

# PENGATURAN PERLINDUNGAN DATA PRIBADI KONSUMEN JASA KEUANGAN DALAM PENGGUNAAN UANG ELEKTRONIK BERBASIS *SERVER*

Sukarelawati Permana

Mahasiswa Program Doktor Ilmu Hukum, Universitas Katolik Parahyangan  
email: 2017822022@student.unpar.ac.id

disampaikan 06/09/2021 – di-review 07/09/2021 – diterima 08/12/2022  
DOI: 10.25123/vej.v8i2.5213

## **Abstract**

*The digitalization of the economy in Indonesia in the Covid-19 pandemic situation has further encouraged banks and business actors to make innovations in order to reduce direct contact with consumers of financial services, one of which is the presence of server-based electronic money. Users who use these services are required to fill in their personal data first. With the provision of personal data belonging to consumers of financial services or users, the issuer of server-based electronic money has an obligation to protect users' personal data so that unauthorized dissemination or misuse of data does not occur. The widespread use of server-based electronic money in public activities makes provisions related to the protection of personal data important in order to protect users. However, it is necessary to examine whether the provisions on the protection of personal data of financial service consumers on server-based electronic money have met best practices. To answer these problems, research was conducted using normative juridical methods sourced from library materials. The results of the research obtained are the protection of personal data of consumers of financial services on server-based electronic money has been regulated in regulations that aim to protect users' personal data. The regulation has adopted the principles of personal data regulation as well as the General Data Protection Regulation (GDPR) and the existing laws and regulations in Indonesia. These regulations play a role in protecting the rights of users regarding their personal data such as the right to assimilate or withdraw the consent that has been given previously.*

## **Keywords:**

*personal data; electronic money; data protection regulations*

## **Abstrak**

Digitalisasi perekonomian di Indonesia dalam situasi pandemi Covid-19 mendorong perbankan maupun pelaku usaha membuat inovasi demi mengurangi kontak langsung. Salah satunya adalah dengan mengembangkan uang elektronik berbasis *server*. Pada saat yang sama, penggunaan uang elektronik berbasis *server* ini akan menjadi tempat terkumpulnya data pribadi pelanggan-pengguna. Sebaliknya pengelola berkewajiban menjaga dan melindungi data pribadi pelanggan. Persoalan yang ditelaah di sini adalah seberapa jauh ketentuan hukum yang ada secara efektif memberikan perlindungan terhadap data pribadi. Penelusuran menunjukkan bahwa ketentuan tentang perlindungan data pribadi di Indonesia tidak hanya merujuk pada peraturan perundang-undangan yang ada namun khususnya pada *General Data Protection Regulation* yang sebenarnya diterbitkan dan diberlakukan untuk Uni Eropa.

## **Kata Kunci:**

data pribadi; uang elektronik; peraturan mengenai perlindungan data pribadi

## Pendahuluan

Adanya perkembangan industri 4.0 sejalan dengan perkembangan teknologi, memberikan dampak positif bagi perekonomian suatu negara. Kehadiran teknologi digital mendorong perekonomian negara menjadi ke arah ekonomi digital. Di Indonesia perkembangan ekonomi digital didukung oleh banyaknya jumlah pengguna internet. Ditambah lagi dengan kondisi pandemi Covid-19 yang saat ini semakin mendorong pertumbuhan ekonomi digital di Indonesia.

Perkembangan teknologi pada sektor perekonomian saat ini menunjukkan bahwa kebutuhan yang ada di masyarakat tidak hanya dapat dilayani sebatas tatap muka (secara tradisional) saja. Namun, yang terjadi ialah adanya tuntutan bahwa layanan atas kebutuhan masyarakat sekarang ini dapat diakses secara tanpa harus dilakukan tatap muka (secara *online*). Sepanjang tahun 2020, terdapat 64 juta unit Usaha Mikro Kecil dan Menengah (UMKM) yang sudah menggunakan *platform* digital dalam kegiatan usahanya. Bahkan sampai kuartal 2021 ini, telah terdapat penambahan di mana 11 juta unit UMKM baru yang menjadikan *platform* digital sebagai media yang mendukung kegiatan usahanya.<sup>1</sup>

Bentuk-bentuk *platform* digital yang banyak digunakan antara lain ialah media sosial, dompet elektronik atau *e-wallet*, *e-commerce*, layanan perbankan, layanan investasi, layanan pinjaman, dan lainnya. Untuk menggunakan *platform digital* tersebut, pengguna diharuskan untuk memberikan data pribadi seperti nama, usia, jenis kelamin, alamat, nomor *handphone*. Bahkan pada beberapa *platform*, meminta pengguna untuk memberikan identitas diri seperti contohnya Kartu Tanda Penduduk (KTP), Surat Izin Mengemudi (SIM), Nomor Pokok Wajib Pajak (NPWP), dan lain-lain.

Salah satu *platform* digital yang saat ini marak digunakan ialah uang elektronik. Dengan adanya uang elektronik, pengguna atau konsumen jasa keuangan dapat melakukan transaksi pembayaran ataupun transfer uang tanpa perlu pergi ke bank atau bertemu langsung dengan orang yang bersangkutan.

---

<sup>1</sup> Putra Ananda, Pandemi Covid-19 Membuat Ekonomi Digital Indonesia Tumbuh Pesat, <https://mediaindonesia.com/ekonomi/397976/pandemi-covid-19-membuat-ekonomi-digital-indonesia-tumbuh-pesat>, diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

Merujuk pada data statistik yang dikeluarkan oleh Bank Indonesia untuk tahun 2021, jumlah uang elektronik yang beredar per-Juli 2021 ialah sebanyak 495.280.424 instrumen. Meskipun jumlah tersebut turun jika dibandingkan pada bulan Mei 2021 yang sebanyak 498.202.416 dan bulan Juni 2021 sejumlah 511.254.525 instrumen namun, jumlah tersebut mengalami peningkatan dari tahun-tahun sebelumnya yang mana pada tahun 2020 sebanyak 432.281.380 instrumen dan tahun 2019 sejumlah 292.299.320 instrumen.<sup>2</sup>

Mudahnya penggunaan *platform* digital diiringi pemberian data pribadi pengguna menjadikan pengguna semakin rentan terhadap pelanggaran data pribadi. Di Indonesia sendiri, kasus pelanggaran data pribadi terjadi dalam bentuk adanya jual beli data pribadi, penggelapan saldo rekening milik nasabah, dan penipuan lainnya yang mengatasnamakan data pribadi milik pihak lain.<sup>3</sup> Sehubungan dengan hal tersebut, perlu adanya pengaturan yang mengatur perihal perlindungan data pribadi tidak hanya sebatas pada transaksi *offline* tetapi juga terhadap transaksi *online* seperti pada transaksi uang elektronik. Kasus terkait kebocoran data pribadi di Indonesia sendiri telah terjadi pada beberapa kali seperti pada Juli 2021, yang dalam hal ini terdapat sebanyak 463.000 dokumen milik nasabah BRI Life (foto KTP, nomor rekening, nomor wajib pajak, akta lahir, maupun rekam medis) yang diperjualbelikan. Selanjutnya, kasus yang terbaru ialah sebanyak 1,3 juta data pengguna *electronic Health Alert Card* (eHAC) yang ditemukan di *server* yang dapat diakses semua orang.<sup>4</sup>

Penelitian ini dilakukan dengan menggunakan metode yuridis normatif untuk mengkaji permasalahan mengenai pengaturan perlindungan data pribadi konsumen jasa keuangan pada uang elektronik berbasis *server* di Indonesia serta

---

<sup>2</sup> Bank Indonesia, Jumlah Uang Elektronik Beredar Tahun 2021, <https://www.bi.go.id/id/statistik/ekonomi-keuangan/ssp/uang-elektronik-jumlah.aspx>, diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

<sup>3</sup> CNN Indonesia, Menkominfo: Kasus Pelanggaran Data Pribadi Sulit Terdeteksi, <https://www.cnnindonesia.com/teknologi/20200225204935-185-478090/menkominfo-kasus-pelanggaran-data-pribadi-sulit-terdeteksi>, diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

<sup>4</sup> Caesar Akbar, 6 Kasus Kebocoran Data Pribadi di Indonesia, <https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia>, diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

untuk mengetahui apakah pengaturan perlindungan tersebut telah sesuai dengan *best practice*. Selain itu, penelitian ini juga mengkaji praktek perlindungan data pribadi dari uang elektronik berbasis *server* yang dijalankan dengan adanya kebijakan privasi dari masing-masing penyedia layanan serta hak dan kewajiban yang dimiliki oleh pemilik data pribadi maupun penyelenggara dari uang elektronik berbasis *server*.

