PLEADS
PADJADJARAN LAW RESEARCH & DEBATE SOCIETY

Padjadjaran Law Review
Volume 9, Nomor 1, 2021

P-ISSN : 2407-6546
E-ISSN : 2685-2357

Kewajiban *Data Controller* dan *Data Processor* Dalam *Data Breach* Terkait Pelindungan Data Pribadi Berdasarkan Hukum Indonesia dan Hukum Singapura: Studi Kasus *Data Breach* Tokopedia

Alvansa Vickya[1] dan Reshina Kusumadewi[2]

Abstrak

Peraturan perihal pelindungan data pribadi didasarkan atas *Fair Information Principles* sebagai prinsip-prinsip yang mengatur hubungan antara bisnis dan pemerintah yang mengumpulkan, menggunakan, dan membuka informasi personal mengenai subjek data yang digunakan oleh banyak negara. Kemudian, muncul *European Union General Data Protection Regulation 2016* sebagai *golden rule* yang menjadi patokan bagi aturan-aturan negara lainnya seperti Singapura. Pengaruh *golden rule* terhadap *Personal Data Protection (Amendment) Act 2020* milik Singapura dapat dilihat pada konsep *data controller*, *data intermediary/processor*, dan *data breach*. Metode penelitian yang digunakan dalam artikel ini ialah penelitian hukum yuridis normatif. Berdasarkan penelitian ini, ditemukan bahwa peraturan perihal pelindungan data pribadi di Indonesia yang ada pada saat ini masih terpisah-pisah dalam beberapa peraturan. Di dalamnya, tidak dikenal konsep *data controller* dan *data processor* sehingga tidak terdapat perbedaan antara penyelenggara sistem elektronik yang melakukan kontrol dan kelola atas data pribadi. Selain itu, tidak terdapat juga pengaturan perihal *data breach*. Hal ini berbeda dibandingkan dengan Singapura yang telah membagi antara *data controller* dan *data intermediary* sehingga terdapat kejelasan mengenai perbedaan kewajiban dan pertanggungjawaban di antara keduanya dalam hal terjadi *data breach*.

Kata Kunci: *data breach*, *data controller*, data pribadi, *data processor*, pelindungan data pribadi

Data Controller and Data Processor Obligations in Data Breach Related to Personal Data Protection Under Indonesian Law and Singapore Law: Tokopedia Data Breach Case Study

Abstract

The regulations regarding the personal data protection are based on the Fair Information Principles as the principles governing the relationship between businesses and governments that collect, use and disclose personal information regarding data subjects used in many countries. Furthermore, the European Union General Data Protection Regulation 2016 emerged as the golden rule which became the benchmark for the regulations of other countries such as Singapore. The effect of the golden rule on Singapore's Personal Data Protection (Amendment) Act 2020 can be seen in the concept of data controller, data intermediary/processor, and data breach. This research uses normative juridical legal research methods. Based on this research, it was found that the existing regulations about Personal Data Protection in Indonesia are still separated in several regulations. Moreover, there is no concept of data controller and data processor so that there is no difference between electronic system administrators who control and manage personal data. In addition, there are also no regulations regarding data breach. This is different from Singapore, which has divided data controller and data intermediary so that there is a solution regarding the differences in obligations and responsibilities between the two in the event of data breach.

***Keywords**: data breach, data controller, data processor, personal data, personal data protection*

1 Fakultas Hukum Universitas Indonesia, Jalan Profesor Djokosoetono, Depok 16424, Jawa Barat, alvansavi@gmail.com, Mahasiswa Sarjana Fakultas Hukum Universitas Indonesia.

2 Fakultas Hukum Universitas Indonesia, Jalan Profesor Djokosoetono, Depok 16424, Jawa Barat, bernardinreshina@gmail.com, Mahasiswa Sarjana Fakultas Hukum Universitas Indonesia.

PLEADS PADJADJARAN LAW RESEARCH & DEBATE SOCIETY
Padjadjaran Law Review
Volume 9, Nomor 1, 2021
P-ISSN : 2407-6546
E-ISSN : 2685-2357

A. Pendahuluan

Konsep privasi pertama kali ditemukan oleh Sir Edward Coke di King's Bench, England pada tahun 1604. Doktrin ini membahas kehidupan pribadi individu di dalam rumah mereka dan hak mereka untuk dibiarkan sendiri dari gangguan publik. Konstruksi dasar ini cocok untuk saat itu, karena kehidupan sosial dan moda komunikasi yang tergolong sederhana yakni melalui tatap muka atau ucapan.[3] Namun, seiring dengan berjalannya waktu, doktrin ini dianggap tidak cukup untuk melindungi privasi seseorang.

Pada tahun 1850 hingga 1900-an di Amerika Serikat, hak individu untuk dibiarkan terancam dengan pertumbuhan media cetak. Sebagai respons dari proliferasi media cetak, Samuel Warren dan Louis Brandeis menciptakan frasa "*the right to be let alone*".[4] Konsep ini dipublikasikan dalam artikel tahun 1890 yang berjudul *The Right to Privacy*. Mereka pada dasarnya memformulasikan privasi sebagai hak untuk mencegah suatu pihak, biasanya media untuk mempublikasikan kebenaran yang memalukan dengan dasar bahwa hal ini mengakibatkan bahaya atau tekanan emosional.

Dalam era digital, gagasan perihal privasi semakin diperkaya dengan informasi hingga istilah privasi dalam penggunaan kontemporer biasanya merujuk pada *informational privacy*.[5] Privasi ini secara umum dapat dipahami sebagai kemampuan individu untuk mengendalikan bagaimana data individu tersebut disimpan dan digunakan.[6] Konsep privasi ini memfokuskan pada data pribadi yang disimpan dan dikomunikasikan antara *electronic databases* serta informasi pribadi yang dikomunikasikan antar individu.[7] Hal ini dikarenakan dalam penggunaan layanan berbasis online, data seseorang mungkin saja akan disimpan dalam jangka waktu yang cukup panjang sehingga terdapat kemungkinan bagi data tersebut dibagikan kepada pihak ketiga.[8] Demi membantu mewujudkan *informational privacy*, dibuatlah pengaturan mengenai pelindungan data pribadi.[9] Meskipun *informational privacy* ini erat kaitannya dengan pelindungan data pribadi, pengaturan pelindungan data pribadi mengatur hal lain juga selain *informational privacy*. Hal ini dikarenakan pelindungan data pribadi mengatur seluruh data yang dapat mengidentifikasi individu.[10]

Banyak negara mendasarkan pelindungan data pribadi atas *Fair Information Principles* **("FIP").** FIP adalah prinsip-prinsip yang mengatur hubungan antara bisnis dan pemerintah yang mengumpulkan, menggunakan, dan membuka informasi personal mengenai subjek data. FIP pertama kali dikembangkan oleh pemerintah Amerika Serikat pada tahun 1970-an, dimana hal

---

3 Sanjay Sharma, *Data Privacy and GDPR Handbook*, Cet. 1, Canada: John Wiley & Sons, Inc, 2020, hlm. 23.

4 *Ibid.*, hlm. 24.

