TAMBAHAN
LEMBARAN NEGARA RI

No. 5348

KOMUNIKASI. INFORMASI. Sistem. Transaksi. Elektronik. Penyelenggaraan. (Penjelasan Atas Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189)

PENJELASAN
ATAS
PERATURAN PEMERINTAH REPUBLIK INDONESIA
NOMOR 82 TAHUN 2012
TENTANG
PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK

I. UMUM

Beberapa ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengamanatkan pengaturan lebih lanjut dalam peraturan pemerintah, yakni pengaturan mengenai Lembaga Sertifikasi Keandalan sebagaimana dimaksud dalam Pasal 10 ayat (2), Tanda Tangan Elektronik sebagaimana dimaksud dalam Pasal 11 ayat (2), penyelenggara sertifikasi elektronik sebagaimana dimaksud dalam Pasal 13 ayat (6), Penyelenggara Sistem Elektronik sebagaimana dimaksud dalam Pasal 16 ayat (2), Penyelenggaraan Transaksi Elektronik sebagaimana dimaksud dalam Pasal 17 ayat (3), penyelenggara Agen Elektronik sebagaimana dimaksud dalam Pasal 22 ayat (2), dan pengelolaan Nama Domain sebagaimana dimaksud dalam Pasal 24 ayat (4).

Pengaturan sebagaimana tersebut di atas merupakan rangkaian penyelenggaraan sistem dan transaksi elektronik sehingga dapat disusun dalam satu peraturan pemerintah yaitu Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Penyelenggara Sistem Elektronik menjamin setiap komponen dan keterpaduan seluruh Sistem Elektronik beroperasi sebagaimana mestinya. Komponen Sistem Elektronik meliputi Perangkat Keras, Perangkat Lunak, tenaga ahli, tata kelola, dan pengamanan. Peraturan Pemerintah ini mengatur kewajiban Penyelenggara Sistem Elektronik pada umumnya dan Penyelenggara Sistem Elektronik untuk pelayanan publik. Penyelenggara Sistem Elektronik untuk pelayanan publik, antara lain diwajibkan untuk menempatkan pusat data dan pusat pemulihan bencana di wilayah Indonesia, wajib memperoleh Sertifikasi Kelaikan Sistem Elektronik dari Menteri, dan wajib terdaftar pada kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

Penyelenggara Sistem Elektronik dapat menyelenggarakan sendiri Sistem Elektroniknya atau mendelegasikan kepada penyelenggara Agen Elektronik. Agen Elektronik dapat diselenggarakan untuk lebih dari satu kepentingan Penyelenggara Sistem Elektronik yang didasarkan pada perjanjian antara para pihak. Penyelenggara Agen Elektronik wajib terdaftar di kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

Penyelenggara Sistem Elektronik dan penyelenggara Agen Elektronik dapat menyelenggarakan Transaksi Elektronik. Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik atau privat. Penyelenggaraan Transaksi Elektronik yang dilakukan para pihak wajib dilakukan dengan iktikad baik dan memperhatikan prinsip kehati-hatian, transparansi, akuntabilitas, dan kewajaran. Transaksi Elektronik dapat dilakukan berdasarkan Kontrak Elektronik atau bentuk kontraktual lainnya.

Dalam setiap penyelenggaraan Transaksi Elektronik diperlukan Tanda Tangan Elektronik yang berfungsi sebagai persetujuan Penanda Tangan atas Informasi Elektronik dan/atau Dokumen Elektronik yang ditandatangani dengan Tanda Tangan Elektronik tersebut. Tanda Tangan Elektronik yang digunakan dalam Transaksi Elektronik dapat dihasilkan melalui berbagai prosedur penandatanganan. Tanda Tangan Elektronik meliputi Tanda Tangan Elektronik tersertifikasi dan Tanda Tangan Elektronik tidak tersertifikasi.

Tanda Tangan Elektronik tersertifikasi dihasilkan oleh penyelenggara sertifikasi elektronik yang dibuktikan dengan Sertifikat Elektronik. Untuk penyelenggara sertifikasi elektronik yang beroperasi di Indonesia wajib memperoleh pengakuan dari Menteri yang terdiri atas tingkatan terdaftar, tersertifikasi, atau berinduk. Kewajiban penyelenggara sertifikasi elektronik antara lain melakukan pendaftaran dan pemeriksaan calon pemilik dan/atau pemegang Sertifikat Elektronik dan menerbitkan Sertifikat Elektronik.

