ribu) data pelanggan terekspos, termasuk informasi kartu kredit, nama, alamat, dan data sensitif lainnya. Pada tahun 2017 UniCredit secara resmi mengumukan publik tentang pencurian data terhadap pelanggan pinjaman akibat vendor eksternal atau dalam hal ini pihak ketiga.

Selanjutnya, pada akhir Juli 2017, UniCredit melaporkan kepada pihak Otoritas Perlindungan Data di Italia yang bernama *Garante per La Protezione Dei Dati*

Personali (Garante), atau dalam hal ini, pihak Otoritas Perlindungan Data Pribadi Italia. Insiden ini diperkirakan mempengaruhi kurang lebih 700.000 (tujuh ratus ribu) hingga 762.000 (tujuh ratus enam puluh dua ribu) nasabah secara kumulatif dari tahun 2016 – 2017. Hasil investigasi Garante menunjukkan manajemen akses tidak memadai. pasca investigasi menyeluruh, pihak Otoritas Privasi Italia menetapkan bahwa insiden 2016 – 2017 adalah merupakan pelanggaran serius meskipun belum ada GDPR sebagai evaluasi pelanggaran pra – GDPR. Dengan berbekal regulasi nasional Italia,"*Codice In Materia di Protezione dei Dati Personali*" (Kode Privasi Italia). Putusan yang dikeluarkan pada tahun 2020 menjatuhkan denda sebesar €600.000 (enam ratus ribu *euro*) atau dalam nilai rupiah tahun 2020, sekitar Rp 10.228.800.000 (10,23 Milyar Rupiah) kepada pihak UniCredit.

Pada tahun 2018, kembali terjadi serangan siber besar terhadap platform *mobile banking* UniCredit yang berdampak kepada nasabah dan mantan nasabah UniCredit. Setelah investigasi menyeluruh, pihak Garante menjatuhkan denda sebesar €2.8 juta *euro* kepada pihak *data controller* atau pengendali data UniCredit serta denda sebesar €800.000 (delapan ratus ribu *euro*) kepada perusahaan pemroses data yang ditunjuk oleh bank (*data processor*). Yang dianggap melanggar Pasal 5 dan Pasal 32 GDPR.

Hal ini membuktikan bahwasanya keamanan data bukan lagi sekedar kewajiban teknis, namun menjadi kewajiban hukum yang berdampak besar secara materiil. Dengan menjatuhkan denda ganda tidak hanya kepada pihak pengendali data namun juga kepada pihak pemroses data, menunjukan bahwa GDPR memiliki cakupan yang luas dalam pertanggungjawaban hukum. Jika dapat disimpulkan dapat berupa;

1. Das Sollen pada ketentuan normatif GDPR

GDPR menetapkan bahwa Pengendali Data (*data controller*) wajib menjamin keamanan pemrosesan data dengan langkah teknis dan terorganisir secara memadai dalam Pasal 32 GDPR. Dimana apabila terjadi pencurian data, Pengendali Data wajib melaporkan kepada otoritas pengawas dalam waktu 72 jam yang tertera pada Pasal 33 GDPR, serta memberikan notifikasi kepada pihak Subjek Data jika insiden tersebut berisiko tinggi di Pasal 34 GDPR. Selanjutnya, sanksi administratif juga diatur dalam Pasal 83 GDPR dengan denda maksimum €20 (dua puluh) juta atau 4% (empat persen) omzet global.

2. Das Sein pada kenyataan empiris

Dalam praktiknya, pihak UniCredit telah memenuhi kewajiban prosedural untuk melakukan notifikasi kepada pihak Otoritas Garante setelah insiden terdeteksi dan melakukan pemberitahuan ke nasabah yang tertera pada Pasal 33 dan Pasal 34 GDPR, pihak UniCredit menyatakan langsung melaporkan insiden langsung tanpa penundaan dalam kurun kurang lebih 2 hari setelah insiden terjadi. Walaupun demikian, UniCredit tetap dinyatakan melanggar GDPR karena gagal memenuhi kewajiban yang tertera pada Pasal 32 GDPR atas keamanan yang memadai, kegagalan prinsip akuntabilitas pada Pasal 5 GDPR serta belum terlaksananya hak ganti rugi seperti tertera pada Pasal 82 GDPR.

Dengan demikian, dapat disimpulkan bahwa Indonesia perlu lebih menguatkan implementasi UU PDP agar lebih sejalan dengan standar internasional

GDPR, khususnya dalam hal mekanisme notifikasi insiden, pemberian kompensasi, sanksi administratif serta pembentukan Otoritas yang berwenang.