5 James H. Moor, "Towards a Theory of Privacy in the Information Age", *ACM SIGCAS Computers and Society*, Volume 27, Issue 3, September 1997, hlm. 30.

6 Robert Walters, Leon Trakman, dan Bruno Zeller, *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches*, Singapura: Springer Nature Singapore Pte Ltd, 2019, hlm. 157.

7 Herman T. Tavani, "Informational Privacy: Concepts, Theories, and Controversies" dalam buku *The Handbook of Information and Computer Privacy*, yang disusun oleh Kenneth Einar Himma dan Herman T. Tavani, Hoboken: John Wiley & Sons, 2008, hlm. 139.

8 Edgar A. Whitley, "Informational Privacy, Consent and The ''Control'' of Personal Data", *Information Security Technical Report*, Volume 14, Issue 3, Agustus 2009, hlm. 155.

9 *Ibid.*

10 Juliane Kokott dan Christhoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, Volume 3, Issue 4, 2013, hlm. 225.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

tersebut diwujudkan dalam *Privacy Act* 1974 dan *the Fair Credit Reporting Act* yang kemudian diterapkan oleh negara-negara lain. FIP terdiri atas lima prinsip:[11]

(1) *There must be no personal data record-keeping systems whose very existence is secret*;
(2) *There must be a way for an individual to find out what information about him is in a record and how it is used*;
(3) *There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent*;
(4) *There must be a way for an individual to correct or amend a record of identifiable information about him*;
(5) *Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data*.

Joel Reidenberg menyimpulkan bahwa FIP menjamin empat pelindungan dasar dari penyalahgunaan data:[12]

(1) *standards for data quality, which ensure that data is acquired legitimately and is used in a manner consistent with the purpose for which it was acquired*;
(2) *standards for transparency or openness of processing, such as giving individuals meaningful notice regarding how their information is being used*;
(3) *special protections for sensitive data (for example, race, sexual preference, political views, or telephone numbers dialed), such as requiring opt-in consent before such data may be used or disclosed; and*
(4) *some standards of enforcement to ensure compliance.*

Seiring dengan berkembangnya teknologi, konsep pelindungan data pribadi juga mengalami perkembangan sehingga mulai dikenal istilah *data controller* dan *data processor*. Dalam hal ini, *data controller* ialah pengendali dari data-data pribadi yang telah diterima, sedangkan *data processor* merupakan pemroses data-data pribadi tersebut. Perkembangan ini disebabkan adanya keuntungan yang lebih besar bagi *data controller* untuk berfokus dalam pengembangan usahanya dan menaruh data-data tersebut pada *data processor* sehingga ia hanya perlu mengendalikan bagaimana *data processor* memproses data-data pribadi tersebut untuk kepentingan *data controller*.[13]

Istilah *data controller* dan *data processor* salah satunya diatur dalam ketentuan *European Union General Data Protection Regulation 2016* **("EU GDPR 2016")**. Berdasarkan ketentuan Pasal 4 ayat (7) dan (8) EU GDPR 2016, *controller* merupakan entitas natural ataupun hukum, otoritas publik, badan pemerintah, atau badan lainnya yang menentukan tujuan dan cara pemrosesan data pribadi baik sendiri maupun bersama-sama, sedangkan *processor* merupakan entitas natural atau hukum, otoritas publik, badan pemerintah, atau badan lainnya sebagai pihak yang melakukan

11 *Ibid.*, hlm. 1509.

12 Joel R. Reidenberg, "Setting Standards for Fair Information Practice in the U.S. Private Sector", *Iowa Law Review*, Volume 80, Issue 497, 1995, hlm. 514-16.

13 Paul Voigt dan Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A Practical Guide*, Switzerland: Springer International Publishing AG, 2017, hlm. 80.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

pemrosesan data pribadi berdasarkan kehendak dari *data controller*.[14]

Berdasarkan Pasal 28 ayat (1) EU GDPR 2016, *data controller* dalam memilih menggunakan jasa *data processor* diharuskan untuk menilai apakah *data processor* tersebut dapat menjamin keamanan yang tinggi.[15] *data processor* tersebut telah dinilai bahwa ia dapat menjamin keamanan yang cukup untuk implementasi hal-hal teknis yang memenuhi kriteria aturan EU GDPR 2016. Selain itu, Penilaian *data controller* yang akan memilih *data processor* juga seharusnya dapat menjamin bahwa pelindungan data tersebut akan selalu ada sehingga dapat dikatakan bahwa kewajiban ini akan selalu ada meskipun telah dilakukan penilaian.[16]

Dalam EU GDPR 2016, terdapat kewajiban-kewajiban yang diemban oleh *data controller* maupun *data processor* itu sendiri. Salah satu kewajiban yang dimiliki oleh *data controller* berdasarkan EU GDPR 2016 tercantum pada Pasal 24 ayat (2) EU GDPR 2016, yakni ia harus mengadakan atau membuat kebijakan pelindungan data yang baik.[17] Sedangkan, salah satu kewajiban yang dimiliki oleh *data processor* dalam EU GDPR 2016 berdasarkan Pasal 33 ayat (2) EU GDPR 2016 ialah memberitahukan atau memberikan notifikasi kepada *controller* terkait kebocoran data (*data breach*) secara langsung setelah terjadi *data breach*.[18] EU GDPR 2016 sendiri dianggap sebagai *golden rule* atau rujukan bagi aturan-aturan lainnya, dimana hal ini dibuktikan dengan harmonisasi terhadap 28 sistem hukum yang berbeda-beda dalam European Union. EU GDPR 2016 sendiri memiliki lingkup keberlakukan yang luas, dimana ia berlaku terhadap bisnis, individual, pengadilan, bahkan pemerintah tanpa memperdulikan hukum nasional dari negara anggota EU itu sendiri.

Perkembangan terkait adanya *data controller* dan *data processor* yang memiliki fungsi dan kedudukan yang berbeda dalam menjaga dan mengelola data pribadi menimbulkan pertanyaan seperti bagaimana kewajiban mereka dalam menjaga dan mengelola data pribadi serta terkait pertanggungjawaban dari keduanya apabila terjadi *data breach*. Pada tahun 2020 sendiri terdapat kasus mengenai *data breach* yang terjadi dari data-data pribadi yang dikuasai oleh Tokopedia. Hal tersebut menimbulkan pertanyaan perihal pertanggungjawaban serta kewajiban dari *data controller* dan *data processor* apabila ditinjau dari Hukum Indonesia serta Hukum Singapura.

B. Metode Penelitian

Metode penelitian yang digunakan dalam artikel ini berupa penelitian yuridis normatif, yaitu penelitian untuk mengetahui hukum positif dari suatu hal, peristiwa, ataupun masalah tertentu.[19] Kemudian, data yang digunakan dalam artikel ini merupakan data sekunder yang terbagi menjadi bahan hukum primer dan bahan hukum sekunder.

