Syiah Kuala Law Journal
FAKULTAS HUKUM UNIVERSITAS SYIAH KUALA
Vol. 7 (3) Desember 2023, pp. 324-335
ISSN : 2580-9059 (online)
2549-1741 (cetak)

# STUDI KOMPARASI PELINDUNGAN DATA PRIBADI WARGA NEGARA INDONESIA DALAM TRANSFER DATA PRIBADI LINTAS BATAS *(TRANSBORDER PERSONAL DATA TRANSFER)* ANTARA INDONESIA DENGAN JEPANG

**Shafira Nadya Nathasya[1], Sinta Dewi Rosadi[2] Garry Gumelar Pratama[3]**
[1,2,3)] Universitas Padjadjaran

**Article Info**
Received: 20/09/2023
Accepted: 10/11/2023

**Kata Kunci :**
Transborder personal data transfer; data pribadi; perlindungan data pribadi

**Abstrak**
Studi ini berfokus pada perlindungan data warga negara Indonesia dalam transfer data pribadi lintas batas antara Indonesia dan Jepang, yang semakin relevan di era konektivitas global dan kemajuan digital. Kekhawatiran mengenai perlindungan terhadap data pribadi dan keamanan data pribadi semakin meningkat mengikuti kemajuan yang ada. Penelitian ini menggunakan pendekatan yuridis komparatif, yang memungkinkan adanya perbandingan antara kerangka hukum dan regulasi yang melindungi data pribadi di kedua negara dan melakukan studi perbandingan terhadap kedua asas tersebut. Temuan dari studi ini menunjukkan bahwa Indonesia dan Jepang telah menerapkan undang-undang untuk melindungi data pribadi warganya. Meskipun terdapat kesamaan dalam perlindungan data pribadi, terdapat perbedaan dalam mekanisme yang mengatur persyaratan transfer data pribadi lintas batas antara kedua negara. Penelitian ini menggunakan metode deskriptif-analitik untuk memberikan gambaran dan analisis penerapan peraturan berdasarkan ketentuan hukum yang berlaku. Tujuan utamanya adalah menganalisis perbedaan dan persamaan antara kedua undang-undang tersebut untuk menarik kesimpulan umum mengenai pendekatan dan aturan yang diterapkan dalam perlindungan data pribadi di Indonesia dan Jepang. Dengan demikian, penelitian ini memberikan wawasan penting tentang pengamanan data pribadi dalam konteks transfer data lintas batas antara kedua negara.



***Corresponding Author:***
Shafira Nadya Nathasya
Email: Shafiranadyanathasya@gmail.com

## I. PENDAHULUAN

Setiap individu memiliki berbagai macam hak yang mendukung kehidupannya dan tidak dapat disalahgunakan oleh siapa pun. Mereka berhak mendapatkan perlindungan hukum terhadap campur tangan atau serangan terhadap kehidupan pribadi dan hak-hak yang mereka miliki, termasuk data yang dimiliki. Secara prinsip, privasi merupakan kewenangan guna mengendalikan informasi pribadi seseorang dan memiliki kapabilitas untuk menentukan bagaimana informasi tersebut diperoleh dan digunakan (Edmon Makarim, 2005). Data dapat dikategorikan sebagai data pribadi individu jika data tersebut terkait dengan pihak yang dapat diidentifikasi atau dengan pihak yang dapat diidentifikasi, yaitu Subjek Data (Council of Europe, 2018). Tujuan utama dari adanya privasi adalah untuk memberikan hak bagi Subjek Data selaku pihak yang memiliki data pribadi tersebut agar dapat

menentukan bagaimana dan kapan percakapan, pemikiran, atau perilaku mana yang dapat dipublikasikan (Westin, 1966). Inisiasi untuk memberikan perlindungan atas privasi di Indonesia diatur pertama kali dalam Undang-Undang Dasar 1945 (Sinta Dewi, 2015). Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (selanjutnya disebut UU PDP) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, mengatur mengenai tindakan-tindakan apa saja yang termasuk dalam pemrosesan data pribadi, hal itu meliputi pemerolehan dan pengumpulan, pengolahan dan penganalisisan, penyimpanan, perbaikan dan pembaharuan, penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan dan/ atau penghapusan atau pemusnahan.