Penulis lampirkan tabel perbandingan terkait upaya perlindungan hukum pencurian data pribadi di Indonesia menggunakan ketentuan Undang – Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi dan di Eropa dengan menggunakan ketentuan *General Data Protection Rights* atas hasil analisa yang dijabarkan pada bab pembahasan.

Tabel 1. Tabel Perbandingan
Tabel Perbandingan Upaya Perlindungan Hukum Pencurian Data Pribadi Di Indonesia dan Eropa

No.	**Aspek Perbandingan**	**Indonesia (UU No. 27 Ta Tentang PDP)**	**Eropa (*General D ction Regulation*)**
1.	Kerangka Dasar Perlindungan Hukum	Mengatur pemrosesan di, hak subjek data, kewaji ndali data, penyeles eta hingga sanksi perdat a. (Pada Pasal 2 – 15 UU PD	Regulasi komprehe enai perlindungan di di Eropa meng p, hak subjek d iban pengendali d er data, sanksi, hin igasi menyeluruh. (Pada Pasal 1 – 5GDP
2.	Upaya Hukum	1. Administratif (peringa , penghentian pemrose Pasal 57 UU PDP 2. Perdata (menuntut rugi) pada Pasal 12 Ayat (3) 3. Pidana (untuk pelangga tu) pada Pasal 65 – 68 UU	1. *Administrative Fine tive Measures* (de istratif) dari *Data Pri rity* pada Pasal 58 da R 2. *Judicial Reme* an dapat menggu pengontrol / pemr pada Pasal 79 GDPR 3. *Compensation Ri* an berhak mendapat g penuh sesuai kerug Pasal 82 GDPR.
3.	Perlindungan Huk Ditawarkan	Menjamin hak ak ikan, hapus data, hak men tujuan hingga pembat osesan pada Pasal 5 – 13	Menjamin hak akses d apus data, hak pembata osesan data, hak kebera hak data untuk ti filkan pada Pasal 12 - R.

4.	Studi Kasus	Kasus Peretasan den *mware* pada PT. Bank Sya esia Tahun 2023.	Kasus Peretasan B redit Italia, Eropa Ta & 2018.
5.	Sanksi	Menawarkan dua jenis sa ; 1. Sanksi administratif (P 8 UU PDP) berupa peringa is, penghentian kegi osesan, hingga de istratif sesuai den uran turunannya. 2. Sanksi Pidana (Pasal 65 – 68 UU PDP) Berupa pidana penjara 4 hingga denda administrati ar rupiah.	Menawarkan satu j i berupa; 1. Sanksi administ 83 GDPR) Berupa denda hingga atau 4% *global an ver* (dipilih yang l), serta peri hentian pemrose atasan, dan penghapu GDPR tidak mem i pidana, namun Ne ota dapat menetap i pidana sesuai huk nal masing – masing.
6.	Pertanggungjawaban ndali Data	1. Pengendali wajib menja anan data, mencegah a , dan pelaporan insiden kep k data pada Pasal 20 – 21 2. Pengendali w rapkan langkah keama num pada Pasal 35 UU PD	1. Pengendali anggung jawab penuh *y*) pada Pasal 24 – 32) 2. Wajib menera p dan langkah keama num serta melapor n maksimal 72 jam s i pada Pasal 33 – 34 GD
7.	Lembaga Pengawas y enang	Pasal 58 – 59 UU P amanatkan pembentu aga Pengawas di Indon n belum dibentuk hingga	Setiap Negara mem aga Pengawas y enden pada Pasal 51 - R yang berwen beri perintah, mengau blokir pemrosesan tuhkan sanksi (con nte Italia)

8.	Kesimpulan	1. Kerangka hukum su adopsi GDPR tetapi se mentasi masih belum ideal 2. Belum ada Lemb was sehingga up lesaian hukum belum da an efektif.	1. GDPR melindungi ak subjek data berikan opsi penyelesa eta dengan jelas, te memberikan kewenan kepada Lemb was independen g – masing Negara.