C. Pembahasan dan Analisis

1. PENGATURAN PELINDUNGAN DATA PRIBADI

a. Pengaturan Perihal Pelindungan Data Pribadi di Indonesia

pelindungan data pribadi di Indonesia diakui dalam konstitusi sebagai hak asasi manusia.

14 Article 4 European Union General Data Protection Regulation 2016.

15 Article 28 European Union General Data Protection Regulation 2016.

16 Paul Voigt dan Axel von dem Bussche, Op.Cit., hlm. 81.

17 Article 24 European Union General Data Protection Regulation 2016.

18 Article 33 European Union General Data Protection Regulation 2016.

19 Soerjono Soekanto, *Pengantar Penelitian Hukum*, Jakarta: UI Press, 1986, hlm. 45.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

Dalam Pasal 28G ayat (1) Undang-Undang Negara Republik Indonesia Tahun 1945 **("UUD NRI 1945")**, disebutkan bahwa setiap orang memiliki hak atas perlindungan diri, keluarga, kehormatan serta harta benda yang ada dalam kekuasaannya.[20] Meskipun terdapat dasar konstitusional atas pelindungan data pribadi, sayangnya hal ini belum diatur secara mendalam dalam sebuah Undang-Undang.

Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik **("UU ITE 2016")** mengatur bahwa orang yang bersangkutan harus memberikan persetujuan atas penggunaan setiap informasi yang menyangkut dirinya.[21] Kemudian, dalam Penjelasan Pasal tersebut dinyatakan bahwa pelindungan data pribadi termasuk salah satu **hak pribadi (*privacy rights*)** dalam pemanfaatan teknologi. Hak pribadi mengandung pengertian sebagai berikut:[22]

(1) Hak pribadi merupakan **hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan**;
(2) Hak pribadi merupakan **hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai**;
(3) Hak pribadi merupakan **hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang**.

Selain itu, dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik **("UU ITE 2008")** terdapat asas *presumed liability* yang tercantum dalam Pasal 15 UU ITE 2008 sebagai pertanggungjawaban perdata.[23] Isi pasal tersebut menyatakan bahwa Penyelenggara Sistem Elektronik memiliki tanggung jawab untuk menyelenggarakan Sistem Elektroniknya secara andal dan aman. Perihal *data breach* pula terdapat pertanggungjawaban pidana yang didasarkan atas Pasal 30 dan 32 UU ITE 2008.[24] Pertanggungjawaban pidana ini ditujukan kepada pihak *data controller* maupun *data processor* apabila dilakukan oleh keduanya. Hal ini didasarkan atas dasar bahwa kedua pihak tersebut seharusnya menjaga kerahasiaan data penggunanya.

Kemudian, diterbitkan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Pelindungan Data Pribadi Dalam Sistem Elektronik **("Permenkominfo 20/2016")**. Sistem Elektronik sendiri didefinisikan sebagai serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.[25] Dalam Peraturan ini, terdapat dua peran dalam Sistem Elektronik yakni Penyelenggara Sistem Elektronik dan Pengguna Sistem Elektronik.[26] Penyelenggara adalah setiap orang, badan

---

20 Pasal 28G Ayat (1) Undang-Undang Dasar Negara Republik Indonesia.

21 Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

22 Penjelasan Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

23 Edmon Makarim, "Pertanggungjawaban Hukum Terhadap Kebocoran data pribadi", https://www.hukumonline.com/berita/baca/lt5f067836b37ef/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-oleh--edmon-makarim?page=2, diunduh 2 Mei 2021.

24 *Ibid*.

25 Pasal 1 angka 5 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang pelindungan data pribadi Dalam Sistem Elektronik.

26 Pasal 1 angka 6 dan 7 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang pelindungan data pribadi Dalam Sistem Elektronik.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

usaha, penyelenggara negara, dan masyarakat yang untuk kepentingannya sendiri atau pihak lain menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik kepada Pengguna Sistem Elektronik. Sementara, Pengguna didefinisikan sebagai setiap orang, badan usaha, penyelenggara negara, dan masyarakat yang memanfaatkan barang, jasa, fasilitas, atau informasi yang disediakan oleh Penyelenggara Sistem Elektronik.

Selanjutnya dalam Pasal 2 Permenkominfo 20/2016, dijelaskan bahwa pelindungan data pribadi dalam Sistem Elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi. Dalam Pasal 36, diatur mengenai sanksi administratif yang dapat dikenakan apabila menyebarluaskan data pribadi, yang berbunyi sebagai berikut:

> "*(1) Setiap Orang yang memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan data pribadi tanpa hak atau tidak sesuai dengan ketentuan dalam Peraturan Menteri ini atau peraturan perundang-undangan lainnya dikenai sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan berupa:*
>
> *a. peringatan lisan;*
> *b. peringatan tertulis;*
> *c. penghentian sementara kegiatan; dan/atau*
> *d. pengumuman di situs dalam jaringan (website online).*"

Kemudian, dikeluarkan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik **("PP PSTE")**. Dalam Pasal 14-18 PP PSTE, telah diberikan standar pelindungan data pribadi yang wajib dilakukan oleh Penyelenggara Sistem Elektronik. Pasal 14 ayat (1), mengatur mengenai pemrosesan data pribadi oleh Penyelenggara Sistem Elektronik yang harus memenuhi prinsip-prinsip pelindungan data pribadi. Selanjutnya, ayat (2) mengatur terkait apa saja yang termasuk dalam kegiatan pemrosesan data pribadi. Namun demikian, dalam PP PSTE tidak disebutkan tentang prosesor data pribadi. Pasal tersebut juga merupakan ketentuan pertama di Indonesia yang memperkenalkan konsep "*data controller*" atau pengendali data pribadi layaknya GDPR, meskipun dalam pengaturan ini tidak ada definisi atau penjelasan mengenai apa yang dimaksud dengan pengendali data pribadi. Selain itu, Penyelenggara Sistem Elektronik juga memiliki kewajiban untuk memberikan notifikasi kepada pengguna apabila terjadi kebocoran data.[27] Hal ini harus dilakukan selayaknya dalam konteks hubungan langsung dengan pengguna.[28]

Dalam sektor *e-commerce*, pelindungan data pribadi diatur dalam Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (**"PP PMSE"**). PP PMSE membagi beberapa peran di dalamnya. Pelaku Usaha Perdagangan Melalui Sistem Elektronik, selanjutnya disebut Pelaku Usaha adalah setiap orang ataupun badan usaha yang melakukan kegiatan usaha di bidang PMSE. Pelaku Usaha dapat dibagi menjadi Pedagang, Penyelenggara Perdagangan Melalui Sistem Elektronik **("PPMSE")** dan Penyelenggara Sarana Perantara. Dalam Pasal 5 PP PMSE, disebutkan bahwa Pelaku Usaha dibagi