Transfer data pribadi lintas batas mengacu atas pergerakan atau transfer data pribadi antar server lintas batas negara (BSA, 2017). Transfer data pribadi lintas batas biasanya dilakukan dengan wujud yang dapat dipahami oleh mesin dan melalui fasilitas telekomunikasi (Peter Robinson, 1986). Karena adanya tingkat perlindungan data yang tidak merata di berbagai negara, perlindungan data telah menjadi hambatan utama dalam tindakan transfer data pribadi lintas batas. Dalam hal ini, prinsip dalam transfer data pribadi harus diselaraskan dengan persyaratan perlindungan data yang efektif, terlepas dari batas-batasnya (Lingjie Kong, 2010). Atas dampak yang dimiliki, membuat adanya tindakan transfer data pribadi lintas batas yang terjadi setiap saat. Hal ini dibuktikan dengan transfer data pribadi lintas batas yang menjadi sumber kehidupan ekonomi baru yang dianggap akan terus tumbuh hingga diperkirakan mencapai 65% PDB dunia pada akhir tahun 2022 (Deloitte, 2022). The International Data Corporation memperkirakan investasi dalam transformasi digital menjadi total USD 6,8 triliun dari tahun 2020 hingga 2023, setara dengan PDB gabungan Prancis dan Jerman (Zurich Insurance, 2022).

Dengan dampak yang dihasilkan, beberapa negara juga mengakui perlindungan data sebagai hak konstitusional individu untuk memperoleh perlindungan terhadap data pribadi mereka dan untuk mendapatkan keadilan jika terjadi pelanggaran terhadap data tersebut, tak terkecuali Indonesia (Sinta Dewi, 2016). terdapat berbagai alasan yang memotivasi negara-negara untuk mengatur aliran data lintas batas, mulai dari menjaga privasi individu dan data pribadi, perlindungan informasi yang dianggap sensitif hingga untuk mengembangkan kapasitas domestik di sektor yang intensif secara digital, sebagai bentuk kebijakan industri digital (OECD, 2022). Dengan adanya privasi, maka akan terdapat persoalan yang mengikuti seperti privasi dapat dilanggar tanpa individu bersangkutan menyadarinya karena individu tersebut tidak pernah diberitahu mengenai aktivitas pengintaian yang memantau dan tidak adanya kapabilitas atau diberikan kesempatan untuk mempertanyakan mengenai aktivitas tersebut (Sinta Dewi, 2015). Pentingnya, konsep privasi itu sendiri adalah konsep yang sulit untuk didefinisikan secara pasti karena bersifat abstrak dan dipengaruhi oleh berbagai faktor seperti konteks sosial dan pandangan masyarakat yang berbeda, sehingga menghasilkan beragam persepsi (Sinta Dewi, 2015).

Terdapat kasus yang dikenal dengan *The Schrems Case* sebagai bukti atas pelanggaran atas privasi yang awalnya tak disadari oleh Subjek Data, yang mana Maximillian Schrems yang telah menjadi pengguna Facebook sejak 2008 berdasarkan pengungkapan Edward Snowden pada tahun 2013 tentang praktik pengawasan yang digunakan oleh badan intelijen Amerika Serikat, Maximillian Schrems mengajukan keluhan kepada Komisaris Perlindungan Data Irlandia yang menuduh bahwa Facebook mentransfer datanya dari server Irlandia Facebook ke Amerika Serikat tanpa persetujuannya dan melanggar persyaratan Uni Eropa untuk memastikan perlindungan data yang setara. Badan Perlindungan Data Irlandia menolak klaim tersebut dan mengatakan bahwa *Privacy Shield* memberikan perlindungan yang cukup. Pengadilan Tinggi Irlandia kemudian mengkonsultasikan atas kasus tersebut dan Mahkamah Uni Eropa menerima evaluasinya. Namun, Mahkamah Uni Eropa membatalkan *Privacy Shield* dan Mahkamah Uni Eropa berpendapat bahwa sebelum menentukan kecukupan tersebut, Komisi Eropa seharusnya menegaskan bahwa hukum domestik negara ketiga yang dalam hal ini hukum domestik Amerika Serikat atau komitmen internasionalnya melindungi hak atas perlindungan data pribadi yang seharusnya pada dasarnya setara (Shakila Bu-Pasha,2017).