Pelaku Usaha yang menyelenggarakan Transaksi Elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan. Lembaga Sertifikasi Keandalan menerbitkan Sertifikat Keandalan melalui proses sertifikasi keandalan yang mencakup pemeriksaan terhadap informasi yang lengkap dan benar dari Pelaku Usaha.

Lembaga Sertifikasi Keandalan dibentuk paling sedikit oleh konsultan Teknologi Informasi, auditor Teknologi Informasi, dan konsultan hukum bidang Teknologi Informasi. Selain itu, profesi lain yang dapat terlibat dalam pembentukan Lembaga Sertifikasi Keandalan adalah akuntan, konsultan manajemen bidang Teknologi Informasi, penilai, notaris, dan profesi lain yang ditetapkan dengan Keputusan Menteri.

Setiap Instansi, Orang, Badan Usaha, dan masyarakat berhak memiliki Nama Domain berdasarkan prinsip pendaftar pertama (*first come first served*). Nama Domain dikelola oleh Pemerintah dan/atau masyarakat. Keberadaan Nama Domain sesungguhnya lahir pada saat suatu nama itu diajukan dan diterima pendaftarannya oleh sistem pencatatan Nama Domain. Sistem tersebut merupakan alamat internet global dimana hierarkis dan sistem pengelolaan Nama Domain mengikuti ketentuan yang dikeluarkan oleh institusi yang berwenang, baik nasional maupun internasional.

II. PASAL DEMI PASAL

Pasal 1

Cukup jelas.

Pasal 2

Cukup jelas.

Pasal 3

Cukup jelas.

Pasal 4

Cukup jelas.

Pasal 5

Cukup jelas.

Pasal 6

Ayat (1)

Huruf a

Yang dimaksud dengan “interkonektivitas” adalah kemampuan untuk terhubung satu sama lain sehingga bisa berfungsi sebagaimana mestinya. Termasuk dalam

pengertian interkonektivitas adalah mencakup kemampuan interoperabilitas.

Yang dimaksud dengan ”kompatibilitas” adalah kesesuaian Sistem Elektronik yang satu dengan Sistem Elektronik yang lainnya.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Huruf f

Yang dimaksud dengan “kejelasan tentang kondisi kebaruan” adalah terdapat informasi yang menjelaskan bahwa Perangkat Keras tersebut merupakan barang baru, diperbaharui kembali *(refurbished)*, atau barang bekas.

Huruf g

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 7

Ayat (1)

Huruf a

Pendaftaran dapat dilakukan oleh penjual atau penyedia (vendor), distributor, atau pengguna.

Huruf b

Yang dimaksud dengan “terjamin keamanan dan keandalan operasi sebagaimana mestinya” adalah

Penyelenggara Sistem Elektronik menjamin Perangkat Lunak tidak berisi instruksi lain daripada yang semestinya atau instruksi tersembunyi yang bersifat melawan hukum (*malicious code*). Contohnya instruksi *time bomb*, program virus, *trojan, worm,* dan *backdoor*. Pengamanan ini dapat dilakukan dengan memeriksa kode sumber.

Huruf c

Cukup jelas.

Ayat (2)

Cukup jelas.

Pasal 8

Ayat (1)

Yang dimaksud dengan "kode sumber" adalah suatu rangkaian perintah, pernyataan, dan/atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang dapat dibaca dan dipahami orang.

Ayat (2)

Yang dimaksud dengan "pihak ketiga terpercaya penyimpan kode sumber (*source code escrow*)" adalah profesi atau pihak independen yang berkompeten menyelenggarakan jasa penyimpanan kode sumber program Komputer atau Perangkat Lunak untuk kepentingan dapat diakses, diperoleh, atau diserahkan kode sumber oleh penyedia kepada pihak pengguna.

Ayat (3)

Cukup jelas.

Pasal 9

Cukup jelas.

Pasal 10

Ayat (1)

Yang dimaksud dengan "tenaga ahli" adalah tenaga yang memiliki pengetahuan dan keterampilan khusus dalam bidang Sistem Elektronik yang dapat dipertanggungjawabkan secara akademis maupun praktis.

Ayat (2)

Cukup jelas.

Pasal 11

Ayat (1)

Yang dimaksud dengan “Sistem Elektronik yang bersifat strategis” adalah Sistem Elektronik yang dapat berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.

Contoh: Sistem Elektronik pada sektor kesehatan, perbankan, keuangan, transportasi, perdagangan, telekomunikasi, atau energi.