---

27 Pasal 14 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

28 Edmon Makarim, Loc.cit.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

menjadi Pelaku Usaha Dalam Negeri dan Pelaku Usaha yang berkedudukan di Luar Negeri.[29]

Dalam Pasal 58 ayat (1) peraturan yang sama disebutkan bahwa:

"Setiap Pelaku Usaha yang memperoleh data pribadi sebagaimana dimaksud pada ayat (1) wajib bertindak sebagai pengemban amanat dalam menyimpan dan menguasai data pribadi sesuai dengan ketentuan peraturan perundang-undangan."[30]

Selanjutnya, dalam Pasal 59 ayat (1) disebutkan bahwa:

"Pelaku Usaha wajib menyimpan data pribadi sesuai standar pelindungan data pribadi atau kelaziman praktik bisnis yang berkembang."[31]

Dalam penjelasan pengaturan tersebut, dijelaskan bahwa standar pelindungan data pribadi yang dimaksud harus memperhatikan keberadaan standar pelindungan data Eropa dan/atau APEC Privacy Frameworks. Dalam pengaturan GDPR di Uni Eropa, pihak yang menyimpan data pribadi harus memiliki sistem pengamanan yang layak untuk mencegah kebocoran atau pemanfaatan data pribadi secara melawan hukum. Pihak tersebut juga harus memiliki tanggung jawab untuk mengganti rugi kerusakan yang terjadi atas data pribadi. Sementara, APEC Privacy Frameworks adalah seperangkat prinsip dan pedoman implementasi yang mengatur orang atau organisasi di sektor publik dan swasta yang mengontrol pengumpulan, penyimpanan, pemrosesan, penggunaan, transfer, atau pengungkapan informasi pribadi bagi negara anggota APEC. Selanjutnya, dalam Pasal 80 PP PMSE diatur sanksi administratif yang dapat dikenakan kepada Pelaku Usaha jika melanggar Pasal 59 ayat (1). Sanksi ini memungkinkan Pelaku Usaha untuk diberikan peringatan tertulis, diblokir layanannya hingga dicabut izin usahanya oleh Menteri Perdagangan.

Selanjutnya, perihal definisi untuk data pribadi dapat merujuk kepada Kitab Undang-Undang Hukum Perdata **("KUHPerdata")**, data pribadi dapat didefinisikan sebagai "benda". "Benda" tersebut dapat dimiliki dan bernilai ekonomis. Benda dapat dikelompokkan ke dalam 4 (empat) kategori yaitu:

(1) Benda berwujud;
(2) Benda tidak berwujud;
(3) Benda bergerak; dan
(4) Benda tidak bergerak.

Sedangkan apabila ditinjau dari karakteristiknya, ciri-ciri dari hak kebendaan adalah:

(1) Merupakan hak mutlak dan dilindungi terhadap pihak ketiga lainnya;
(2) Pihak (orang) yang menguasai suatu benda memiliki hak atas benda tersebut;
(3) Dalam konteks pelunasan utang, hak kebendaan memberikan hak untuk didahulukan pelunasan utangnya;
(4) Hak kebendaan memberikan hak kepada seseorang untuk melakukan gugatan.

Sebagaimana KUHPerdata, tidak ada yang membatasi bahwa data pribadi untuk dapat dikategorikan sebagai benda. Hal tersebut dikarenakan data pribadi dapat dideskripsikan sebagai benda tidak berwujud dan jika menjadi bagian dari *big data* maka data pribadi tersebut dapat bernilai ekonomis sehingga memberikan pemegang data pribadi

[29] Pasal 5 Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

[30] Pasal 58 Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Penyelenggara Perdagangan Melalui Sistem Elektronik.

[31] Pasal 59 Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Penyelenggara Perdagangan Melalui Sistem Elektronik.

hak yang dapat dipertahankan kepada pihak-pihak lainnya.[32]

Pasal 1 angka 1 Permenkominfo 20/2016, mendefinisikan data pribadi sebagai berikut:[33]

> "*data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya*."

Berbeda dengan definisi dalam Permenkominfo 20/2016, Pasal 1 angka 29 PP PSTE berbunyi sebagai berikut:[34]

> **"***data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik.*"

Definisi mengenai data pribadi tersebut, tidak mengatur perihal kepemilikan data pribadi. Hal ini kemudian akan berkaitan dengan hak dan kewajiban apa saja yang dimiliki para pihak dalam menangani data pribadi seseorang.

b. Pengaturan Perihal Pelindungan Data Pribadi di Singapura

Pengaturan perihal pelindungan data pribadi juga terdapat di Singapura yang diawali dengan *Personal Data Protection Act 2012* yang kemudian diamandemen terakhir kalinya dengan *Act No. 40 of 2020* sehingga bernama *Personal Data Protection (Amendment) Act 2020* **("PDPA 2020")** yang berlaku sejak 1 Februari 2021. Dalam Pasal 2 PDPA 2020 dijelaskan pengertian terkait data pribadi atau *Personal Data*, yakni:

> "*"personal data" means data, whether true or not, about an individual who can be identified*
>
> *(a) from that data; or*
>
> *(b) from that data and other information to which the organisation has or is likely to have access;*"

Berdasarkan Pasal 2 PDPA 2020 di atas, dapat disimpulkan bahwa data pribadi merupakan data terkait individu yang dapat diidentifikasi dari data itu sendiri atau data beserta informasi lainnya yang mungkin dimiliki oleh organisasi yang menguasai data tersebut.[35] Namun, Personal Data Protection Commission **("PDPC")** menyebutkan bahwa data pribadi tidak terbatas pada satu jenis data saja, tetapi juga seluruh data yang mengakibatkan seorang individu dapat diidentifikasi serta tidak mempermasalahkan apabila data itu benar atau akurat serta baik berbentuk data elektronik maupun bentuk lainnya. Terdapat dua dasar untuk menentukan suatu data termasuk data pribadi, yakni tujuan dari informasi dalam data berkaitan dengan individu dan individu tersebut dapat diidentifikasi dari data tersebut. Kedua dasar tersebut harus terpenuhi untuk menggolongkan suatu data ke dalam data pribadi.[36]

Selain itu, terdapat juga pengertian mengenai *data processor* seperti dalam EU

---

32 Setyawati Fitri Anggraeni, "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum di Indonesia", *Jurnal Hukum dan Pembangunan*, No. 48, Issue 4, 2018, hlm. 818.

33 Pasal 1 angka 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang pelindungan data pribadi Dalam Sistem Elektronik.

34 Pasal 1 angka 29 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

35 Article 2 Singapore Personal Data Protection (Amendment) Act 2020.

36 Personal Data Protection Commission Singapore, "ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PDPA (Revised 1 February 2021)", https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en, diunduh 3 Mei 2021.