Kasus tersebut seolah memberikan fakta bahwa adanya tindakan transfer data pribadi lintas batas bukan tanpa hambatan. Salah satu permasalahannya adalah masalah yurisdiksi yang meliputi pilihan hukum yang berlaku dianggap cukup kompleks dalam aliran data pribadi lintas batas (OECD, 2013). Hal ini dikarenakan setiap negara memiliki hukumnya sendiri yang merupakan hukum domestik atau bagian dari hukum domestik (OECD, 2000). Selain itu, terdapat hambatan lainnya yaitu Peraturan penyimpanan lokal dan pemrosesan lokal yaitu persyaratan untuk menyimpan dan/atau memproses data pada server yang berlokasi di negara tertentu, Peraturan mengenai perlindungan data pribadi yang mengatur mengenai pengumpulan, penggunaan, dan transfer data pribadi, Keamanan siber yang meliputi kumpulan teknologi, proses, dan kontrol yang dirancang untuk melindungi sistem, jaringan, dan data dari eksploitasi yang tidak sah, hingga Pembatasan penggunaan Internet, penyensoran, dan pemblokiran terhadap transfer data (The OECD, 2020).

Adanya kewajiban tingkat perlindungan yang sama atau yang memadai bertujuan untuk meminimalisir adanya kegagalan dalam pemrosesan data pribadi. Pasal 37 Data Protection Act 2018 dikatakan bahwa data pribadi yang diproses untuk tujuan penegakan hukum apapun wajib memadai, relevan, dan tidak berlebihan sehubungan dengan tujuan pemrosesannya, hal ini pun selaras dengan salah satu prinsip perlindungan data pribadi dalam EU General Data Protection Regulation dan The Madrid Resolution: International Standards on the Protection of Personal Data and Privacy. Perlindungan yang sama dalam ketentuan ini mengacu kepada penggunaan kata yang digunakan EU untuk menggambarkan negara, wilayah, sektor, atau organisasi internasional lain yang dianggapnya memberikan tingkat perlindungan data yang pada dasarnya setara dengan yang ada di dalam EU (Information Commisioner's, 2022). Maka, transfer data pribadi ke negara lain di luar Uni Eropa

dapat terjadi ketika Komisi Eropa telah memutuskan bahwa negara tujuan data ketiga memberikan tingkat perlindungan data yang setara (Security, 2022).

Menurut Pasal 56 Ayat 2 UU PDP, ketika melakukan transfer data pribadi, pihak yang mengendalikan data pribadi harus memastikan bahwa negara tempat pihak yang mengendalikan data pribadi dan/atau pemroses data pribadi yang menerima transfer memiliki tingkat perlindungan data pribadi yang setara atau lebih tinggi dari yang ditetapkan dalam UU PDP. Dengan diaturnya mengenai kewajiban akan standar yang dianggap setara dan memadai antara negara pengirim dan negara penerima dalam proses transfer data pribadi lintas batas diharapkan pula kepatuhan mengenai standarisasi tersebut karena transfer data tetap menjadi masalah penting bagi pihak yang aktivitas bisnisnya melibatkan transfer data pribadi di negara non-UE ketiga. Mengingat beratnya sanksi jika terjadi pelanggaran aturan perlindungan data pribadi yang dapat mencapai €20 juta atau 4% dari omset global tahunan pihak tersebut (Deloitte, 2022). Di Asia Pasifik, Jepang menjadi negara pertama yang mendapatkan Keputusan Kecukupan atau *Adequacy Decision* oleh Komisi Eropa pada 23 Januari 2019. *Adequacy Decision* tersebut mengizinkan transfer data pribadi dari Wilayah Ekonomi Eropa yaitu 28 negara anggota Uni Eropa ditambah Norwegia, Liechtenstein, dan Islandia) ke Jepang. Komisi Perlindungan Informasi Pribadi Jepang atau *Japan's Personal Information Protection Commission* (selanjutnya disebut PPC) juga mengeluarkan pemberitahuan pada hari yang sama yang menunjukkan bahwa negara-negara anggota EEA ditambahkan ke *whitelist* atau daftar putih Jepang untuk transfer data lintas batas (Tim & Shino, 2023).