## Pembahasan

### Data Pribadi dan Perlindungan Data

Definisi data pribadi ialah segala informasi yang memiliki kaitan dengan perorangan yang dapat dilakukan identifikasi atau teridentifikasi (*data subject*); perorangan yang dapat dilakukan identifikasi ialah seseorang yang teridentifikasi baik langsung maupun tidak, yang secara khusus ditunjukkan melalui penanda yaitu nama, nomor identitas, lokasi dari data, identifikasi *online* atau faktor-faktor spesifik seperti fisik, psikologis, *genetic*, mental, ekonomi, budaya atau identitas sosial yang berasal dari perorangan tersebut.<sup>5</sup>

Lebih jauh, menurut Orla Lynskey<sup>6</sup>, terdapat dua perbedaan mengenai data dalam ruang lingkup “data pribadi” dan *privacy*: Pertama, tidak seperti gagasan “gangguan privasi”, gagasan tentang “data pribadi” tidak tergantung pada konteks. Kedua, pengertian tentang data pribadi termasuk data yang berkaitan dengan individu yang tidak dikenal namun dapat diidentifikasi. Richard Murphy mendefinisikan ruang lingkup informasi pribadi sebagai terdiri dari “setiap data tentang seorang individu yang dapat diidentifikasi oleh individu tersebut”. Namun demikian definisi Murphy terlalu luas karena ada sejumlah besar informasi yang dapat diidentifikasi kepada kita dan yang kita lakukan. Perlindungan Data pribadi merupakan hak asasi manusia sebagai bagian dari hak *privacy* yang mendapatkan

---

<sup>5</sup> Article 4 paragraph 1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)) (EU 2016/679).

<sup>6</sup> Orla Lynskey, “Deconstructing Data Protection: the ‘Added-Value’ of a Right to Data Protection in the EU Legal Order”. *International and Comparative Law Quarterly*, (2014) 63 (3). pp. 569-59.

jaminan perlindungan baik instrument hukum internasional dan konstitusi negara. Dari pengertian data pribadi di atas, dapat terlihat bahwa seseorang yang dapat diidentifikasi adalah seseorang yang dapat dikenali/diidentifikasi secara langsung maupun tidak langsung berdasarkan nomor tanda pengenal atau berdasarkan satu atau lebih faktor spesifik dari identifikasi fisik, psikologi, mental, budaya atau sosial. Entitas yang dilindungi dalam mekanisme perlindungan data pribadi adalah “orang perorangan” (natural person) bukan “badan hukum” (legal person).

Ketentuan mengenai data pribadi saat ini masih berada dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Dalam UU ITE tersebut hanya dicantumkan satu pasal terkait perlindungan data pribadi, yang mengatur bahwa penggunaan informasi yang dilakukan melalui media elektronik dengan kaitannya data pribadi seseorang, wajib untuk dilakukan atas dasar adanya persetujuan dari pihak tersebut.<sup>7</sup> Turunan dari UU ITE tersebut dibuat Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang merupakan pengaturan lanjut perihal data pribadi. Selain itu, terdapat Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik yang masih berlaku, yang merupakan turunan dari Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagai peraturan pemerintah sebelumnya.

Lebih lanjut, ketentuan mengenai data pribadi di Indonesia mulai dirancang untuk dimuat dalam undang-undang tersendiri. Draft Rancangan Undang-Undang Perlindungan Data Pribadi (RUU Perlindungan Data Pribadi) 2020 (Januari), memberikan definisi data pribadi yaitu seluruh data yang berkaitan dengan seseorang baik yang teridentifikasi maupun dapat diidentifikasi baik secara tersendiri atau dikombinasi dengan informasi lainnya yang dilakukan secara langsung maupun tidak, dengan penggunaan sistem elektronik maupun

---

<sup>7</sup> Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

nonelektronik.<sup>8</sup> Perumusan RUU Perlindungan Data Pribadi ini dilakukan sebagai salah satu bentuk perwujudan hak asasi manusia terkait perlindungan diri pribadi. Selain itu pula RUU ini merupakan bentuk jaminan hak warga negara atas perlindungan diri pribadinya, menumbuhkan serta meningkatkan kesadaran masyarakat, dan menjamin adanya pengakuan serta penghormatan mengenai pentingnya perlindungan data pribadi.<sup>9</sup>

Data pribadi dan perlindungan data memiliki perbedaan yaitu:<sup>10</sup>

- a. Data pribadi berkaitan dengan siapa atau pihak mana yang secara sah memiliki akses data tersebut atau berkaitan dengan hak dan kepentingan dari pemilik data, pengendali data<sup>11</sup>, dan prosesor data. Sementara perlindungan data berfokus pada upaya-upaya perlindungan data atau juga melindungi data dari upaya akses yang tidak sah.
- b. Data pribadi titik beratnya ialah terhadap hukum dan proses<sup>12</sup>, sementara perlindungan data titik beratnya ialah control atas keamanan dari data atau *technical control*<sup>13</sup>.
- c. Pada data pribadi terjadi kontrol terhadap data apa saja yang dapat dibagikan ke siapa atau pihak mana oleh pemilik data tersebut. Sementara itu, dalam perlindungan data yang terjadi ialah kontrol atas hal-hal yang berkaitan dengan perlindungan data pribadi oleh organisasi atau perusahaan.
- d. Fokus dari data pribadi ialah terkait risiko adanya penjualan ataupun terjadinya penyebaran yang tidak sah atau tanpa izin dari pemilik data pribadi. Sementara

---

<sup>8</sup> Pasal 1 angka 1 Draf Rancangan Undang-Undang tentang Perlindungan Data Pribadi 2020 (Januari).

<sup>9</sup> Bagian Pertimbangan dalam Draf Rancangan Undang-Undang tentang Perlindungan Data Pribadi 2020 (Januari).

<sup>10</sup> Oktarina Paramitha Sandy, Mengenal Perbedaan *Data Privacy* dan *Data Protection*, <https://m.cyberthreat.id/read/8878/Mengenal-Perbedaan-Data-Privacy-dan-Data-Protection>, diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

<sup>11</sup> Pengendali data adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan data pribadi (Pasal 1 angka 3 Rancangan Undang-Undang Perlindungan Data Pribadi).

<sup>12</sup> Bisa dalam bentuk proses tata kelola dan kepatuhan terhadap aspek kontraktual dan regulasi yang berlaku.

<sup>13</sup> Bentuk implementasi teknologi seperti implementasi solusi *encryption*, *data loss/leakage prevention*, *tokenization*, *anonymization*, dan lain-lain.

itu, perlindungan data memiliki fokus pada cara-cara yang dapat dilakukan guna menghindari risiko terjadinya peretasan.

### ***General Data Protection Regulation (GDPR)***

Pengaturan mengenai data pribadi terdapat dalam *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* atau yang dikenal juga sebagai *General Data Protection Regulation (GDPR)*. Ketentuan yang ada di GDPR berlaku bagi individu, perusahaan atau organisasi yang melakukan kegiatan penyimpanan, pengolahan atau pemrosesan data pribadi atas penduduk yang ada di Uni Eropa. Tujuan dari dibuatnya GDPR sendiri ialah untuk melindungi data pribadi seseorang yang diperoleh perusahaan agar tidak dipergunakan oleh pihak-pihak lain yang tidak memiliki kewenangan atas data tersebut secara semena-mena. Menurut GDPR, data pribadi yang dikontrol ialah:<sup>14</sup>

- a. Informasi dasar contohnya ialah nama, nomor identitas, alamat;
- b. Data *website* yang digunakan misalnya seperti lokasi, *cookie*, alamat IP, *Radio Frequency Identification (RFID)*;
- c. Data kesehatan dan genetik;
- d. Data biometrik;
- e. Data etnis dan ras;
- f. Pendapat politik; serta
- g. Orientasi seksual.

Berlakunya ketentuan yang ada di GDPR tidak terbatas hanya di Uni Eropa saja, melainkan juga berlaku terhadap seluruh kegiatan yang melakukan penyimpanan dan pengolahan data pribadi yang ada di Indonesia. Hal ini disebutkan dalam Pasal 3 GDPR yang menyebutkan bahwa ketentuan yang ada di GDPR berlaku pula terhadap kegiatan pemrosesan data pribadi yang berkaitan

---

<sup>14</sup> Libera, Pengaruh GDPR sebagai Perlindungan Data Pribadi & Keberlakuannya bagi Startup, <https://libera.id/blogs/apa-itu-gdpr-dan-keberlakuannya-di-indonesia>, diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

dengan kegiatan pengontrolan ataupun pengolahan baik yang terjadi di Uni Eropa maupun wilayah lain.<sup>15</sup>

Contohnya yang terjadi ialah Google dan Facebook yang sering mengirimkan *email* kepada penggunanya terkait adanya pembaruan kebijakan privasi yang berisi penjelasan mengenai data apa saja yang digunakan oleh perusahaan disertai dengan tujuan dari penggunaannya. Meskipun di dalam GDPR disebutkan bahwa subjek dari ketentuan tersebut ialah penduduk di Uni Eropa, tetapi apabila aplikasi atau situs yang diakses penduduk selain dari Uni Eropa memiliki dan juga melakukan pemrosesan data pribadi, maka aplikasi atau situs tersebut wajib tunduk pada ketentuan yang ada di GDPR. Oleh karena itu, ketentuan tersebut berlaku pula di Indonesia. Dengan berlakunya GDPR, pelaku usaha dapat mengambil tindakan-tindakan yang bertujuan memperbaiki prosedur terkait data pribadi dengan cara melakukan perubahan atas syarat dan ketentuan yang berlaku maupun kebijakan privasi yang ada agar disesuaikan dengan ketentuan di GDPR maupun peraturan perundang-undangan yang ada di Indonesia.<sup>16</sup> Data pribadi yang diatur dalam GDPR diharuskan untuk:<sup>17</sup>

- a. diproses<sup>18</sup> secara hukum, adil dan perlakuan yang transparan berkaitan dengan *data subject* (berdasarkan hukum, adil, dan transparan);
- b. dihimpun dengan tujuan yang spesifik, jelas, dan berdasarkan hukum serta tidak dilaksanakan lebih lanjut dengan perlakuan yang bertentangan dari tujuan-tujuan tersebut; pemrosesan selanjutnya dilakukan demi tercapainya tujuan-tujuan yang berkaitan dengan kepentingan umum, penelitian ilmiah atau sejarah ataupun tujuan statistik yang tidak dianggap bertentangan dari tujuan diawal;

---

<sup>15</sup> Pasal 3 GDPR.