Ayat (2)

Cukup jelas.

Ayat (3)

Yang dimaksud dengan “peraturan perundang-undangan” antara lain peraturan perundang-undangan di bidang ketenagakerjaan.

Ayat (4)

Cukup jelas.

Pasal 12

Ayat (1)

Huruf a

Yang dimaksud dengan “perjanjian tingkat layanan (*service level agreement*)” adalah pernyataan mengenai tingkatan mutu layanan suatu Sistem Elektronik.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Ayat (2)

Cukup jelas.

Pasal 13

Yang dimaksud dengan “menerapkan manajemen risiko” adalah melakukan analisis risiko dan merumuskan langkah mitigasi dan penanggulangan untuk mengatasi ancaman, gangguan, dan hambatan terhadap Sistem Elektronik yang dikelolanya.

Pasal 14

Ayat (1)

Yang dimaksud dengan ”kebijakan tata kelola” antara lain, termasuk kebijakan mengenai kegiatan membangun struktur organisasi, proses bisnis (*business process*), manajemen kinerja, dan menyediakan personel pendukung pengoperasian Sistem Elektronik untuk memastikan Sistem Elektronik dapat beroperasi sebagaimana mestinya.

Ayat (2)

Cukup jelas.

Pasal 15

Cukup jelas.

Pasal 16

Ayat (1)

Tata kelola Sistem Elektronik yang baik (*IT Governance*) mencakup proses perencanaan, pengimplementasian, pengoperasian, pemeliharaan, dan pendokumentasian.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 17

Ayat (1)

Yang dimaksud dengan “rencana keberlangsungan kegiatan (*business continuity plan*)” adalah suatu rangkaian proses yang dilakukan untuk memastikan terus berlangsungnya kegiatan dalam kondisi mendapatkan gangguan atau bencana.

Ayat (2)

Yang dimaksud dengan “pusat data (*data center*)” adalah suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.

Yang dimaksud dengan “pusat pemulihan bencana (*disaster recovery center*)” adalah suatu fasilitas yang digunakan untuk memulihkan kembali data atau informasi serta fungsi-fungsi penting Sistem Elektronik yang terganggu atau rusak akibat terjadinya bencana yang disebabkan oleh alam atau manusia.

Ayat (3)

Cukup jelas.

Pasal 18

Ayat (1)

Mekanisme rekam jejak audit (*audit trail*) meliputi antara lain:

a. memelihara log transaksi sesuai kebijakan retensi data penyelenggara, sesuai ketentuan peraturan perundang-undangan;

b. memberikan notifikasi kepada konsumen apabila suatu transaksi telah berhasil dilakukan;

c. memastikan tersedianya fungsi jejak audit untuk dapat mendeteksi usaha dan/atau terjadinya penyusupan yang harus di-*review* atau dievaluasi secara berkala; dan

d. dalam hal sistem pemrosesan dan jejak audit merupakan tanggung jawab pihak ketiga, maka proses jejak audit tersebut harus sesuai dengan standar yang ditetapkan oleh Penyelenggara Sistem Elektronik.

Ayat (2)

Yang dimaksud dengan “pemeriksaan lainnya” antara lain pemeriksaan untuk keperluan mitigasi atau penanganan tanggap darurat (*incident response*).

Pasal 19

Cukup jelas.

Pasal 20

Ayat (1)

Yang dimaksud dengan ”gangguan” adalah setiap tindakan yang bersifat destruktif atau berdampak serius terhadap Sistem Elektronik sehingga Sistem Elektronik tersebut tidak bekerja sebagaimana mestinya.

Yang dimaksud dengan ”kegagalan” adalah terhentinya sebagian atau seluruh fungsi Sistem Elektronik yang bersifat esensial sehingga Sistem Elektronik tidak berfungsi sebagaimana mestinya.

Yang dimaksud dengan ”kerugian” adalah dampak atas kerusakan Sistem Elektronik yang mempunyai akibat hukum bagi pengguna, penyelenggara, dan pihak ketiga lainnya baik materil maupun immateril.

Ayat (2)

Yang dimaksud dengan ”sistem pencegahan dan penanggulangan” antara lain *antivirus, anti spamming, firewall, intrusion detection, prevention system,* dan/atau pengelolaan sistem manajemen keamanan informasi.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 21

Cukup jelas.

Pasal 22

Ayat (1)

Cukup jelas.