Diharapkan dengan disahkannya UU PDP dapat lebih mengakomodir mengenai transfer data pribadi lintas batas lebih rinci agar Penyelenggara Sistem Elektronik yang melakukan transfer data pribadi lintas batas tidak lagi seolah meraba-raba atau mengira-ngira bahwa sistem keamanan yang mereka miliki memadai dan setara dengan UU PDP dan Subjek Data dapat lebih merasa aman mengenai data yang akan diproses. Terlebih, diharapkan dengan disahkannya UU PDP dapat berkaca pada PPC yang telah mendapatkan *Adequacy Decision* dari EU GDPR sejak tahun 2019 sekaligus menjadi negara pertama di Asia Pasifik yang mendapatkan *Adequacy Decision.*

## II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis komparatif yang melibatkan komparasi antara regulasi suatu negara dengan regulasi negara lain yang berkaitan dengan topik yang sama. (Nudirman Munir, 2017). Spesifikasi Penelitian ini adalah Deskriptif-Analitis dengan dirancang untuk memberikan gambaran serta analisis penerapan dalam peraturan berdasarkan ketentuan hukum yang berlaku tentang suatu objek atau keadaan masalah sehingga dapat dianalisis dengan ditarik kesimpulan umum (Ashofa Burhan, 2013).

## III. HASIL PENELITIAN DAN PEMBAHASAN

### 3.1. Analisa Japan's Act on the Protection of Personal Information

Suatu undang-undang mengenai data pribadi apabila benar-benar diterapkan, baru dapat bertindak untuk membantu melindungi Subjek Data. Oleh karena itu, penting untuk mempertimbangkan isi atau muatan yang terkandung dalam undang-undang yang berlaku (Lingjie Kong, 2010). Pada 2019 Jepang dan Uni Eropa mengakui sistem perlindungan data masing-masing telah setara yang memungkinkan data pribadi mengalir bebas di antara kedua belah pihak. Setelah dilakukan tinjauan, dikatakan bahwa prinsip kesetaraan yang dimiliki oleh Jepang telah berhasil diterapkan (Reed Smith, 2023). APPI sendiri mengalami beberapa kali amandemen sejak disahkan pada tahun 2003. Amandemen pertama dilakukan di tahun 2016 dan saat ini APPI terdapat amandemen yang terbaru pada tahun 2020 (Didomi, 2023). Amandemen APPI yang disetujui pada Juni 2020 yang akan berlaku penuh pada 1 April 2022 (Yoshifumi Onodera, 2022). Dalam hal ini, Pasal 24 menjadi landasan APPI dalam rangka tindakan pemrosesan transfer data pribadi lintas batas. APPI menggunakan penggunaan kalimat operator bisnis atau pelaku usaha yang menangani data pribadi yang merupakan pihak yang memiliki database informasi pribadi untuk penggunaan bisnis atau komersil. Namun, institusi pemerintah, pemerintah daerah, badan administratif independen, dan badan administratif berbadan hukum lokal dikecualikan sebagaimana diatur Pasal 2 Ayat 5 APPI. Terdapat beberapa ketentuan mengenai data pribadi yang hanya dapat ditransfer ke negara lain jika adanya ketentuan yang terpenuhi, yaitu:

1. Pelaku usaha harus memastikan bahwa pihak penerima data pribadi memiliki tingkat perlindungan yang memadai;
2. Jika negara atau organisasi penerima tidak menyediakan tingkat perlindungan data yang memadai, bisnis harus mengambil tindakan yang diperlukan untuk memastikan perlindungan data pribadi, seperti:
    a. Menggunakan klausul kontrak standar;
    b. Memperoleh persetujuan individu; atau
    c. Menerapkan langkah-langkah pengamanan tambahan untuk melindungi data pribadi.

Selain Pasal 24, terdapat ketentuan lain yang mengatur mengenai persyaratan dan ketentuan lainnya jika data pribadi yang ditransfer termasuk dalam kategori khusus seperti informasi tentang agama, ras, atau kesehatan. Pelaku usaha harus memperoleh persetujuan eksplisit dari individu sebelum mengumpulkan dan mentransfer data pribadi sensitif tersebut dan diatur dalam Pasal 17 dan 18 APPI, yaitu:

1. Pasal 17 APPI

a. Data pribadi sensitif, seperti informasi tentang agama, ras, orientasi seksual, atau kondisi kesehatan, hanya dapat dikumpulkan dengan persetujuan eksplisit dari individu yang bersangkutan.

b. Jika data pribadi sensitif tersebut diperoleh dari sumber lain selain dari individu yang bersangkutan, bisnis harus memberikan pemberitahuan kepada individu tersebut dan memperoleh persetujuannya sebelum data tersebut digunakan.