<sup>16</sup> Libera, *supra note* 13.

<sup>17</sup> Pasal 5 ayat (1) GDPR.

<sup>18</sup> Pemrosesan merupakan segala tindakan atau serangkaian tindakan yang dilaksanakan pada data pribadi atau serangkaian data pribadi, secara otomatis maupun tidak, seperti pengumpulan, perekaman, organisasi, penataan, penyimpanan, adaptasi atau perubahan, pengambilan, konsultasi, penggunaan, pengungkapan melalui transmisi, menyebarluaskan atau menyediakan, pembatasan, penghapusan atau penghancuran (Pasal 4 ayat (2) GDPR).

- c. kecukupan, relevansi serta sebatas apa yang dibutuhkan sebagaimana tujuan data tersebut diproses (*data minimisation*);
- d. tepat serta apabila diperlukan, terus dilakukan pembaruan; tindakan-tindakan beralasan harus dilakukan agar menjamin bahwa data pribadi yang bertentangan dengan tujuan dari pemrosesannya itu dilakukan penghapusan atau perbaikan tanpa ditunda (*akurasi*);
- e. disimpan dengan bentuk yang memungkinkan untuk dilakukan identifikasi *data subjects* sebatas pada apa yang dibutuhkan untuk tujuan diprosesnya data pribadi tersebut; penyimpanan data pribadi dapat dilakukan untuk periode yang lebih lama, selama data tersebut diproses dengan tujuan untuk mencapai kepentingan umum, penelitian ilmiah atau sejarah ataupun tujuan statistik berdasarkan pelaksanaan teknis dan tindakan-tindakan organisasi yang dibutuhkan sesuai dengan GDPR dalam hal menjaga hak dan kebebasan dari *data subject (storage limitation)*;
- f. dilakukan pemrosesan dengan memastikan keamanan dari data pribadi tersebut sesuai, termasuk adanya perlindungan atas pemrosesan yang tidak sah atau bertentangan dengan hukum yang ada. Selain itu, penghindaran dari terjadinya kehilangan, kerusakan atau kehancuran data, dengan menggunakan teknis dan tindakan-tindakan organisasi yang sesuai (*integrity and confidentiality*).

### **Pengaturan Perlindungan Data Pribadi di Indonesia**

Perlindungan data pribadi pada uang elektronik berbasis *server* tidak dapat dipisahkan kaitannya dengan perlindungan konsumen, terlebih mengingat banyaknya kegiatan konsumsi barang dan/atau jasa yang saat ini memerlukan pengisian data pribadi milik konsumennya. Perlindungan konsumen sendiri memiliki definisi yaitu segala bentuk usaha yang dilakukan demi menjamin terlaksananya kepastian hukum yang memberikan perlindungan kepada konsumen yang memanfaatkan produk dan/atau jasa. Definisi tersebut tertuang dalam Pasal 1 angka 1 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

dan Pasal 1 angka 3 Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia.

Dalam RUU Perlindungan Data Pribadi, data pribadi dibagi menurut sifatnya yaitu umum dan spesifik. Lebih lanjut, yang dimaksud dengan data pribadi menurut sifatnya yang umum yaitu:<sup>19</sup>

- a. nama lengkap;
- b. jenis kelamin;
- c. kewarganegaraan;
- d. agama; dan/atau
- e. data pribadi yang digabungkan dengan maksud mengidentifikasi seseorang.

Kemudian, data pribadi menurut sifatnya yang spesifik yaitu berupa:<sup>20</sup>

---

<sup>19</sup> Pasal 3 ayat (2) Draf Rancangan Undang-Undang Perlindungan Data Pribadi 2020 (Januari).  
<sup>20</sup> Id., Pasal 3 ayat (3). GDPR memberikan larangan terhadap pemrosesan data pribadi yang menerangkan hal-hal diantaranya ialah ras atau etnik asal, pendapat politik, kepercayaan memeluk agama atau filosofi, atau keanggotaan dalam serikat pekerja, dan pemrosesan data genetik dan biometrik yang bertujuan secara unik mengidentifikasi seseorang, data yang berkaitan dengan kesehatan atau kehidupan ataupun orientasi seksual seseorang (Pasal 9 ayat (1) GDPR). Namun ketentuan tersebut dapat dikecualikan apabila: (Pasal 9 ayat (2) GDPR)

- a. Telah diberikan persetujuan secara eksplisit untuk pemrosesan data pribadi atas satu atau beberapa tujuan tertentu;
- b. Pemrosesan diperlukan dengan tujuan menjalankan kewajiban dan melaksanakan hak-hak tertentu oleh pengendali data pribadi atau *data subject* dibidang ketenagakerjaan dan *social security* dan *social protection law* sepanjang diotorisasi oleh peraturan perundang-undangan;
- c. Pemrosesan diperlukan demi melindungi kepentingan vital dari *data subject* atau perorangan lainnya. Dalam hal ini *data subject* tersebut memiliki ketidakcakapan secara fisik ataupun hukum untuk memberikan persetujuan;
- d. Pemrosesan dilaksanakan dalam rangka kegiatan-kegiatan yang sah dan perlindungan yang sesuai oleh Yayasan, asosiasi atau badan nirlaba dengan tujuan politik, filosofi, keagamaan atau serikat pekerja dan dengan kondisi bahwa pemrosesan semata-mata berkaitan pada anggota atau mantan anggota organisasi atau perorangan yang memiliki kontak rutin sehubungan dengan tujuan organisasi serta data pribadi tidak diungkapkan di luar dari organisasi tanpa adanya persetujuan dari pemilik data pribadi;
- e. Pemrosesan yang secara nyata dipublikasikan oleh pemilik data pribadi;
- f. Pemrosesan yang dilakukan untuk penerbitan, pelaksanaan, atau pembelaan atas tuntutan hukum atau ketika pengadilan bertindak dalam kapasitasnya;
- g. Pemrosesan dilakukan untuk tujuan kepentingan publik dengan dasar peraturan perundang-undangan yang mana proporsional dengan tujuan yang ingin dicapai, menghormati esensi hak atas perlindungan data pribadi dan menyediakan tindakan-tindakan spesifik dan sesuai guna melindungi hak-hak dasar dan kepentingan dari pemilik data pribadi;
- h. Pemrosesan dilakukan dengan tujuan mencegah atau *occupational medicine*, untuk menilai kapasitas kerja dari pekerja, diagnosis medis, penyediaan kesehatan atau

- a. data dan informasi mengenai kesehatan;
- b. data mengenai biometrik;
- c. data terkait genetika;
- d. kehidupan/orientasi seksual;
- e. pandangan politik;
- f. catatan kejahatan;
- g. data anak;
- h. data keuangan pribadi; dan/atau
- i. data lainnya yang berdasarkan peraturan perundang-undangan.

Perlindungan terkait data pribadi mencakup antara lain perlindungan terhadap kegiatan perolehan, pengumpulan, pengolahan, penganalisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan atas data pribadi.<sup>21</sup> Cakupan pemrosesan sebagaimana yang disebutkan tersebut, wajib dilakukan dengan sertifikasi menurut peraturan perundang-undangan yang berlaku.<sup>22</sup> Terdapat beberapa asas dalam perlindungan data pribadi yang baik, antara lain:<sup>23</sup>

- a. adanya penghormatan atas data pribadi sebagai suatu privasi<sup>24</sup>;
- b. data pribadi itu memiliki sifat rahasia sebagaimana yang telah dilakukan persetujuan<sup>25</sup> dan/atau sesuai dengan ketentuan peraturan perundang-undangan;

---

perawatan social atau manajemen sistem dan layanan kesehatan atau perawatan social berdasarkan peraturan perundang-undangan;

- i. Pemrosesan yang dilakukan dengan tujuan kepentingan publik pada area kesehatan public seperti melindungi dari ancaman lintas batas atau menjamin standar yang tinggi berkaitan dengan kualitas dan keamanan perawatan kesehatan dan produk medis atau alat-alat medis;
- j. Pemrosesan yang dilakukan untuk mewujudkan tujuan kepentingan publik, penelitian ilmiah atau historis ataupun tujuan statistik.