Sumber : Data Diolah

SIMPULAN

Secara normatif (*das sollen),* UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi telah mengadopsi prinsip – prinsip utama dari GDPR, seperti hak subjek data, kewajiban notifikasi, dan pertanggungjawaban Pengendali Data. Namun, pada implementasinya *(das sein)*, mekanisme penyelesaiannya masih menghadapi kendala besar lantaran pada saat itu UU PDP masih dalam masa transisi dan belum ada lembaga/instansi nasional yang secara resmi menjadi pihak regulator. Hal ini tercermin pada hasil studi kasus PT. Bank Syariah Indonesia (BSI) yang berjalan tidak transparan, lambat, dan tidak diikuti dengan penjatuhan sanksi yang tegas terhadap Pengendali Data yang lalai. Ketidakhadiran Otoritas Perlindungan Data Pribadi yang independen menyebabkan koordinasi antar Lembaga Pengawas sektoral (seperti Kementerian Komunikasi Digital, OJK, BSSN) menjadi tidak terintegrasi dan lemah dalam penegakan hukum. Sebaliknya, mekanisme penyelesaian yang tertera dalam GDPR dapat lebih memberikan sisi yang komprehensif, terstruktur, dan memiliki efek jera yang tinggi, seperti yang terjadi pada kasus UniCredit yang diselesaikan secara transparan oleh Otoritas Perlindungan Data Pribadi Italia (Garante) dengan denda administratif yang signifikan dan membuat jera. Sehingga diharapkan, pemerintah Republik Indonesia dapat segera mengesahkan pembentukan Otoritas Perlindungan Data Pribadi Nasional yang menjadi regulator utama dalam sektor perlindungan data pribadi dengan menerapkan UU PDP seutuhnya.

Demi meningkatkan keefektivitasan perlindungan dan menjaga data pribadi agar terhindar dari kemungkinan – kemungkinan yang tidak diinginkan, disarankan bagi pihak pemerintah dan pembuat kebijakan Republik Indonesia, dalam hal ini Presiden untuk segera mempercepat pembentukan Otoritas Perlindungan Data Pribadi yang independen dan berwenang. Dibekali dengan kewenangan penuh untuk melakukan pengawasan, investigasi, dan penjatuhan sanksi administratif yang tegas dan proporsional, sebagaimana mandat Pasal 58 UU PDP. Otoritas ini harus terbebas dari intervensi politik dan memiliki sumber daya yang memadai. Selanjutnya diiringi dengan meningkatkan koordinasi dan sinkronisasi antar Lembaga Pengawas Sektoral, dalam hal ini Komdigi, OJK, serta BSSN perlu linear dengan ketentuan OPDP dalam menangani insiden yang berkaitan dengan Data Pribadi.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dalam pelaksanaan penelitian ini. Ucapan terima kasih secara khusus disampaikan kepada dosen pembimbing atas bimbingan dan masukan yang konstruktif, serta kepada rekan-rekan akademisi dan mitra diskusi yang turut memberikan pandangan kritis dalam penyusunan tulisan ini.

Apresiasi juga diberikan kepada pihak-pihak yang telah membantu dalam proses teknis, seperti korektor, juru ketik, dan penyedia bahan referensi. Penulis tidak lupa menyampaikan penghargaan kepada institusi yang telah memberikan dukungan fasilitas maupun sumber daya selama proses penelitian berlangsung.

DAFTAR RUJUKAN

Graham Greenleaf, 2021, Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, *Privacy Laws & Business International Report,* Issue 169, hlm. 10.

Dewa Made Gede, 2018, Perlindungan Data Kependudukan dalam UU Administrasi Kependudukan, *Jurnal Legislasi Indonesia*, Vol. 15, No. 3, hlm. 221.

Sinta Dewi Rosadi, 2021, Urgensi Perlindungan Data Pribadi dalam Sistem Elektronik, *Jurnal Rechts Vinding*, Vol. 10, No. 1, hlm.67.

Amirudin dan H Zainal Asikin, Pengantar Metode Penelitian Hukum, Jakarta: Raja Grafindo Persada,2006 ,hlm.118.

Adi Nugroho, 2018, *Cyberlaw: Aspek Hukum Teknologi Informasi,* Bandung, Refika Aditama, hlm. 115.

Iqbal, Muhammad dan Andri Gunawan "Metode Penelitian Hukum Normatif dan penerapan slogisme dalam menarik Kesimpulan hukum (*Jurnal Penelitian Hukum*,2021), Vol.15 No.1

Soerjono Soekanto dan Sri Mamuji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, Jakarta: Raja Grafindo Persada, 2013, hlm.13.

Nugroho, S.S.,& Haryani, A.T., *Metologi Riset Hukum* (Lakeisha: Klaten, 2020), hlm.70.

Undang – Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi Tahun 2022

General Data Protection Rights 2018

Kompas.com, Maullana I. 2024. "Kasus Kejahatan Siber Turun Menjadi 3.331 Sepanjang 2024." nasional.kompas.com/read/2024/12/31/15115151/kasus-kejahatan-siber-turun-menjadi-3331-sepanjang-2024;