GDPR 2016, tetapi dengan definisi lain, yakni *data intermediary*. Namun, tidak terdapat definisi perihal *data controller* sebagai pihak yang mengendalikan bagaimana data diproses. *data intermediary* dijelaskan dalam Pasal 2 PDPA, yaitu:

> "*"data intermediary" means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation;*
> *"organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not—*
> *(a) formed or recognised under the law of Singapore; or*
> *(b) resident, or having an office or a place of business, in Singapore;*"

Dalam ketentuan tersebut, terdapat kesamaan definisi dengan *data processor* dalam EU GDPR 2016, dimana kesamaan antara *data intermediary* dengan *data processor*. *data intermediary* di sini bertindak sebagai pihak yang memproses data untuk pihak lain, tetapi tidak termasuk atau menjadi bawahan pihak yang lainnya. Hal ini sama seperti pengertian *data processor* dalam EU GDPR 2016 berupa *data processor* sebagai pemroses data-data untuk kepentingan *data controller*.[37]

Meskipun tidak terdapat definisi perihal *data controller*, tetap diakui bahwa terdapat *data controller* dalam PDPA. Hal tersebut terdapat dalam Pasal 4 ayat (2) serta ayat (3) PDPA 2020 tercantum perbedaan kewajiban antara *data intermediary* dengan *Organisation* yang hanya menguasai data pribadi serta tidak memproses data pribadi.[38] Dalam ketentuan tersebut disebutkan bahwa seluruh *Organisation* yang mengendalikan data tunduk atas seluruh aturan dalam PDPA, sedangkan *data intermediary* tidak tunduk kepada seluruh aturan dalam PDPA misalnya ia hanya tunduk pada aturan yang berkaitan dengan pelindungan data pribadi, penyimpanan data pribadi, dan notifikasi kepada *data controller* apabila terjadi *data breach*.[39] Meskipun data pribadi diproses oleh *data intermediary*, *data controller* tetap berkewajiban atas data pribadi tersebut atas dasar bahwa meskipun data pribadi diproses oleh pihak lain, ia tetap bertanggung jawab bagaikan *data controller* tersebut melakukan pemrosesan datanya sendiri.[40]

Salah satu kewajiban yang dimiliki oleh *data controller* dan *data intermediary* dalam PDPA ialah terkait pelindungan data pribadi yang tercantum pada Pasal 24 PDPA 2020. Isi dari ketentuan tersebut adalah:

> "*An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent*
> *(a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and*
> *(b) the loss of any storage medium or device on which personal data is stored*."

Dalam ketentuan tersebut dijelaskan bahwa baik *data controller* ataupun *data intermediary* diharuskan membuat keamanan terkait data pribadi, baik yang dikuasainya ataupun dikendalikan olehnya dengan tujuan untuk mencegah akses, pengumpulan, penggunaan, pengungkapan, penyalinan,

---

37 *Ibid*., hlm. 24.

38 Article 4 Singapore Personal Data Protection (Amendment) Act 2020.

39 Warren B. Chik, "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform", *Computer Law and Security Review*, Volume 29, Issue 5, 2013, hlm. 563.

40 Personal Data Protection Commission Singapore, *Op.Cit.*, hlm. 25.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

modifikasi ataupun penghapusan, atau risiko serupa serta mencegah hilangnya tempat penyimpanan data pribadi ditempatkan.[41] Kewajiban tersebut tidak dibedakan antara bagi *data controller* maupun bagi *data intermediary* sebab keduanya akan menguasai data tersebut, dimana *data controller* akan mengendalikan data untuk diproses oleh *data intermediary*.

Pencegahan di atas dapat dikatakan berupa pencegahan *data breach* sesuai interpretasi *data breach* dalam Pasal 26A PDPA 2020 berupa:[42]

> "*"data breach", in relation to personal data, means*
>
> *(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or*
>
> *(b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur*."

Apabila *data breach* tersebut tetap terjadi, maka terdapat beberapa kewajiban yang ditujukan bagi *data controller* dan *data intermediary,* dimana kewajiban tersebut diatur dalam *Part VIA* tentang *Notification of Data Breaches* PDPA 2020. Dalam terjadinya *data breach,* terdapat kewajiban yang tercantum dalam Pasal 26C dan 26D PDPA 2020, dimana *data controller* diharuskan melakukan penilaian apakah *data breach* tersebut merupakan *notifiable data breach* atau dapat disebut sebagai *data breach* yang harus diberitahukan dengan dasar mengenai akibat atau jangkauan *data breach* tersebut.[43] Apabila *data breach* itu memiliki akibat yang signifikan terhadap individu yang datanya terbocorkan atau terjadinya *data breach* dengan lingkup yang luas, *data breach* tersebut termasuk ke dalam *data breach* yang harus diberitahukan. Pemberitahuan atau notifikasi terkait *data breach* wajib disampaikan pada PDPC dalam waktu 3 hari setelah dilakukan penilaian serta masing-masing individu yang terkena dampak *data breach*. Akan tetapi, notifikasi terhadap individu tidak perlu dilakukan apabila tidak terdapat dampak buruk yang signifikan bagi individu yang terkena *data breach* atau apabila diperintahkan untuk tidak diberikannya notifikasi terhadap individu yang terdampak *data breach*. Kewajiban-kewajiban yang telah disebutkan tersebut berbeda dengan kewajiban *data intermediary* yang hanya diharuskan untuk memberitahukan atau memberikan notifikasi segera setelah *data breach* terjadi kepada *data controller* dan *public agency* sesuai Pasal 26C dan 26E PDPA 2020.[44] *public agency* dalam PDPA didefinisikan sebagai pemerintah, pengadilan terkait, serta badan hukum spesifik yang diatur dalam *Gazette* oleh menteri.[45]

Dasar untuk menilai apakah suatu *data breach* termasuk ke dalam *notifiable data breach* disebutkan dalam *Advisory Guidelines On Key Concepts In The PDPA (Revised 1 February 2021)* yang mengatakan bahwa *data breach* tersebut haruslah dalam lingkup yang signifikan dengan kriteria minimal data

41 Article 24 Singapore Personal Data Protection (Amendment) Act 2020.

42 Article 26A Singapore Personal Data Protection (Amendment) Act 2020

43 Article 26C dan 26D Singapore Personal Data Protection (Amendment) Act 2020.

44 Article 26C dan 26E Singapore Personal Data Protection (Amendment) Act 2020.

45 Personal Data Protection Commission Singapore, *Op.Cit*., hlm. 24.

pribadi dari lima ratus atau lebih individu. Apabila *data controller* tidak dapat memberikan estimasi yang sebenarnya, tetapi terdapat kemungkinan bahwa *data breach* tersebut berdampak pada setidaknya lima ratus individu, maka *data breach* yang terjadi termasuk ke dalam *notifiable data breach*.[46]