<sup>21</sup> Pasal 2 ayat (1) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

<sup>22</sup> Id., Pasal 4.

<sup>23</sup> Id., Pasal 2 ayat (2).

<sup>24</sup> Yaitu kebebasan yang dimiliki oleh setiap pemilik data pribadi dalam mengungkapkan atau tidak perihal rahasia terkait data pribadinya, kecuali hal tersebut ditentukan lain menurut peraturan perundang-undangan yang ada (Id., Pasal 2 ayat (3)).

<sup>25</sup> Persetujuan diberikan ketika pemilik data pribadi telah memberikan konfirmasi atas kebenaran, kedudukan kerahasiaan serta tujuan dari dilakukannya pengelolaan data pribadi (diatur dalam Id., Pasal 2 ayat (4)). Ketentuan mengenai persetujuan dalam Pasal 7 GDPR yang

- c. didasari oleh adanya persetujuan;
- d. keterkaitan dengan tujuan kegiatan yang berupa perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan;
- e. kepatutan dari sistem elektronik yang dipergunakan;
- f. adanya itikad baik dengan segera memberitahukan secara tertulis kepada pemilik data pribadi mengenai kegagalan dalam melaksanakan perlindungan data pribadi;
- g. tersedianya aturan internal yang mengatur mengenai pengelolaan perlindungan data pribadi;
- h. tanggung jawab terhadap data pribadi yang berada pada penguasaan pengguna;
- i. kemudahan terhadap akses maupun koreksi atas data oleh pemilik data pribadi; dan
- j. kepaduan, kecermatan, dan keabsahan<sup>26</sup> serta kemutakhiran data pribadi.

Dalam RUU Perlindungan Data Pribadi terdapat sedikit perbedaan dalam kegiatan pemrosesan data pribadi yang mengatur bahwa pemrosesan ialah kegiatan yang dilakukan untuk memperoleh dan mengumpulkan; mengolah dan menganalisis; menyimpan; memperbaiki dan memperbarui; menampilkan, mengumumkan, mentransfer, menyebarluaskan, atau mengungkapkan; dan/atau

---

mengatur bahwa pemrosesan dilakukan berdasarkan persetujuan, maka pengendali data pribadi harus dapat mendemonstrasikan bahwa *data subject* telah menyetujui untuk dilakukannya pemrosesan data pribadi miliknya. Apabila persetujuan *data subject* diberikan secara tertulis, serta bertautan dengan hal-hal lain, maka permintaan atas persetujuan tersebut harus disampaikan dengan bentuk atau metode yang jelas dapat diperbedakan dari yang lain, dapat dimengerti dan mudah untuk diakses, serta menggunakan bahasa yang jelas dan umum. *Data subject* juga harus memiliki hak untuk melakukan penarikan kembali atas persetujuan yang telah diberikannya kapanpun. Namun, penarikan kembali atas persetujuan tersebut tidak boleh berimbas kepada validitas pemrosesan berdasarkan pemrosesan sebelum terjadinya penarikan. Sebelum memberikan persetujuan, *data subject* harus diberikan informasi, serta penarikan kembali persetujuan haruslah semudah pemilik data pribadi memberikan persetujuannya.

<sup>26</sup> Yang dimaksud dengan keabsahan ialah kegiatan yang berupa memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, menyebarluaskan, dan memusnahkan data pribadi yang dilakukan berdasarkan hukum yang berlaku (Pasal 2 ayat (5) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik).

menghapuskan atau memusnahkan. Untuk melakukan pemrosesan data pribadi sebagaimana tersebut dilakukan dengan prinsip antara lain:<sup>27</sup>

- a. Data pribadi dikumpulkan dengan cara-cara yang terbatas dan spesifik, berdasarkan hukum, patut, dan serta transparan.
- b. Dilaksanakan berdasarkan tujuannya.
- c. Dilaksanakan dengan menjamin hak dari pemilik data pribadi<sup>28</sup>.

---

<sup>27</sup> Pasal 17 ayat (1) dan (2) Draft Rancangan Undang-Undang Perlindungan Data Pribadi 2020 (Januari).

<sup>28</sup> Hak-hak yang dimiliki oleh pemilik data pribadi dalam Draft Rancangan Undang-Undang Perlindungan Data Pribadi 2020 (Januari) antara lain:

- a. Meminta informasi mengenai kejelasan identitas, dasar kepentingan hukum, maksud dari permintaan dan pemakaian data pribadi, dan tanggung jawab pihak yang memintakan data pribadi (Pasal 4).
- b. Mengisi data pribadi miliknya dengan lengkap sebelum dilakukan pemrosesan oleh pengendali data pribadi (Pasal 5). (Pengendali data pribadi ialah pihak yang menetapkan tujuan serta memiliki kendali atas kegiatan pemrosesan data pribadi berdasarkan Pasal 1 angka 3 Draft Rancangan Undang-Undang Perlindungan Data Pribadi 2020 (Januari)).
- c. Mengakses data pribadi miliknya sebagaimana yang diatur dalam peraturan perundang-undangan (Pasal 6).
- d. Melakukan pembaruan dan/atau perbaikan atas kesalahan ataupun adanya ketidakakuratan dalam data pribadi miliknya menurut ketentuan perundang-undangan (Pasal 7).
- e. Melakukan pengakhiran dari kegiatan pemrosesan, penghapusan, dan/atau pemusnahan data pribadi miliknya (Pasal 8)
- f. Melakukan penarikan kembali atas persetujuan pemrosesan yang telah diberikan kepada pengendali data pribadi (Pasal 9).
- g. Melakukan pengajuan keberatan terhadap perbuatan pengambilan keputusan yang hanya berdasarkan pada pemrosesan profil seseorang secara otomatis (*profiling*) (Pasal 10).
- h. Memutuskan antara memilih atau tidak memilih pemrosesan data pribadi yang dilakukan dengan mekanisme pseudonim terhadap maksud tertentu (Pasal 11). (Mekanisme pseudonim dalam penjelasan Pasal 11 ialah pemrosesan data pribadi yang dilakukan dengan cara sedemikian rupa yang mengakibatkan data pribadi tidak dapat dihubungkan kembali dengan pemilik data pribadi yang teridentifikasi atau dapat diidentifikasi tanpa adanya penambahan informasi).
- i. Melakukan penundaan atau pembatasan terhadap pemrosesan data pribadi yang dilakukan dengan wajar yang mana sesuai dengan tujuan dari pemrosesan data pribadi (Pasal 12).
- j. Melakukan penuntutan atau mendapatkan kompensasi terhadap pelanggaran atas data pribadi miliknya sebagaimana yang diatur dalam peraturan perundang-undangan (Pasal 13).
- k. Memperoleh dan/atau menggunakan data pribadi miliknya dari pengendali data pribadi dengan bentuk yang sesuai secara tatanan dan/atau format yang umum digunakan atau dapat dibaca oleh sistem elektronik atau perangkat keras yang dipakai dalam interoperabilitas antarsistem elektronik (Pasal 14 ayat (1)).
- l. Memakai dan menyampaikan data pribadi miliknya kepada pengendali data pribadi lainnya, sepanjang sistem tersebut dapat saling berkomunikasi secara aman sesuai dengan prinsip perlindungan data pribadi berdasarkan undang-undang perlindungan data pribadi (Pasal 14 ayat (2)).

- d. Dilaksanakan dengan tepat, lengkap, tidak menyesatkan, terbaru, serta dapat dipertanggungjawabkan.
- e. Dilaksanakan dengan melindungi keamanan data pribadi dari hal-hal yang melanggar hukum seperti pengaksesan, pengungkapan, perubahan yang dilakukan secara ilegal, penyelewengan, perusakan, dan/atau kehilangan data pribadi.
- f. Kegiatan pemrosesan data pribadi dijalankan dengan menginformasikan maksud dan aktivitas pemrosesan, maupun kegagalan yang terjadi dalam melindungi data pribadi.
- g. Data pribadi dilenyapkan dan/atau dihapus ketika durasi penyimpanan telah berakhir atau adanya permohonan dari pemilik data pribadi, kecuali ditetapkan lain menurut peraturan perundang-undangan; dan
- h. Kegiatan pemrosesan data pribadi dijalankan dengan bertanggung jawab serta berpegang teguh pada prinsip perlindungan data pribadi dan secara jelas dapat dibuktikan.