2. Pasal 18 APPI

a. Pelaku usaha hanya dapat memanfaatkan data pribadi sensitif sebagaimana maksud yang telah ditentukan dan diberitahukan kepada individu yang bersangkutan.

b. Jika pelaku usaha ingin menggunakan data pribadi sensitif tersebut untuk tujuan lain selain dari tujuan awal yang telah diberitahukan, pelaku usaha harus memperoleh persetujuan eksplisit dari individu yang bersangkutan.

c. Pelaku usaha juga tidak boleh mentransfer data pribadi sensitif ke pihak ketiga tanpa persetujuan eksplisit dari Subjek Data yang bersangkutan, kecuali jika diatur oleh undang-undang atau jika diperlukan untuk melindungi kepentingan publik.

d. Pelaku usaha harus memberikan perlindungan tambahan yang memadai untuk data pribadi sensitif, seperti menerapkan pengamanan tambahan untuk mencegah akses yang tidak sah atau penggunaan yang tidak sah.

Selain itu, pelaku usaha juga harus melaporkan setiap pelanggaran data yang terjadi selama proses transfer, baik kepada individu yang terkena dampak maupun kepada otoritas yang berwenang yaitu *Personal Information Protection Commission* atau PPC sebagaimana dalam Pasal 33 APPI, yaitu:

1. Pelaku usaha yang mengelola data pribadi harus memberikan pemberitahuan kepada Subjek Data yang terkena dampak jika terjadi pelanggaran data yang dapat membahayakan hak dan kepentingan Subjek Data terkait dan pemberitahuan harus dilakukan secepat mungkin setelah pelanggaran terdeteksi sebagai halnya diatur dalam Pasal 33 ayat 1.

2. Pelaku usaha juga harus melaporkan pelanggaran data tersebut kepada Komisi Perlindungan Informasi Pribadi Jepang (PPC) dalam waktu 10 hari setelah pelanggaran terjadi sebagaimana diatur dalam Pasal 33 ayat 2.

3. Jika pelaku usaha telah mengambil tindakan untuk memperbaiki pelanggaran data atau mencegah kerusakan lebih lanjut setelah pelanggaran terjadi, pemberitahuan memungkinkan untuk tidak diberikan kepada Subjek Data yang terkena dampak. Namun, pelaku usaha masih harus melaporkan pelanggaran tersebut kepada PPC sebagaimana dalam Pasal 33 ayat 3.

4. Jika pelaku usaha tidak memberikan pemberitahuan sesuai Pasal 33 ayat 1 dan ayat 2, Subjek Data yang terkena dampak atau PPC dapat mengajukan tuntutan perdata atau tindakan hukum lainnya dalam Pasal 33 ayat 4.

Dalam hal ini, pihak yang mentransfer data pribadi harus mengambil tindakan yang tepat untuk memastikan data pribadi akan dilindungi secara memadai, sebagaimana diwajibkan oleh APPI. Hal-hal tersebut diatur dengan tujuan agar hak privasi individu dilindungi sebagaimana menjadi tujuan adanya APPI. APPI tidak secara tegas menyebutkan adanya sanksi apabila terdapat pelanggaran data pribadi dalam kaitannya dengan transfer data pribadi lintas batas. Namun, dalam Pasal 82 hingga Pasal 88 diatur mengenai beberapa sanksi yang berkaitan dengan data pribadi, antara lain:

1. Pasal 82, yaitu pemberian sanksi bagi Ketua, Anggota Komisi, Penasihat Ahli, dan pejabat sekretariat yang membocorkan atau menggunakan rahasia secara sembunyi-sembunyi yang diketahuinya dalam menjalankan tugasnya dan berlaku setelah mereka pensiun dari tugasnya diancam dengan pidana penjara dengan kerja wajib paling lama 2 (dua) tahun atau denda paling banyak 1.000.000 yen.
2. Pasal 83, yaitu pemberian sanksi bagi pelaku usaha yang tidak mengambil tindakan sesuai dengan rekomendasi yang diberikan oleh PPC jika PPC menyatakan bahwa terdapat pelanggaran serius terhadap hak dan kepentingan individu sebagaimana dalam Pasal 42 ayat 2. Diberikan sanksi pidana kurungan kerja paksa paling lama 1 (satu) tahun atau denda paling banyak 1.000.000 yen.
3. Pasal 84, yaitu pemberian sanksi bagi pelaku usaha yang termasuk di dalamnya direktur, pegawai, perwakilan, atau administratornya dalam badan hukum maupun non-badan hukum yang telah menyediakan atau menggunakan basis data informasi pribadi secara diam-diam, termasuk yang seluruhnya atau sebagian digandakan atau diproses yang mereka tangani sehubungan dengan bisnis mereka untuk tujuan mencari keuntungan sendiri atau pihak ketiga secara tidak sah, dipidana dengan pidana penjara dengan masa kerja paling lama 1 (satu) tahun atau denda paling banyak 500.000 yen.
4. Pasal 85, yaitu pemberian sanksi berupa denda paling banyak 500.000 yen:
    a. Jika seseorang gagal menyampaikan laporan atau materi berdasarkan ketentuan Pasal 40 ayat (1) atau salah menyampaikan laporan atau materi, atau yang gagal menjawab pertanyaan yang diajukan oleh staf yang bersangkutan atau salah menjawab pertanyaan, atau menolak, menghalangi, atau menghindari pemeriksaan.

b. Jika seseorang gagal menyampaikan laporan atau menyampaikan laporan palsu sebagaimana PPC meminta organisasi perlindungan data pribadi yang terakreditasi untuk melaporkan layanan akreditasinya.

c. Pasal 86, pemberlakuan sanksi bagi pihak yang melanggar Pasal 82 dan Pasal 84 yang melakukan pelanggaran di luar Jepang.

5. Pasal 87, yaitu pemberian sanksi bagi:

   a. Wakil korporasi atau pegawai atau pekerja lain dari korporasi atau perseorangan yang melakukan pelanggaran sebagaimana dimaksud dalam Pasal 83 sampai dengan Pasal 85 yang berkaitan dengan usaha korporasi atau perseorangan, selain pelakunya adalah dipidana, korporasi atau orang perseorangan diancam dengan pidana denda yang ditentukan dalam pasal yang bersangkutan.

   b. Persekutuan atau yayasan tanpa badan hukum, wakil atau pengurus perkumpulan atau yayasan mewakilinya dalam hal tindakan prosedural dan ketentuan hukum acara pidana yang menjadikan korporasi sebagai tergugat atau tersangka.

6. Pasal 88, yaitu pemberian sanksi paling banyak 100.000 yen bagi:

   a. Pelaku usaha yang melanggar Pasal 26 ayat 2.

   b. Seseorang yang bukan merupakan organisasi perlindungan data pribadi terakreditasi tidak boleh menggunakan sebutan dari organisasi perlindungan data pribadi yang terakreditasi.

   c. Seseorang yang melakukan pelanggaran dalam Pasal 58 atau Pasal 59 ayat 2.

   d. Pelaku usaha yang tidak melaporkan perubahan yang terjadi sebagaimana diatur dalam Pasal 60 ayat (1) atau yang tidak melaporkan perubahan yang terjadi dalam keadaan lain sebagai halnya dalam Pasal 60 ayat (2).

### 3.2. Komparasi antara Undang-Undang Nomor 27 Tentang Pelindungan Data Pribadi dengan Act on the Protection of Personal Information

Setelah dilakukannya Analisa terhadap APPI, maka dapat dilakukan studi komparasi atas UU PDP dengan APPI yang jika ditarik lebih luas, terdapat beberapa poin yang dapat menjadi perbedaan antara UU PDP dan APPI, yaitu:

I. Perbedaan antara UU PDP dan APPI

   A. Pengaturan terhadap Data Pseudonim, UU PDP tidak memiliki aturan mengenai data pseudonym sedangkan APPI memiliki aturan mengenai data pseudonim;

   B. Ruang Lingkup Regulasi, UU PDP mengatur mengenai ruang lingkup hanya untuk sektor privat dan tidak berlaku untuk pemrosesan data pribadi oleh orang perorangan

dalam kegiatan pribadi atau rumah tangga sedangkan APPI mengatur mengenai ruang lingkup untuk setiap bisnis yang menyediakan pusat data pribadi untuk penggunaan komersial;