Ayat (2)

Yang dimaksud dengan “Informasi Elektronik dan/atau Dokumen Elektronik yang dapat dipindahtangankan” adalah surat berharga atau surat yang berharga dalam bentuk elektronik.

Yang dimaksud dengan “Informasi Elektronik dan/atau Dokumen Elektronik harus unik” adalah Informasi Elektronik dan/atau Dokumen Elektronik dan/atau pencatatan Informasi dan/atau Dokumen Elektronik tersebut merupakan satu-satunya yang merepresentasikan satu nilai tertentu.

Yang dimaksud dengan “Informasi Elektronik dan/atau Dokumen Elektronik harus menjelaskan penguasaan” adalah Informasi Elektronik dan/atau Dokumen Elektronik tersebut harus menjelaskan sifat penguasaan yang direpresentasikan dengan sistem kontrol atau sistem pencatatan atas Informasi Elektronik dan/atau Dokumen Elektronik yang bersangkutan.

Yang dimaksud dengan “Informasi Elektronik dan/atau Dokumen Elektronik harus menjelaskan kepemilikan” adalah Informasi Elektronik dan/atau Dokumen Elektronik tersebut harus menjelaskan sifat kepemilikan yang direpresentasikan oleh adanya sarana kontrol teknologi yang menjamin hanya ada satu salinan yang sah (*single authoritative copy*) dan tidak berubah.

Pasal 23

Yang dimaksud dengan “interoperabilitas” adalah kemampuan Sistem Elektronik yang berbeda untuk dapat bekerja secara terpadu.

Yang dimaksud dengan ”kompatibilitas” adalah kesesuaian Sistem Elektronik yang satu dengan Sistem Elektronik yang lainnya.

Pasal 24

Ayat (1)

Cukup jelas.

Ayat (2)

Contoh edukasi yang dapat disampaikan kepada Pengguna Sistem Elektronik adalah:

a. menyampaikan kepada Pengguna Sistem Elektronik akan pentingnya menjaga keamanan *Personal Identification Number* (*PIN*)/*password* misalnya:

1. merahasiakan dan tidak memberitahukan *PIN*/*password* kepada siapapun termasuk kepada petugas penyelenggara;
2. melakukan perubahan *PIN*/*password* secara berkala;
3. menggunakan *PIN*/*password* yang tidak mudah ditebak (penggunaan identitas pribadi seperti tanggal lahir);
4. tidak mencatat *PIN*/*password*; dan
5. *PIN* untuk satu produk hendaknya berbeda dari *PIN* produk lainnya.

b. menyampaikan kepada Pengguna Sistem Elektronik mengenai berbagai modus kejahatan Transaksi Elektronik; dan

c. menyampaikan kepada Pengguna Sistem Elektronik mengenai prosedur dan tata cara pengajuan klaim.

Pasal 25

Kewajiban menyampaikan informasi kepada Pengguna Sistem Elektronik dimaksudkan untuk melindungi kepentingan Pengguna Sistem Elektronik.

Pasal 26

Ayat (1)

Penyediaan fitur dimaksudkan untuk melindungi hak atau kepentingan Pengguna Sistem Elektronik.

Ayat (2)

Cukup jelas.

Pasal 27

Cukup jelas.

Pasal 28

Cukup jelas.

Pasal 29

Cukup jelas.

Pasal 30

Cukup jelas.

Pasal 31

Ayat (1)

Cukup jelas.

Ayat (2)

Standar dan/atau persyaratan teknis Sertifikasi Kelaikan Sistem Elektronik memuat antara lain ketentuan mengenai pendaftaran, persyaratan audit, dan tata cara uji coba.

Ayat (3)

Cukup jelas.

Pasal 32

Cukup jelas.

Pasal 33

Cukup jelas.

Pasal 34

Ayat (1)

Cukup jelas.

Ayat (2)

Huruf a

Yang dimaksud dengan bentuk "visual" adalah tampilan yang dapat dilihat atau dibaca, antara lain tampilan grafis suatu *website*.

Huruf b

Yang dimaksud dengan bentuk "audio" adalah segala sesuatu yang dapat didengar, antara lain layanan telemarketing.

Huruf c

Contoh bentuk data elektronik adalah *electronic data capture* (*EDC*), *radio frequency identification* (*RFI*), dan *barcode recognition*.

Electronic data capture (*EDC*) adalah Agen Elektronik untuk dan atas nama Penyelenggara Sistem Elektronik yang bekerjasama dengan penyelenggara jaringan. *EDC* dapat digunakan secara mandiri oleh lembaga keuangan bank dan/atau bersama-sama dengan lembaga keuangan atau nonkeuangan lainnya.