Hal penting terkait pemrosesan data pribadi menurut Pasal 18 ayat (1) RUU ini ialah keharusan akan adanya persetujuan sah yang didapatkan dari pemilik data pribadi yang disampaikan dengan maksud untuk melaksanakan satu atau beberapa tujuan tertentu. Namun, hal ini dapat dikecualikan demi:<sup>29</sup>

- a. Pelaksanaan kewajiban dalam suatu perjanjian yang mengatur bahwa pemilik data pribadi menjadi salah satu pihak atau dalam rangka pemenuhan permintaan pemilik data pribadi sebelum melakukan perjanjian;
- b. Pengendali data pribadi melaksanakan kewajiban hukumnya sebagaimana yang diatur dalam ketentuan peraturan perundang-undangan;

---

Terdapat pengecualian dari beberapa hak pemilik data pribadi tersebut di atas, yang mengatur bahwa hak pemilik tidak berlaku untuk: (Pasal 16 ayat (1))

- a. Keperluan pertahanan dan keamanan nasional;
- b. Keperluan dalam proses penegakan hukum;
- c. Keperluan umum yang dilakukan demi penyelenggaraan negara;
- d. Keperluan pengawasan pada sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan; atau
- e. Agregat data yang kegiatan pemrosesannya dilakukan dengan tujuan kepentingan statistik dan penelitian ilmiah dalam rangka penyelenggaraan negara.

<sup>29</sup> Id., Pasal 18 ayat (2).

- c. Pelaksanaan perlindungan terhadap kepentingan yang sah (*vital interest*) dari pemilik data pribadi;
- d. Menjalankan kewenangan yang ada pada pengendali data pribadi berdasarkan ketentuan peraturan perundang-undangan;
- e. Pengendali data pribadi melakukan pemenuhan atas kewajibannya dalam hal pelayanan publik demi kepentingan umum; dan/atau
- f. Melakukan pemenuhan terhadap kepentingan sah lainnya dengan mengindahkan tujuan, keperluan, dan kesepadanan antara kepentingan pengendali data pribadi dengan hak pemilik dari data pribadi.

Pemrosesan data pribadi selain diatur dalam RUU Perlindungan Data Pribadi, dapat ditemui juga dalam Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran (PBI Sistem Pembayaran). Pasal 107 menyebutkan bahwa dalam kegiatan pemrosesan data dan/atau informasi yang berkaitan dengan sistem pembayaran, maka Penyedia Jasa Pembayaran (PJP)<sup>30</sup>, Penyelenggara Infrastruktur Sistem Pembayaran (PIP)<sup>31</sup>, dan/atau pihak yang melakukan kerja sama dengan PJP dan PIP berkewajiban untuk:

- a. Mempraktikkan prinsip perlindungan data pribadi yang meliputi pula pemenuhan aspek persetujuan dari pengguna jasa atas penggunaan data pribadi miliknya;
- b. Melakukan pemenuhan terhadap mekanisme pemrosesan data dan/atau informasi perihal sistem pembayaran<sup>32</sup> yang ditentukan oleh Bank Indonesia,

---

<sup>30</sup> Penyedia Jasa Pembayaran ialah bank atau lembaga selain dari bank yang menjadi penyedia jasa dalam memudahkan transaksi pembayaran pengguna jasa (Pasal 1 angka 4 Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran).

<sup>31</sup> Penyelenggara Infrastruktur Sistem Pembayaran ialah pihak yang mengusahakan infrastruktur untuk digunakan dalam melaksanakan pemindahan dana bagi kepentingan anggotanya (Pasal 1 angka 5 Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran).

<sup>32</sup> Mekanisme kegiatan pemrosesan data dan/atau informasi pembayaran dapat dilakukan oleh: (Penjelasan Pasal 107 ayat (1) huruf b Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran)

1. Pengguna jasa dengan PJP atau PIP;
2. Antar PJP atau PIP;
3. Antara PJP atau PIP dengan Bank Indonesia;
4. Antarpengguna jasa; dan
5. Antara pengguna jasa dengan Bank Indonesia.

hal ini meliputi mekanisme pemrosesan menggunakan infrastruktur data dan sistem pembayaran Bank Indonesia;

- c. Melaksanakan pemenuhan terhadap prosedur penggunaan infrastruktur data pihak ketiga yang diatur oleh Bank Indonesia;
- d. Mengaplikasikan tata kelola risiko siber dalam penyelenggaraan sistem pembayaran, yang didalamnya meliputi standar keamanan sistem informasi; dan
- e. Menjalankan ketentuan yang ada di peraturan perundang-undangan.

Berkenaan dengan tata kelola kegiatan pemrosesan data dan/atau informasi sistem pembayaran sebagaimana yang disebutkan di atas, mencakup pula akses dan mekanisme pemrosesan; pembakuan data, teknis, keamanan, dan tata kelola; dan/atau mekanisme lainnya yang ditentukan oleh Bank Indonesia.<sup>33</sup>

Selanjutnya PJP dan/atau PIP dapat mengadakan pertukaran data individual nasabah dengan PJP dan/atau PIP lainnya maupun pihak terkait lain sepanjang mengikuti ketentuan peraturan perundang-undangan tentang perlindungan data pribadi dan aturan dari Bank Indonesia.<sup>34</sup> Pertukaran tersebut dilakukan dengan:<sup>35</sup>

- a. Secara langsung oleh PJP dan/atau PIP; dan/atau
- b. Menggunakan sarana pengelolaan data dan/atau sistem pembayaran terpadu yang diselenggarakan atau disediakan oleh Bank Indonesia.

PJP dan PIP juga dapat melakukan pengiriman data individual nasabah kepada pihak lain yang berada di luar wilayah hukum Indonesia, sepanjang mematuhi peraturan perundang-undangan terkait perlindungan data pribadi serta pengaturan dari Bank Indonesia. Apabila kegiatan pengiriman data individual nasabah tidak dijalankan sebagaimana yang terdapat dalam ketentuan peraturan perundang-undangan dan/atau dengan tujuan demi melindungi kepentingan nasional, maka Bank Indonesia berhak melakukan penghentian pengiriman data tersebut.<sup>36</sup>

---

<sup>33</sup> Id., Pasal 107 ayat (2).

<sup>34</sup> Id., Pasal 108 ayat (1).

<sup>35</sup> Id., Pasal 108 ayat (2).

<sup>36</sup> Id., Pasal 109 ayat (1) dan (2).

## **Kewajiban yang Dimiliki Pengendali Data Pribadi**

RUU Perlindungan Data Pribadi menyebutkan bahwa pengendali data pribadi berkewajiban untuk menjaga kerahasiaan data pribadi ketika melakukan pemrosesan sebagai halnya yang diatur di Pasal 21 ayat (1). Hal tersebut dapat dilakukan pengecualian manakala:<sup>37</sup>

- a. Adanya persetujuan yang diberikan oleh pemilik data pribadi;
- b. Diperlukan ketika melakukan pemenuhan kewajiban dan/atau hak tertentu yang dimiliki pengendali data pribadi atau dari pemilik data pribadi yang ada pada bidang ketenagakerjaan, jaminan sosial, perpajakan, control pada sektor keuangan, pengelolaan administrasi kependudukan, dan/atau kesejahteraan sosial yang memberikan perlindungan atas hak dasar dan kepentingan dari pemilik data pribadi;
- c. Dibutuhkan dengan bertujuan demi melindungi kepentingan dari pemilik data pribadi yang tidak cakap fisik maupun hukum; dan/atau
- d. Dibutuhkan untuk membantu proses penegakan hukum.

Pengendali data pribadi memiliki kewajiban untuk menginformasikan perihal:<sup>38</sup>

- a. Keabsahan dari kegiatan pemrosesan data pribadi;
- b. Tujuan dilakukannya pemrosesan data pribadi;
- c. Jenis serta keterkaitan data pribadi yang akan diproses;
- d. Durasi penyimpanan dokumen yang berisi data pribadi;
- e. Paparan perihal informasi yang dikumpulkan;
- f. Durasi kegiatan pemrosesan data pribadi; serta
- g. Hak yang dimiliki oleh pemilik data pribadi.

Pengendali data pribadi dalam melaksanakan aktivitas pemrosesan data diharuskan untuk membuktikan bahwa pemilik data pribadi telah memberikan persetujuan. Serta apabila informasi sebagaimana yang disebutkan di atas mengalami perubahan, maka pengendali data pribadi memiliki kewajiban untuk

---

<sup>37</sup> Pasal 21 ayat (2) Draf Rancangan Undang-Undang Perlindungan Data Pribadi 2020 (Januari).