Terhadap *data breach* yang terjadi, terdapat pengaturan terkait pidana denda yang dijatuhkan kepada *data controller* dan *data intermediary* yang tidak menjalankan kewajibannya berdasarkan *Part III, IV, V, VI, VIA,* ataupun *VIB* PDPA 2020. Pidana denda tersebut diatur maksimal sebanyak $1.000.000,00 (satu juta dollar singapura) sesuai ketentuan Pasal 48J PDPA 2020. Meskipun telah diatur maksimal, terdapat kemungkinan untuk dijatuhkan denda yang lebih tinggi dari yang diatur. Hal tersebut ditujukan atas kasus pelanggaran terhadap PDPA 2020 yang serius sehingga PDPC memiliki fleksibilitas dalam menentukan denda.[47]

2. *DATA BREACH* TOKOPEDIA

Pada Maret 2020, Tokopedia mengalami *data breach*. Dalam peristiwa ini, sebanyak kurang lebih 15 juta data pengguna telah diperjualbelikan di suatu situs.[48] Dalam perkembangannya, pada bulan Juli 2020, Akun Cellibis membagikan 91 juta data pengguna Tokopedia dalam suatu laman grup di Facebook. Sesuai dengan ketentuan yang berlaku, Tokopedia menyurati para pelanggannya terkait dengan kebocoran data.[49] Kebocoran data ini lantas menimbulkan reaksi dari kalangan konsumen.

Komunitas Konsumen Indonesia **("KKI")** melalui kuasa hukumnya, yaitu Akhmad Zaenuddin mengajukan gugatan terhadap Tokopedia ke Pengadilan Negeri Jakarta Pusat perihal Perbuatan Melawan Hukum dengan No. Pendaftaran Online: PN JKT.PST-0520201XD pada 6 Mei 2020. Berdasarkan keterangan Ketua KKI David Tobing, gugatan tersebut diajukan berdasarkan kesalahan dari Tokopedia sebagai Penyelenggara Sistem Elektronik dalam menyimpan dan melindungi kerahasiaan data pribadi serta hak privasi akun dari para pengguna Tokopedia yang diperjualbelikan.[50] Di sisi lain, kalangan pengusaha menganggap Tokopedia adalah korban dari kebocoran data pengguna.

Ketua Umum Asosiasi E-commerce Indonesia **("IdEA")**, Ignatius Untung, mengaku prihatin terhadap kejadian yang menimpa Tokopedia serta para penggunanya. Akan tetapi, ia menyatakan bahwa Tokopedia juga merupakan korban dalam kejadian ini.[51] Dilansir melalui situs Alibaba cloud, Tokopedia saat ini menjalankan infrastruktur Teknologi Informasi mereka pada tiga lokasi:

---

46 *Ibid*., hlm. 140.

47 Personal Data Protection Commission Singapore, "ADVISORY GUIDELINES ON ENFORCEMENT OF THE DATA PROTECTION PROVISIONS", https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-Enforcement-of-DP-Provisions-1-Feb-2021.pdf?la=en, diunduh 3 Mei 2021.

48 CNN Indonesia, "15 Juta Akun Pengguna Tokopedia Diisukan Bocor", https://www.cnnindonesia.com/teknologi/20200502203806-185-499449/15-juta-akun-pengguna-tokopedia-diisukan-bocor, diunduh 1 Mei 2021.

49 Kompas.com, "CEO Tokopedia Surati Pengguna Pasca Kebocoran Data Begini Isinya", https://tekno.kompas.com/read/2020/05/12/17250087/ceo-tokopedia-surati-pengguna-pasca-kebocoran-data-begini-isinya?page=all, diunduh 1 Mei 2021.

50 Hukumonline, "Kasus Bocornya Data Pribadi Konsumen Tokopedia Berujung Ke Meja Hijau", https://www.hukumonline.com/berita/baca/lt5eb331b39427b/kasus-bocornya-data-pribadi-konsumen-tokopedia-berujung-ke-meja-hijau/ , diunduh 3 Mei 2021.

51 Noverius Laoli, "Asosiasi E-Commerce Sebut Tokopedia Merupakan Korban Kebocoran Data Pengguna", https://industri.kontan.co.id/news/asosiasi-e-commerce-sebut-tokopedia-merupakan-korban-ats-kebocoran-data-pengguna, diunduh 5 Mei 2021.

Alibaba Cloud Singapura, AWS Singapura, serta Biznet Jakarta.[52]

a. *Data Breach* Tokopedia Ditinjau Berdasarkan Pengaturan Pelindungan Data Pribadi di Indonesia

Pada kasus ini, data yang bocor dalam kasus ini termasuk nama dan alamat email, tanggal lahir, hobi, pendidikan, kode aktivasi *email*, kode *reset password*, detail lokasi, *ID messenger*, *hash password*, waktu pembuatan akun, hingga waktu terakhir *log-in*.[53] Data tersebut termasuk dalam definisi data pribadi dalam PP PSTE, yakni setiap data seseorang yang secara langsung ataupun tidak langsung, sendiri maupun dikombinasi dengan informasi lainnya, serta teridentifikasi dan/atau dapat diidentifikasi melalui Sistem Elektronik.

Dalam hal ini, Tokopedia tetap bertanggungjawab terhadap terjadinya kebocoran data ini atas dasar asas *presumed liability* dalam Pasal 15 UU ITE 2008. Lebih lanjut, berdasarkan PP PMSE, dalam kasus ini Tokopedia dikategorikan sebagai PPMSE, yakni Pelaku Usaha penyedia sarana Komunikasi Elektronik yang digunakan untuk transaksi Perdagangan. Sementara, Pasal 22 ayat (3) PP PMSE menyatakan bahwa pihak yang melakukan penyediaan ruangan untuk penempatan, pemuatan, atau penyimpanan informasi termasuk dalam Penyelenggara Sarana Perantara. Jika dikaitkan dengan kasus kebocoran data Tokopedia, maka pihak yang melakukan pekerjaan penempatan, pemuatan atau penyimpanan data pribadi, yakni Alibaba Cloud Singapura, AWS Singapura, serta Biznet Jakarta, dapat dikatakan sebagai Penyelenggara Sarana Perantara.