C. Pengaturan mengenai Pemerintah Pusat, UU PDP menyatakan bahwa Pemerintah Pusat merujuk pada Presiden Republik Indonesia sedangkan APPI tidak merujuk secara spesifik mengenai Pemerintah Pusat;
D. Pengaturan mengenai Pemerintah Daerah, UU PDP tidak mengatur mengenai kewenangan atau tanggung jawab yang dimiliki oleh Pemerintah Daerah dalam pelindungan data pribadi sedangkan APPI mengatur mengenai adanya kewenangan dan tanggung jawab yang dimiliki oleh Pemerintah Daerah dalam pelindungan data pribadi
E. Masa Retensi Data, UU PDP mengatur bahwa jika data pribadi dapat dihapuskan dan diakhiri pemrosesannya apabila telah mencapai masa retensi sedangkan APPI tidak secara jelas menyatakan mengenai adanya retensi data
F. Pemberlakuan Peraturan, UU PDP berlaku untuk setiap orang, badan publik, dan organisasi internasional yang melakukan perbuatan hukum di Indonesia atau di luar wilayah hukum Indonesia namun memiliki akibat hukum di Indonesia atau bagi Subjek Data WNI sedangkan APPI berlaku dalam rangka memberikan prinsip dasar untuk kebijakan dan otoritas pengaturan pemerintah, serta kewajiban pelaku bisnis swasta yang menangani informasi pribadi;
G. Sanksi atas Pelanggaran Data Pribadi, UU PDP hanya mengatur adanya sanksi administratif sedangkan APPI mengatur mengenai adanya sanksi administratif dan sanksi pidana.

II. Persamaan antara UU PDP dan APPI

Selain diatur mengenai adanya perbedaan antara kedua regulasi dari dua negara tersebut, terdapat pula beberapa poin persamaan antara UU PDP dan APPI, antara lain:

A. Tujuan Peraturan, Tujuan adanya UU PDP dan APPI untuk melindungi privasi data pribadi individu dari penggunaan yang tidak sah atau penyalahgunaan oleh pihak lain;
B. Definisi atas Data Pribadi, Baik UU PDP dan APPI memiliki definisi mengenai data pribadi yang berarti informasi yang dapat mengidentifikasi seseorang secara langsung maupun tidak langsung;
C. Hak Subjek Data, Keduanya memberikan hak yang sama kepada Subjek Data untuk mengakses, memperbaiki, menghapus, dan membatasi penggunaan data pribadi mereka oleh perusahaan atau organisasi yang mengolah data tersebut;

D. Persetujuan oleh Subjek Data, Persetujuan yang diberikan oleh Subjek Data baik di Indonesia maupun di Jepang sama-sama harus diberikan sebelum tindakan pengumpulan dan pemrosesan data pribadi dilakukan.
E. Adanya ketentuan Komisi Perlindungan Data Pribadi, Terdapat Komisi yang bertanggung jawab atas perlindungan data pribadi baik di Indonesia maupun di Jepang. Di Indonesia hingga saat ini hanya disebut dengan Lembaga sedangkan di Jepang bernama Personal Information Protection Commission atau PPC;
F. Adanya Pemberlakuan Sanksi, UU PDP dan APPI memiliki sanksi yang diatur mengenai pelanggaran data pribadi dengan sama-sama memiliki sanksi administratif;
G. Notifikasi atas Pelanggaran Data Pribadi, baik UU PDP dan APPI memberlakukan kewajiban untuk memberi tahu Subjek Data dan otoritas terkait jika terjadi pelanggaran data yang dapat menyebabkan kerugian;
H. Ketentuan mengenai Keamanan Data Pribadi, UU PDP dan APPI mewajibkan untuk menerapkan tindakan keamanan yang sesuai untuk melindungi informasi pribadi dari akses, pengungkapan, atau penyalahgunaan yang tidak sah.