<sup>38</sup> Id., Pasal 24 ayat (1).

menginformasikan hal tersebut kepada pemilik data pribadi dengan jangka waktu maksimal 7x24 jam setelah adanya perubahan.<sup>39</sup>

Di samping itu, pengendali data pribadi berkewajiban dalam melakukan penghentian aktivitas pemrosesan data pribadi manakala terjadi penarikan kembali persetujuan dari pemilik data pribadi yang dilakukan terhitung paling lambat 3x24 jam sejak diterimanya permintaan penarikan.<sup>40</sup> Pasal 26 ayat (1) RUU Perlindungan Data Pribadi mengatur bahwa pengendali data pribadi berkewajiban untuk menunda dan membatasi aktivitas pemrosesan data pribadi yang dilakukan sebagian maupun seluruhnya dalam jangka waktu maksimal 2x24 jam sejak diterimanya permohonan untuk menunda dan membatasi pemrosesan. Tetapi, terhadap penundaan dan pemrosesan tersebut dapat dilakukan pengecualian untuk hal:<sup>41</sup>

- a. Pengaturan dalam peraturan perundang-undangan yang didalamnya menyebutkan bahwa penundaan dan pembatasan pemrosesan data pribadi tidak dapat dilaksanakan;
- b. Memberikan dampak yang membahayakan keselamatan dari pihak lain; dan/atau
- c. Adanya perjanjian secara tertulis antara pemilik data pribadi dengan pengendali data pribadi yang didalamnya mengatur penundaan dan pembatasan pemrosesan data pribadi tidak dapat dilaksanakan.

Selain itu, kewajiban pengendali data pribadi disebutkan lebih lanjut, antara lain:

- a. Melindungi dan menjamin keamanan dari data pribadi yang diprosesnya dengan menjalankan:<sup>42</sup>
  1. Penataan dan pengaplikasian langkah teknis operasional demi melindungi data pribadi dari adanya gangguan pemrosesan yang melanggar ketentuan dari peraturan perundang-undangan; dan

---

<sup>39</sup> Id., Pasal 24 ayat (2) dan (3).

<sup>40</sup> Id., Pasal 25 ayat (1) dan (2).

<sup>41</sup> Id., Pasal 26 ayat (2).

<sup>42</sup> Id., Pasal 27.

2. Penetapan tingkat keamanan data pribadi dengan menilai sifat serta risiko dari data pribadi yang perlu dilindungi dalam pelaksanaan pemrosesan data pribadi.
- b. Mengawasi setiap pihak terkait dalam pelaksanaan pemrosesan data pribadi.<sup>43</sup>
  - c. Menjamin terlindunginya data pribadi dari pemrosesan ilegal.<sup>44</sup>
  - d. Menangkal terjadinya akses ilegal dengan menerapkan sistem keamanan terhadap data pribadi yang diprosesnya dan/atau melakukan pemrosesan data pribadi dengan memanfaatkan sistem elektronik secara aman, terpercaya dan bertanggung jawab.<sup>45</sup>
  - e. Mendokumentasikan seluruh kegiatan pemrosesan data pribadi.<sup>46</sup>
  - f. Memberikan akses atas data pribadi yang dilakukan pemrosesan disertai rekam jejak pemrosesan sesuai durasi penyimpanan data pribadi kepada pemilik data pribadi. Akses tersebut diberikan paling lambat 3x24 jam sejak diterimanya permintaan akses.<sup>47</sup>
  - g. Menolak pemberian akses untuk melakukan pergantian data pribadi kepada pemilik data pribadi apabila didapati atau diduga:<sup>48</sup>
    1. Membahayakan keamanan atau kesehatan baik fisik maupun mental dari pemilik data pribadi dan/atau orang lain;
    2. Berakibat pada penyingkapan data pribadi milik orang lain; dan/atau
    3. Berbenturan dengan kepentingan pertahanan dan keamanan nasional.
  - h. Melakukan pembaruan dan/atau perbaikan kesalahan dan/atau ketidakakuratan data pribadi paling lambat 1x24 jam sejak diterimanya permohonan untuk memperbarui dan/atau memperbaiki data pribadi. Disertai pemberitahuan akan hasil tersebut kepada pemilik data pribadi.<sup>49</sup>

---

<sup>43</sup> Id., Pasal 28.

<sup>44</sup> Id., Pasal 29.

<sup>45</sup> Id., Pasal 30 ayat (1) dan (2).

<sup>46</sup> Id., Pasal 31.

<sup>47</sup> Id., Pasal 32 ayat (1) dan (2).

<sup>48</sup> Id., Pasal 33.

<sup>49</sup> Id., Pasal 34 ayat (1) dan (2).

- i. Menjamin ketepatan, kelengkapan, dan kesesuaian data pribadi dengan ketentuan peraturan perundang-undangan yang berlaku dengan menjalankan verifikasi.<sup>50</sup>
- j. Melaksanakan kegiatan pemrosesan data pribadi sejalan dengan tujuan dari pemrosesan yang telah disetujui oleh pemilik data pribadi.<sup>51</sup>
- k. Mengakhiri pemrosesan data pribadi apabila:<sup>52</sup>
  - 1. Masa penyimpanan telah selesai;
  - 2. Tercapainya tujuan dari pemrosesan; atau
  - 3. Pemilik data pribadi mengajukan permintaan.
- l. Menghapus data pribadi jika:<sup>53</sup>
  - 1. Tidak lagi dibutuhkan dalam mencapai tujuan kegiatan pemrosesan data pribadi;
  - 2. Adanya penarikan persetujuan dalam pemrosesan oleh pemilik data pribadi;
  - 3. Pemilik data pribadi mengajukan permintaan; atau
  - 4. Perolehan dan/atau pemrosesan data pribadi yang bertentangan dengan hukum.
- m. Memusnahkan data pribadi jika:<sup>54</sup>
  - 1. Sudah tidak ada manfaatnya lagi;
  - 2. Masa penyimpanan yang telah habis dan memiliki keterangan bahwa telah dimusnahkan menurut jadwal penyimpanan arsip;
  - 3. Pemilik data pribadi yang mengajukan permintaan; atau
  - 4. Tidak memiliki hubungan dengan penyelesaian dari proses hukum suatu perkara.
- n. Memberitahukan dengan bentuk tertulis dalam durasi 3x24 jam kepada pemilik data pribadi dan Menteri apabila telah terjadi kegagalan dalam perlindungan

---

<sup>50</sup> Id., Pasal 35 ayat (1) dan (2).

<sup>51</sup> Id., Pasal 36.

<sup>52</sup> Id., Pasal 37.

<sup>53</sup> Id., Pasal 38 ayat (1). Data pribadi yang telah dihapus dapat dilakukan pemulihan atau diperlihatkan kembali secara lengkap apabila terdapat permintaan secara tertulis dari pemilik data pribadi yang dapat diajukan sebelum melewati masa retensi yang ada dalam ketentuan peraturan perundang-undangan sebagaimana yang disebutkan dalam Pasal 38 ayat (3) dan (4) Rancangan Undang-Undang Perlindungan Data Pribadi.

<sup>54</sup> Id., Pasal 39.

data pribadi. Pemberitahuan tersebut memuat data pribadi yang terekspos, waktu dan penjelasan bagaimana data pribadi telah terungkap, serta upaya penindakan dan pemulihan yang diambil terhadap terungkapnya data pribadi.<sup>55</sup>

- o. Melakukan pemenuhan kewajibannya dalam rangka melaksanakan prinsip perlindungan data pribadi sebagai bentuk tanggung jawab.<sup>56</sup>

Terhadap kewajiban di atas, terdapat beberapa pengecualian yang mengatur bahwa kewajiban dari pengendali data pribadi tidak berlaku dalam hal:<sup>57</sup>

- a. Keperluan dalam pertahanan dan keamanan nasional;
- b. Keperluan dalam proses penegakan hukum;
- c. Kepentingan umum yang dilakukan demi penyelenggaraan negara;
- d. Kebutuhan untuk melakukan pengawasan pada sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan; atau
- e. Agregat data yang aktivitas pemrosesannya diarahkan pada manfaat untuk kepentingan statistik dan penelitian ilmiah dalam rangka penyelenggaraan negara.

### **Uang Elektronik Berbasis *Server* beserta Perlindungan Data Pribadi**

Ketentuan yang membahas mengenai uang elektronik sebelumnya diatur dalam Peraturan Bank Indonesia Nomor 20/6/2018 tentang Uang Elektronik (PBI Uang Elektronik). Namun, setelah diterbitkannya Peraturan Bank Indonesia Nomor 23/6/PBI tentang Penyedia Jasa Pembayaran (PBI PJP), ketentuan PBI Uang Elektronik tersebut dicabut dan dinyatakan tidak berlaku lagi.<sup>58</sup> Menurut PBI PJP, definisi dari uang elektronik ialah perangkat pembayaran yang memiliki unsur antara lain:<sup>59</sup>

---

<sup>55</sup> Id., Pasal 40 ayat (1) dan (2). Selanjutnya dalam ayat (3) disebutkan bahwa pengendali data pribadi berkewajiban untuk menginformasikan kepada masyarakat perihal terjadinya kegagalan dalam perlindungan data pribadi pada keadaan tertentu. Pengertian dari keadaan tertentu tersebut antara lain ialah kegagalan dalam melaksanakan perlindungan data pribadi yang berdampak pada terganggunya pelayanan publik dan/atau memberikan dampak yang serius terhadap kepentingan masyarakat.

<sup>56</sup> Id., Pasal 41.

<sup>57</sup> Id., Pasal 42.

<sup>58</sup> Pasal 273 Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran.

<sup>59</sup> Id., Pasal 156.