Terkait dengan pelindungan data pribadi, tidak terdapat perbedaan kewajiban antara PPMSE dan Penyelenggara Sarana Perantara. Keduanya, berdasarkan Pasal 59 disamakan kewajibannya dengan penyebutan klausul "Pelaku Usaha". Pasal ini mengatur mengenai kewajiban untuk memenuhi kaidah pelindungan data pribadi secara umum yang merujuk kepada standar pelindungan data Eropa dan/atau APEC Privacy Frameworks. Selanjutnya, dalam Pasal 36 Permenkominfo 20/2016, diatur bahwa setiap orang yang melanggar ketentuan dalam Peraturan Menteri tersebut dapat dikenakan sanksi:

> "*(1) Setiap Orang yang memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan data pribadi tanpa hak atau tidak sesuai dengan ketentuan dalam Peraturan Menteri ini atau peraturan perundang-undangan lainnya dikenai sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan berupa:*
>
> *a. peringatan lisan;*
> *b. peringatan tertulis;*
> *c. penghentian sementara kegiatan; dan/atau*
> *d. pengumuman di situs dalam jaringan (website online).*"

Penggunaan klausula "setiap orang" dalam pasal ini berarti setiap orang, tidak

---

52 Alibaba Cloud, "Tokopedia", https://www.alibabacloud.com/id/customers/tokopedia, diakses pada 1 Mei 2021.

53 Kompas.com "Kebocoran Data 15 Juta Pengguna Pengakukan Tokopedia dan Analisis Ahli", https://tekno.kompas.com/read/2020/05/03/03330087/kebocoran-data-15-juta-pengguna-pengakuan-tokopedia-dan-analisis-ahli?page=all, diunduh 1 Mei 2021.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

terbatas pada Penyelenggara Sistem Elektronik, dapat diberikan sanksi administratif jika melakukan pelanggaran terhadap ketentuan Peraturan Menteri tersebut. Hal ini berarti siapapun yang tanpa hak atau tidak sesuai dengan ketentuan perundang-undangan memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan data pribadi dapat dikenakan sanksi administratif.

Dalam kasus ini, tersebarnya data dari pengguna Tokopedia dapat dikatakan melanggar Pasal 36 Permenkominfo 20/2016. Berdasarkan pasal tersebut, tidak hanya Tokopedia saja yang dapat dikenakan sanksi, tetapi juga layanan *hosting* tempat pengumpulan, pengolahan, penyimpanan data pribadi.

b. *Data Breach* Tokopedia Ditinjau Berdasarkan *Personal Data Protection (Amendment) Act 2020* Singapura

Pada *data breach* Tokopedia, terdapat dua pihak utama yang bertanggung jawab atas insiden yang terjadi, yakni Tokopedia sebagai *data controller* yang mengendalikan data-data milik pengguna Tokopedia dan Alibaba Cloud Singapura, AWS Singapura, serta Biznet Jakarta sebagai *data intermediaries* yang memproses data-data pribadi pengguna Tokopedia. Tidak disebutkan dengan jelas apakah kebocoran data tersebut dari data pribadi yang memang diproses oleh ketiganya atau dari salah satu *data intermediaries* yang bekerja sama dengan Tokopedia. Kebocoran data tersebut memenuhi unsur akses, pengumpulan, penggunaan, penyebaran, dan penyalinan data-data pribadi pengguna Tokopedia sehingga termasuk ke dalam unsur-unsur *data breach* pada Pasal 26A PDPA 2020.[54]

Data-data yang terekspos dalam insiden ini adalah nama dan alamat email, tanggal lahir, hobi, pendidikan, kode aktivasi *email*, kode *reset password*, detail lokasi, *ID messenger*, *hash password*, waktu pembuatan akun, hingga waktu terakhir *log-in*. Apabila dikaitkan dengan Pasal 2 PDPA 2020, dapat dikatakan bahwa pengguna Tokopedia dapat diidentifikasi berdasarkan data tersebut sehingga ia termasuk ke dalam ruang lingkup personal data.[55] Hal ini didasarkan atas dapat diidentifikasinya individu dengan mengetahui data-data tersebut serta sejak awal memang informasi dari data tersebut ditujukan untuk mengidentifikasi individu. Berdasarkan pemaparan di atas, dapat disimpulkan bahwa data yang terekspos dalam data breach ini adalah data pribadi dari para pengguna Tokopedia.

Setelah ditemukan bahwa telah terjadi *data breach* dengan adanya penjualan terkait data-data pribadi yang dikontrol oleh Tokopedia, timbul permasalahan mengenai apakah *data intermediaries* tidak mengetahui terjadinya *data breach* karena memang data tersebut tidak diproses oleh ketiganya secara bersamaan atau tidak memberikan notifikasi kepada Tokopedia selaku *data controller*. Hal ini berkaitan dengan kewajiban *data intermediaries* untuk memberikan notifikasi bahwa telah terjadi *data breach* terkait data yang dikelola atas kepentingan Tokopedia sebagai *data controller*. Jika tidak terdapat notifikasi yang diberikan dari *data intermediaries*, terjadi pelanggaran terhadap Pasal 26C dan 26E PDPA yang mengharuskan

[54] Article 26A Singapore Personal Data Protection (Amendment) Act 2020.

[55] Article 2 Singapore Personal Data Protection (Amendment) Act 2020.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

data intermediaries memberikan notifikasi kepada *data controller* dan *public agency*.[56]

Perihal kewajiban untuk *data controller* sendiri dalam terjadinya *data breach* ini telah dipenuhi oleh pihak Tokopedia. Setelah diketahui terjadi *data breach*, pihak Tokopedia memberitahukan dan bekerja sama dengan pemerintah. Sebelum itu juga, Pihak Tokopedia telah menjalankan proses investigasi serta melakukan langkah-langkah yang diperlukan dalam memastikan keamanan akun dan transaksi dari para penggunanya. Pihak Tokopedia selain memberitahukan terkait *data breach* ini kepada pemerintah, ia juga memberitahukan *data breach* yang dialaminya kepada pengguna Tokopedia. Tindakan dari pihak Tokopedia tersebut telah memenuhi ketentuan Pasal 26D PDPA, yakni memberikan notifikasi kepada *commission*, dimana dalam hal ini adalah pemerintah serta kepada masing-masing individual yang terdampak *data breach*.[57]

Terjadinya *data breach* terhadap data yang dikontrol Tokopedia ini hingga saat ini dapat dikatakan tidak terdapat pelanggaran berdasarkan PDPA 2020 oleh Tokopedia sebagai *data controller*, tetapi terdapat kemungkinan pelanggaran oleh *data intermediaries*, yakni Alibaba Cloud Singapura, AWS Singapura, serta Biznet Jakarta. Hal ini disebabkan Tokopedia tidak mengetahuinya sendiri, melainkan setelah adanya penjualan terkait data pribadi pengguna Tokopedia. Selain itu, terdapat kemungkinan bahwa *data intermediaries* tidak melaksanakan kewajibannya dengan memberitahukan kepada Tokopedia selaku *data controller* bahwa telah terjadi *data breach* atau *data intermediaries* tidak mengetahui telah terjadi *data breach* sehingga tidak dapat memberikan notifikasi terjadinya *data breach* kepada Tokopedia selaku *data controller*. Oleh karena itu, dapat dikatakan bahwa terdapat kemungkinan hanya terjadi pelanggaran oleh *data intermediaries*, yakni BizNet Jakarta, Alibaba Cloud Singapura, dan AWS Singapura dengan tidak memenuhi kewajibannya dalam memberikan notifikasi kepada Tokopedia selaku *data controller*.