Dalam hal Transaksi Elektronik dilakukan dengan menggunakan kartu Bank X pada *EDC* milik Bank Y, maka Bank Y akan meneruskan transaksi tersebut kepada Bank X, melalui penyelenggara jaringan tersebut.

Huruf d

Cukup jelas.

Pasal 35

Ayat (1)

Huruf a

Informasi tentang identitas penyelenggara Agen Elektronik paling sedikit memuat logo atau nama yang menunjukkan identitas.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 36

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Yang dimaksud dengan "perlakuan yang sama" antara lain pemberlakuan tarif, fasilitas, persyaratan, dan prosedur yang sama.

Ayat (4)

Cukup jelas.

Pasal 37

Cukup jelas.

Pasal 38

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Huruf a

Yang dimaksud dengan "kerahasiaan" adalah sesuai dengan konsep hukum tentang kerahasiaan (*confidentiality*) atas informasi dan komunikasi secara elektronik.

Huruf b

Yang dimaksud dengan "integritas" adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas informasi elektronik.

Huruf c

Yang dimaksud dengan "ketersediaan" adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas informasi elektronik.

Huruf d

Yang dimaksud dengan "keautentikan" adalah sesuai dengan konsep hukum tentang keautentikan (*authentication*) yang mencakup keaslian (originalitas) atas isi suatu informasi elektronik.

Huruf e

Yang dimaksud dengan "otorisasi" adalah sesuai dengan konsep hukum tentang otorisasi (*authorization*) berdasarkan lingkup tugas dan fungsi pada suatu organisasi dan manajemen.

Huruf f

Yang dimaksud dengan "kenirsangkalan" adalah sesuai dengan konsep hukum tentang nirsangkal (*nonrepudiation*).

Pasal 39

Ayat (1)

Huruf a

Dalam melakukan pengujian keautentikan identitas dan memeriksa otorisasi Pengguna Sistem Elektronik, perlu memperhatikan antara lain:

1. kebijakan dan prosedur tertulis untuk memastikan kemampuan untuk menguji keautentikan identitas dan memeriksa kewenangan Pengguna Sistem Elektronik;
2. metode untuk menguji keautentikan; dan
3. kombinasi paling sedikit 2 (dua) faktor autentikasi (*two factor authentication*) adalah *"what you know"* (*PIN/password*), "*what you have*" (kartu magnetis dengan *chip*, *token*, *digital signature*), "*what you are*" atau "biometrik" (retina dan sidik jari).

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Perlindungan terhadap kerahasiaan Data Pribadi Pengguna Sistem Elektronik juga harus dipenuhi dalam hal penyelenggara menggunakan jasa pihak lain (*outsourcing*).

Huruf e

Cukup jelas.

Huruf f

Cukup jelas.

Huruf g

Prosedur penanganan tersebut juga harus dipenuhi dalam hal penyelenggara menggunakan jasa pihak lain (*outsourcing*).

Ayat (2)

Dalam menyusun dan menetapkan prosedur untuk menjamin transaksi tidak dapat diingkari oleh Pengguna Sistem Elektronik harus memperhatikan:

a. sistem Transaksi Elektronik telah dirancang untuk mengurangi kemungkinan dilakukannya transaksi secara tidak sengaja (*unintended*) oleh para pengguna yang berhak;

b. seluruh identitas pihak yang melakukan transaksi telah diuji keautentikan atau keasliannya; dan

c. data transaksi keuangan dilindungi dari kemungkinan pengubahan dan setiap pengubahan dapat dideteksi.

Pasal 40

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Huruf a

Yang dimaksud dengan “antar-Pelaku Usaha” adalah Transaksi Elektronik dengan model transaksi *business to business*.

Huruf b

Yang dimaksud dengan “antara Pelaku Usaha dengan konsumen” adalah Transaksi Elektronik dengan model transaksi *business to consumer*.

Huruf c

Yang dimaksud dengan “antarpribadi” adalah Transaksi Elektronik dengan model transaksi *consumer to consumer*.

Huruf d

Yang dimaksud dengan “antar-Instansi” adalah Transaksi Elektronik dengan model transaksi antar-Instansi.

Huruf e

Cukup jelas.

Ayat (4)

Cukup jelas.

Pasal 41

Cukup jelas.

Pasal 42

Cukup jelas.