## IV. KESIMPULAN

Studi komparasi antara UU PDP dan APPI menghasilkan bahwa terdapat beberapa perbedaan antara UU PDP dan APPI dalam hal perlindungan data pribadi. UU PDP tidak mengatur mengenai data pseudonim, ruang lingkup regulasinya terbatas pada sektor privat, dan tidak mengatur kewenangan Pemerintah Daerah serta masa retensi data yang jelas. Di sisi lain, APPI mengatur mengenai data pseudonim, mencakup ruang lingkup untuk bisnis komersial, mengatur kewenangan Pemerintah Daerah, namun tidak secara jelas menyebutkan mengenai retensi data. UU PDP juga memiliki penerapan yang lebih luas, mencakup setiap orang, badan publik, dan organisasi internasional, sedangkan APPI berfokus pada prinsip dasar untuk kebijakan pemerintah dan kewajiban pelaku bisnis swasta. Sanksi yang diatur oleh UU PDP hanya administratif, sedangkan APPI mencakup sanksi pidana. Meskipun ada perbedaan tersebut, UU PDP dan APPI juga memiliki persamaan penting. Tujuan keduanya adalah melindungi privasi data pribadi individu dari penggunaan yang tidak sah atau penyalahgunaan oleh pihak lain. Definisi data pribadi, hak subjek data, persetujuan oleh subjek data, keberadaan komisi perlindungan data pribadi, pemberlakuan sanksi administratif, notifikasi atas pelanggaran data pribadi, dan ketentuan keamanan data pribadi juga merupakan persamaan di antara keduanya. Dalam rangka perlindungan data pribadi, perbedaan dan persamaan antara UU PDP dan APPI dapat memberikan gambaran tentang pendekatan dan regulasi yang berlaku di Indonesia dan Jepang terkait perlindungan atas data pribadi.

## DAFTAR PUSTAKA

Act on the Protection of Personal Information

BSA. (2017). Cross-Border Data Flows. Diakses pada 15 Juni 2023 dari https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf

Council of Europe. European Union Agency for Fundamental Rights. (2018). Handbook on European Data Protection Law. France: Council of Europe.

Deloitte. (n.d.). GDPR. Diakses pada 13 Desember 2022 dari https://www2.deloitte.com/al/en/pages/legal/articles/gdpr.html

Didomi. (n.d.). Japan Data Protection Law (APPI): Everything You Need to Know. Diakses pada 07 Mei 2023 dari https://blog.didomi.io/en/japan-data-protection-law-appi-everything-you-need-to-know

Edmon Makarim. (2005). Pengantar Hukum Telematika Suatu Kompilasi Kajian. Jakarta: PT Raja Grafindo Persada.

Information Commissioner's Office. (n.d.). Data protection and the EU in detail. Diakses pada 13 Desember 2022 dari https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/adequacy/

Lingjie Kong. (2010). Data Protection and Transborder Data Flow in the European and Global Context. The European Journal of International Law, 21(2).

OECD. (2000). Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks. OECD Digital Economy Papers No. 66. Paris: OECD Publishing.

OECD. (2013). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD.

OECD. (2020). Measuring the Economic Value of Data and Cross-Border Data Flows. OECD Digital Economy Papers, No. 297.

OECD. (2022). Taking Stock of Key Policies and Initiatives: OECD Background Report for the G7 Digital and Technology Track. Germany: OECD Publishing.

Peter Robinson. (1986). Legal Issues Raised by Transborder Data Flow. Canada-United States Law Journal, 11(32).

Reed Smith LLP. (n.d.). EU-Japan Adequacy Decision Now in Force. Diakses pada 16 Maret 2023 dari https://www.whitecase.com/insight-alert/eu-japan-adequacy-decision-now-force

Shakila Bu-Pasha. (2017). Cross-Border Issues Under EU Data Protection Law With Regards to Personal Data Protection. Information & Communications Technology Law, 26(3).

Sinta Dewi Rosadi. (2015). Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional. Bandung: Refika Aditama.

Sinta Dewi Rosadi. (2015). Privacy on Personal Data from International Law, Regional, and National Perspectives. Jakarta: Refika Aditama.

Sinta Dewi Rosadi. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. Yustisia Jurnal Hukum, 5(1).

The OECD Digital Library. (2020). Measuring the Economic Value of Data and Cross-Border Data Flows. OECD Digital Economy Papers, No. 297.

Tim Hickman, Shino Asayama. (n.d.). EU-Japan Adequacy Decision Now in Force. Diakses pada 02 Mei 2023 dari https://www.lexology.com/library/detail.aspx?g=a0ec5936-1360-4424-b200-5b7268a01073

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Westin, A. F. (1966). Privacy and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy. Columbia Law Review, 66(6).

Yoshifumi Onodera. (2022). Data Protection & Privacy 2022 Japan: Law & Practices. Japan: Chambers Global Practices Guides.

Zurich Insurance Group. (2022). Cross-border data flows: Designing a global architecture for growth and innovation. Zurich Insurance Group.