D. Penutup

Konsep pelindungan data pribadi di dunia diawali dengan konsep privasi itu sendiri, dimana muncul prinsip pelindungan data pribadi yang dinamakan FIP sebagai prinsip-prinsip yang mengatur hubungan antara bisnis dan pemerintah yang mengumpulkan, menggunakan, dan membuka informasi personal mengenai subjek data. Kemudian, pada tahun 2016 muncul EU GDPR 2016 sebagai *golden rule* yang memengaruhi aturan-aturan negara lainnya seperti Singapura. Meskipun Singapura telah membuat Personal Data Protection Act pada 2012, ia tetap melakukan amandemen pada tahun 2020 yang menghasilkan PDPA 2020 dengan isi yang menyerupai EU GDPR 2016 seperti adanya pengaturan mengenai *data controller* dan *data intermediary/processor* dan tanggung jawab keduanya dalam hal terjadi *data breach*. Hal ini berbeda dengan peraturan perihal pelindungan data pribadi di Indonesia yang ada pada saat ini masih terbagi-bagi dalam beberapa peraturan. Di dalamnya, tidak diatur dengan jelas konsep *data controller* dan *data processor* sehingga tidak terdapat perbedaan antara penyelenggara sistem elektronik yang melakukan kontrol dan kelola atas data pribadi serta tidak terdapat pengaturan

[56] Article 26C dan 26E Singapore Personal Data Protection (Amendment) Act 2020.

[57] Article 26D Singapore Personal Data Protection (Amendment) Act 2020.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

perihal *data breach*. Hal ini berbeda dengan Singapura dalam PDPA 2020 yang telah membagi dengan jelas antara *data controller* dan *data intermediary* sehingga terdapat perbedaan kewajiban dan pertanggungjawaban di antara keduanya dalam hal terjadi *data breach*.

Sebaiknya, peraturan terkait pelindungan data pribadi di Indonesia dibuat dalam bentuk Undang-Undang yang berisi aturan secara komprehensif perihal pelindungan data pribadi, dimana aturan ini akan mencakup pihak-pihak yang mengumpulkan, menggunakan, serta mengelola data pribadi itu sendiri seperti PDPA 2020. Dengan adanya satu aturan yang berbentuk Undang-Undang mengakibatkan adanya payung hukum yang dengan pasti menjamin pelindungan data pribadi di Indonesia. Hal ini mengakibatkan apabila terjadi *data breach*, dapat dipertanggungjawabkan terjadinya *data breach* tersebut terhadap *data controller* dan/atau *data processor* yang mengalaminya.

Daftar Pustaka

Buku

Sharma, Sanjay, *Data Privacy and GDPR Handbook*, Cet. 1, Canada: John Wiley & Sons, Inc, 2020.

Soerjono Soekanto, *Pengantar Penelitian Hukum*, UI Press, Jakarta, 1986.

Voigt, Paul dan Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A Practical Guide*, Springer International Publishing AG, Switzerland, 2017.

Walters, Robert, Leon Trakman, dan Bruno Zeller, *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches*, Singapura: Springer Nature Singapore Pte Ltd, 2019.

Artikel Dalam Buku

Tavani, Herman T., "Informational Privacy: Concepts, Theories, and Controversies" dalam buku The Handbook of Information and Computer Privacy, yang disusun oleh Kenneth Einar Himma dan Herman T. Tavani, Hoboken: John Wiley & Sons, 2008.

Artikel Jurnal

Anggraeni, Setyawati Fitri, "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum di Indonesia", *Jurnal Hukum dan Pembangunan*, Volume 48, Issue 4, 2018.

Chik, Warren B., "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform", *Computer Law and Security Review*, Volume 29, No. 5, Oktober 2013.

Kokott, Juliane dan Christoph Sobotta, "The Distinction Between Data Privacy and Data Protection in The Jurisprudence of The CJEU and The ECtHR", *International Data Privacy Law*, Volume 3, Issue 4, 2013.

Moor, James H., "Towards a Theory of Privacy in the Information Age", *ACM SIGCAS Computers and Society*, Volume 27, Issue 3, September 1997.

Reidenberg, Joel R., "Setting Standards for Fair Information Practice in the U.S. Private Sector", *Iowa Law Review*, Volume 80, Issue 497, 1995.

Whitley, Edgar A., "Informational Privacy, Consent and The ''Control'' of Personal Data", Information Security Technical Report, Volume 14, Issue 3, Agustus 2009.

Internet

Alibaba Cloud, "Tokopedia", https://www.alibabacloud.com/id/customers/tokopedia, diakses pada 1 Mei 2021.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

CNN Indonesia, "15 Juta Akun Pengguna Tokopedia Diisukan Bocor", https://www.cnnindonesia.com/teknologi/20200502203806-185-499449/15-juta-akun-pengguna-tokopedia-diisukan-bocor, diunduh 1 Mei 2021.

Edmon Makarim, "Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi", https://www.hukumonline.com/berita/baca/lt5f067836b37ef/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-oleh--edmon-makarim?page=2, diunduh 2 Mei 2021.

Hukumonline, "Kasus Bocornya Data Pribadi Konsumen Tokopedia Berujung Ke Meja Hijau", https://www.hukumonline.com/berita/baca/lt5eb331b39427b/kasus-bocornya-data-pribadi-konsumen-tokopedia-berujung-ke-meja-hijau/ , diunduh 3 Mei 2021.

Kompas.com, "CEO Tokopedia Surati Pengguna Pasca Kebocoran Data Begini Isinya", https://tekno.kompas.com/read/2020/05/12/17250087/ceo-tokopedia-surati-pengguna-pasca-kebocoran-data-begini-isinya?page=all, diunduh 1 Mei 2021.

Kompas.com "Kebocoran Data 15 Juta Pengguna Pengakukan Tokopedia dan Analisis Ahli", https://tekno.kompas.com/read/2020/05/03/03330087/kebocoran-data-15-juta-pengguna-pengakuan-tokopedia-dan-analisis-ahli?page=all, diunduh 1 Mei 2021.

Noverius Laoli, "Asosiasi E-Commerce Sebut Tokopedia Merupakan Korban Kebocoran Data Pengguna", https://industri.kontan.co.id/news/asosiasi-e-commerce-sebut-tokopedia-merupakan-korban-ats-kebocoran-data-pengguna, diunduh 5 Mei 2021.

Personal Data Protection Commission Singapore, "ADVISORY GUIDELINES ON ENFORCEMENT OF THE DATA PROTECTION PROVISIONS (Revised 1 February 2021)", https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-Enforcement-of-DP-Provisions-1-Feb-2021.pdf?la=en, diunduh 3 Mei 2021.

Personal Data Protection Commission Singapore, "ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PDPA (Revised 1 February 2021)", https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en, diunduh 3 Mei 2021.

Peraturan Perundang-Undangan

European Union General Data Protection Regulation 2016.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Penyelenggara Perdagangan Melalui Sistem Elektronik.

Singapore Personal Data Protection (Amendment) Act 2020.

Undang-Undang Dasar Negara Republik Indonesia 1945.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.