- a. Dibuat dengan dasar sumber dana<sup>60</sup> yang berbentuk nilai uang rupiah yang sebelumnya telah disetor terlebih dahulu kepada PJP yang menjalankan pengelolaan sumber dana; dan
- b. Sumber dana yang berbentuk nilai uang rupiah yang disimpan melalui media elektronik *server* atau *chip*.

Pada uang elektronik, berdasarkan media penyimpanannya dibedakan antara *server based* dan *chip based*. Media penyimpanan uang elektronik *server based* ialah penyimpanan yang dilakukan dengan menggunakan *server*, sementara *chip based* ialah penyimpanan yang dilakukan melalui *chip*.<sup>61</sup>

PJP yang melaksanakan kegiatan pengelolaan sumber dana dalam hal menerbitkan uang elektronik, memiliki kewenangan dalam menetapkan masa berlaku dari media uang elektronik dengan pertimbangan:<sup>62</sup>

- a. Batas usia teknis yang dipakai dalam sarana uang elektronik; dan
- b. Aspek lainnya.

Meskipun masa berlakunya telah habis, nilai dari uang elektronik yang masih belum digunakan tidak berarti hilang atau terhapus sebagaimana yang diatur dalam Pasal 161 ayat (3) PBI PJP. Untuk itu, PJP wajib untuk memberitahukan kepada pengguna uang elektronik perihal telah berakhirnya masa berlaku uang elektronik disertai tata cara penyelesaian nilai uang elektronik yang belum dipakai.<sup>63</sup>

Dalam melaksanakan pemrosesan data dan/atau informasi di bidang Sistem Pembayaran, PJP dan/atau pihak yang melakukan kerja sama dengan PJP memiliki kewajiban untuk:<sup>64</sup>

- a. Mengaplikasikan prinsip perlindungan data pribadi<sup>65</sup> yang didalamnya meliputi pemenuhan aspek persetujuan pengguna terhadap data pribadi miliknya dalam hal:

---

<sup>60</sup> Sumber dana yang dipakai dalam menjalankan kewajiban pelaksanaan transaksi pembayaran dan pengelolaan dalam suatu akun untuk kegiatan pembayaran (Id., Pasal 1 angka 13).

<sup>61</sup> Id., Pasal 159 huruf a.

<sup>62</sup> Id., Pasal 161 ayat (1) dan (2).

<sup>63</sup> Id., Pasal 161 ayat (4).

<sup>64</sup> Id., Pasal 257 ayat (1).

<sup>65</sup> Pengaplikasian prinsip perlindungan data pribadi dijalankan dengan melakukan pertimbangan terhadap aspek kepentingan publik dan/atau persyaratan lainnya yang ditentukan oleh lembaga yang berwenang (Id., Pasal 257 ayat (2)).

1. Dikumpulkannya data pribadi secara terbatas dan untuk hal tertentu, sah menurut hukum, patut, serta transparan;
  2. Kegiatan pemrosesan data pribadi dilaksanakan berdasarkan tujuannya;
  3. Menjamin hak yang dimiliki pemilik data pribadi dalam pemrosesan data pribadi;
  4. Kegiatan pemrosesan data pribadi dijalankan dengan cara-cara yang tepat, lengkap, tidak menyimpang, terbaru, dapat dipertanggungjawabkan, serta berdasarkan tujuannya;
  5. Kegiatan pemrosesan data pribadi dilaksanakan dengan menjamin keamanan dari data pribadi dalam hal terjadinya kehilangan, penyelewengan, akses dan pengungkapan yang ilegal, serta penggantian atau perusakan data pribadi;
  6. Kegiatan pemrosesan data pribadi dilaksanakan dengan menginformasikan tujuan dari dikumpulkannya data, kegiatan pemrosesan, serta kegagalan yang terjadi dalam melindungi data pribadi; dan
  7. Kegiatan pemrosesan data pribadi yang dihapuskan atau dimusnahkan dengan pengecualian masih adanya durasi penyimpanan berdasarkan kebutuhan menurut ketentuan peraturan perundang-undangan.
- b. Pelaksanaan tata cara pemrosesan data dan/atau informasi Sistem Pembayaran yang ditentukan Bank Indonesia;
  - c. Pelaksanaan tata cara penggunaan sarana data dari pihak ketiga yang ditetapkan oleh Bank Indonesia;
  - d. Mengaplikasikan tata kelola risiko siber dalam pengelolaan Sistem Pembayaran yang meliputi standar keamanan sistem informasi;
  - e. Memperhatikan integritas data yang mewakili fakta atau keadaan yang sesungguhnya serta menggunakan cara-cara yang transparan secara konsisten; dan
  - f. Melaksanakan ketentuan yang ada di peraturan perundang-undangan.

PBI PJP juga mengatur bahwa dalam melindungi konsumen jasa keuangan, PJP yang menerbitkan uang elektronik memiliki keharusan dalam membatasi permintaan dan penggunaan data dan/atau informasi milik pengguna dari uang

elektronik, sebatas pada hal-hal yang dibutuhkan dalam menyelenggarakan uang elektronik.<sup>66</sup> Di samping itu, dalam PBI PJP disebutkan bahwa PJP dan/atau pihak yang bekerja sama dengan PJP terkait kegiatan pemrosesan data dan/atau informasi mengenai sistem pembayaran yang dilaksanakan dengan memanfaatkan sarana data pihak ketiga, wajib untuk memastikan kerahasiaan dan perlindungan data yang disimpan atau diproses.<sup>67</sup>

DANA, Link Aja, GoPay, Ovo, ShopeePay, OttoCash merupakan beberapa contoh dari penerbit uang elektronik berbasis *server* yang saat ini berkembang. Masing-masing penerbit uang elektronik tersebut mengeluarkan kebijakan privasi yang dapat dilihat pada *website* ataupun aplikasi yang bersangkutan. Kebijakan privasi tersebut dibuat dengan bertujuan demi memastikan bahwa pengguna telah mengerti dan menyetujui metode yang digunakan penerbit uang elektronik dalam mendapatkan, memproses, memanfaatkan, menyimpan, dan melakukan pengungkapan perihal data pribadi pengguna.

Misalnya praktek yang terjadi pada salah satu penerbit uang elektronik berbasis *server*, penerbit uang elektronik dimaksud menyebutkan perolehan dan pengumpulan data pribadi dapat diperoleh secara langsung ataupun tidak langsung ketika pengguna menggunakan aplikasi. Data pribadi tersebut berupa hal-hal yang memiliki hubungan informasi komputer, perangkat telepon, bagian dari perangkat keras lainnya, perangkat lunak, serta jaringan telekomunikasi yang digunakan oleh pengguna dalam mengakses atau menggunakan aplikasi. Informasi data pribadi pengguna juga dapat diperoleh ketika pendaftaran dalam melakukan pembuatan akun produk uang elektronik. Data tersebut ialah berupa nama, tanggal lahir, alamat, nomor telepon, *email*, foto dan kartu identitas. Informasi lainnya juga dapat diperoleh penerbit uang elektronik dimaksud melalui pengguna yang berupa nomor rekening bank, informasi tagihan dan pentransferan, data transaksi, nomor

---

<sup>66</sup> Id., Pasal 177.

<sup>67</sup> Id., Pasal 260 beserta Penjelasan Pasal 260 huruf c.

kartu kredit dan/atau debit dan tanggal kadaluwarsanya, dan informasi lainnya yang berasal dari cek atau wesel.<sup>68</sup>

Selain perolehan dan pengumpulan data pribadi, kebijakan privasi yang ada di penerbit uang elektronik tersebut berisi mengenai pemakaian dan pengungkapan data pribadi, aktivitas pemasaran langsung, langkah dalam mengamankan dan menyimpan, layanan pihak ketiga dan situs *website*, pergantian kebijakan privasi, ketentuan lain, pernyataan, melakukan penjagaan terkait keamanan data milik pengguna, penyimpanan dan pemusnahan data, serta informasi lebih lanjut. Berdasarkan kebijakan privasi tersebut, penerbit uang elektronik tersebut dapat meneruskan data pribadi pengguna ke pihak:<sup>69</sup>

- a. Perusahaan yang merupakan anggota grup dari penerbit uang elektronik tersebut maupun perusahaan yang memiliki relasi dengan grup penerbit uang elektronik tersebut.
- b. Agen, kontraktor, dan penyedia layanan pihak ketiga yang mempunyai hubungan kerja sama dalam menyediakan layanan kepada pengguna agar terhindar dari penipuan, pengumpulan tagihan, *input* data, pengelolaan *database*, promosi, pemasaran, riset, *survey*, pelayanan pelanggan, layanan teknologi, informasi produk dan layanan serta layanan perpanjangan pembayaran.
- c. Pihak-pihak yang mempunyai kaitan referensi bisnis atau perjanjian-perjanjian profitabel lainnya yang meliputi pihak ketiga dan pihak yang sepenuhnya atau sebagian dikuasai oleh penerbit uang elektronik tersebut.
- d. *Merchant* dan organisasi lainnya yang berupa perkumpulan kartu, jaringan pembayaran atau institusi keuangan, pembayaran menggunakan produk uang elektronik tersebut yang dilakukan ke pihak mana atau melalui siapa pembayaran tersebut dilakukan.
- e. Institusi keuangan pihak ketiga, perbankan, agen penerimaan, lembaga pembiayaan, dan agen kredit.

---

<sup>68</sup> Kebijakan Privasi Akun Pengguna Dana, <https://www.dana.id/policy>, diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

<sup>69</sup> Id.

- f. Penyedia jasa yang merupakan pihak ketiga.
- g. Konsultan profesional, lembaga penegak hukum, perusahaan asuransi, pemerintah dan pihak berwenang lainnya sesuai dengan keperluan, permohonan yang dilakukan secara sah serta mengikuti peraturan yang berlaku.
- h. Pihak-pihak yang turut serta dalam unifikasi, pengambilalihan, transaksi pembiayaan atau kegiatan usaha patungan dengan penerbit uang elektronik tersebut.

Contoh praktek pada penerbit uang elektronik lainnya yang menjelaskan dalam kebijakan privasinya mengenai pengumpulan dan penggunaan informasi berupa nama, nomor ponsel, alamat surel, alamat tinggal, KTP, alamat *internet protocol*, informasi terkait manufaktur, jenis, dan sistem operasi yang ada pada perangkat yang digunakan. Kebijakan privasi penerbit uang elektronik tersebut juga berisi tentang *cookies*<sup>70</sup>, keamanan, keamanan pembayaran, perubahan kebijakan privasi, serta *disclaimer*.<sup>71</sup>

## Penutup

Pengaturan mengenai perlindungan data pribadi secara umum, dapat ditemukan dalam GDPR dan perundang-undangan di Indonesia yaitu Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik dan RUU Perlindungan Data Pribadi. Ketentuan tersebut melindungi hak-hak dari pengguna atau pemilik data pribadi agar datanya tidak tersebar tanpa persetujuan atau disalahgunakan.

Perlindungan data pribadi yang terdapat pada uang elektronik berbasis server telah diatur dalam Pasal 107 PBI Sistem Pembayaran serta ketentuan yang ada dalam PBI PJP. Berdasarkan PBI Sistem Pembayaran dan PBI PJP tersebut, PJP

---

<sup>70</sup> ialah berkas data kecil yang diposisikan *browser* pada komponen internet milik pengguna yang memiliki kemampuan dalam penyimpanan informasi atau mengingat aktivitas dan preferensi dari pengguna selama waktu ke waktu (Kebijakan Privasi Link Aja, <https://www.linkaja.id/kebijakan-privasi>, diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB).

<sup>71</sup> Kebijakan Privasi Link Aja, <https://www.linkaja.id/kebijakan-privasi>, diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

selaku penyelenggara uang elektronik harus mengikuti prinsip-prinsip yang ada dalam perlindungan data pribadi. Sebagai pelaksanaan dari perlindungan data pribadi, para penerbit uang elektronik mencantumkan kebijakan privasi yang harus diketahui oleh penggunanya. Isi dari kebijakan privasi tersebut dapat berupa cara atau metode yang digunakan dalam memperoleh dan mengumpulkan data pribadi, penggunaan data pribadi, penguasaan data pribadi, langkah-langkah yang diambil dalam menjaga keamanan dan penyimpanan, layanan pihak ketiga dan *website*, kebijakan privasi yang berubah, pengaturan mengenai ketentuan lain, pernyataan, pemeliharaan dan pemusnahan data. Pengguna dari uang elektronik berbasis *server* tersebut, dengan demikian mengikatkan dirinya dengan ketentuan yang ada pada penerbit uang elektronik serta menyetujui ketentuan kebijakan privasi yang ada pada penerbit uang elektronik. Di samping itu, dengan ketentuan kebijakan privasi tersebut penerbit uang elektronik memiliki kewajiban dalam penyelenggaraan keamanan terhadap data pribadi yang diperoleh dan tidak menjual ataupun menyebarkan data pribadi pengguna selain dari yang telah disetujui kecuali yang dipergunakan untuk proses hukum atau yang diatur dalam undang-undang.

Dengan demikian, dapat dipastikan bahwa pengaturan terkait perlindungan data pribadi konsumen jasa keuangan pada uang elektronik berbasis *server* di Indonesia tersebut telah mengadopsi berbagai prinsip pengaturan perlindungan data pribadi pada umumnya sebagaimana diatur dalam GDPR dan berbagai peraturan perundang-undangan di Indonesia. Peraturan-peraturan tersebut berperan dalam melindungi hak-hak pengguna terkait data pribadi miliknya seperti hak untuk melakukan pembauran ataupun menarik kembali persetujuan yang telah diberikan sebelumnya.

## Daftar Pustaka

### Buku:

- Adrian Sutedi, *Tanggung Jawab Produk dalam Hukum Perlindungan Konsumen*, Ghalia Indonesia, Jakarta, 2008
- Ahmadi Miru dan Sutarman Yodo, *Hukum Perlindungan Konsumen*, Raja Grafindo Persada, Jakarta, 2017
- Jane K. Winn, *Consumer Protection in the Age of the Information Economy*, Ashgate Publishing Company, 2006
- Janus Sidabolok, *Hukum Perlindungan Konsumen di Indonesia*, PT Citra Aditya Bakti, Bandung, 2010
- Solikin M. Juhro, 2020, *Pengantar Kebanksentralan Teori dan Kebijakan*, Rajawali Pers, Depok, 2020

### Jurnal:

- Badan Penelitian dan Pengembangan SDM Kementerian Komunikasi dan Informatika, *Perkembangan Ekonomi Digital di Indonesia: Strategi dan Sektor Potensial*, Puslitbang Aptika dan IKP, 2019
- Bank Indonesia, *Blueprint Sistem Pembayaran Indonesia 2025*, Bank Indonesia, Jakarta, 2019
- Bank Indonesia, *Kajian Pengaturan Data Policy Bidang Sistem Pembayaran*, Departemen Kebijakan Sistem Pembayaran, Bank Indonesia, 2020
- Herdi Setiawan, Mohammad Ghufron, dan Dewi Astutty Mochtar, *Perlindungan Hukum Terhadap Data Pribadi Konsumen dalam Transaksi E-Commerce*, MLJ Merdeka Journal, 1 (2): 102-111, 2020
- Orla Lynskey, *Deconstructing Data Protection: the 'Added-Value' of a Right to Data Protection in the EU Legal Order*, *International and Comparative Law Quarterly*, 63 (3), 2014
- Rosalinda Elsina Latumanhina, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*, *Jurnal Gema Aktualita*, Vol. 3 No. 2, Desember 2014
- Sandryones Palinggi, Erich C. Limbongan, *Pengaruh Internet Terhadap Industri E-Commerce dan Regulasi Perlindungan Data Pribadi Pelanggan di Indonesia*, Seminar Nasional Riset dan Teknologi (SEMNAS RISTEK) 2020

### Peraturan:

- Draft Rancangan Undang-Undang Perlindungan Data Pribadi Tahun 2020 (Januari)
- Peraturan Bank Indonesia Nomor 20/6/2018 tentang Uang Elektronik
- Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia
- Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran
- Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran
- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

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

**Situs Daring:**

Bank Indonesia. "Jumlah Uang Elektronik Beredar Tahun 2021". <<https://www.bi.go.id/id/statistik/ekonomi-keuangan/ssp/uang-elektronik-jumlah.aspx>>. diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

Caesar Akbar. "6 Kasus Kebocoran Data Pribadi di Indonesia". <<https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia>>. diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

CNN Indonesia. "Menkominfo: Kasus Pelanggaran Data Pribadi Sulit Terdeteksi". <<https://www.cnnindonesia.com/teknologi/20200225204935-185-478090/menkominfo-kasus-pelanggaran-data-pribadi-sulit-terdeteksi>>. diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

Kebijakan Privasi Akun Pengguna Dana. <<https://www.dana.id/policy>>. diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

Kebijakan Privasi Link Aja. <<https://www.linkaja.id/kebijakan-privasi>>. diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

Libera. "Pengaruh GDPR sebagai Perlindungan Data Pribadi & Keberlakuannya bagi Startup". <<https://libera.id/blogs/apa-itu-gdpr-dan-keberlakuannya-di-indonesia>>. diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

Oktarina Paramitha Sandy. "Mengenal Perbedaan *Data Privacy* dan *Data Protection*". <<https://m.cyberthreat.id/read/8878/Mengenal-Perbedaan-Data-Privacy-dan-Data-Protection>>. diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.

Putra Ananda. "Pandemi Covid-19 Membuat Ekonomi Digital Indonesia Tumbuh Pesat". <<https://mediaindonesia.com/ekonomi/397976/pandemi-covid-19-membuat-ekonomi-digital-indonesia-tumbuh-pesat>>. diakses pada tanggal 15 Oktober 2021 pukul 17.40 WIB.