Pasal 43

Ayat (1)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Jaringan Sistem Elektronik adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup atau terbuka.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 44

Ayat (1)

Ketentuan ini dimaksudkan untuk melindungi Pengguna Sistem Elektronik dari pengiriman Informasi Elektronik yang bersifat mengganggu (*spam*).

Contoh bentuk *spam* yang umum dikenal misalnya *spam* e-mail, *spam* pesan instan, *spam* *usenet newsgroup*, *spam* mesin pencari informasi web (*web search engine spam*), *spam* blog, *spam* berita pada telepon genggam, dan *spam* forum Internet.

Ayat (2)

Cukup jelas.

Pasal 45

Cukup jelas.

Pasal 46

Ayat (1)

Cukup jelas.

Ayat (2)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Yang dimaksud dengan “kewajaran” adalah mengacu pada unsur kepatutan yang berlaku sesuai dengan kebiasaan atau praktik bisnis yang berkembang.

Pasal 47

Ayat (1)

Contoh Transaksi Elektronik dapat mencakup beberapa bentuk atau varian antara lain:

a. kesepakatan tidak dilakukan secara elektronik namun pelaksanaan hubungan kontraktual diselesaikan secara elektronik;

b. kesepakatan dilakukan secara elektronik dan pelaksanaan hubungan kontraktual diselesaikan secara elektronik; dan

c. kesepakatan dilakukan secara elektronik dan pelaksanaan hubungan kontraktual diselesaikan tidak secara elektronik.

Ayat (2)

Cukup jelas.

Pasal 48

Ayat (1)

Cukup jelas.

Ayat (2)

Peraturan perundang-undangan dimaksud antara lain Undang-Undang tentang Perlindungan Konsumen.

Ayat (3)

Cukup jelas.

Pasal 49

Cukup jelas.

Pasal 50

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Huruf a

Tindakan penerimaan yang menyatakan persetujuan antara lain dengan mengklik persetujuan secara elektronik oleh Pengguna Sistem Elektronik.

Huruf b

Cukup jelas.

Pasal 51

Ayat (1)

Cukup jelas.

Ayat (2)

Yang dimaksud dengan "secara setimbang" adalah memperhatikan kepentingan kedua belah pihak secara adil (*fair*).

Pasal 52

Ayat (1)

Tanda Tangan Elektronik berfungsi sebagaimana tanda tangan manual dalam hal merepresentasikan identitas Penanda Tangan. Dalam hal pembuktian keaslian (autentikasi) tanda tangan manual dapat dilakukan melalui verifikasi atau pemeriksaan terhadap spesimen Tanda Tangan Elektronik dari Penanda Tangan.

Pada Tanda Tangan Elektronik, Data Pembuatan Tanda Tangan Elektronik berperan sebagai spesimen Tanda Tangan Elektronik dari Penanda Tangan.

Tanda Tangan Elektronik harus dapat digunakan oleh para ahli yang berkompeten untuk melakukan pemeriksaan dan pembuktian bahwa Informasi Elektronik yang ditandatangani dengan Tanda Tangan Elektronik tersebut tidak mengalami perubahan setelah ditandatangani.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 53

Cukup jelas.

Pasal 54

Ayat (1)

Akibat hukum dari penggunaan Tanda Tangan Elektronik tersertifikasi atau yang tidak tersertifikasi berpengaruh terhadap kekuatan nilai pembuktian.

Tanda Tangan Elektronik yang tidak tersertifikasi tetap mempunyai kekuatan nilai pembuktian meskipun relatif lemah karena masih dapat ditampik oleh yang bersangkutan atau relatif dapat dengan mudah diubah oleh pihak lain.

Dalam praktiknya perlu diperhatikan rentang kekuatan nilai pembuktian dari Tanda Tangan Elektronik yang bernilai pembuktian lemah, seperti tanda tangan manual yang dipindai (*scanned*) menjadi Tanda Tangan Elektronik sampai dengan Tanda Tangan Elektronik yang bernilai pembuktian paling kuat, seperti Tanda Tangan Digital yang diterbitkan oleh penyelenggara sertifikasi elektronik yang tersertifikasi.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 55

Ayat (1)

Yang dimaksud dengan “unik” berarti setiap kode apapun yang digunakan atau difungsikan sebagai Data Pembuatan Tanda Tangan Elektronik harus merujuk hanya pada satu subjek hukum atau satu entitas yang merepresentasikan satu identitas.

Ayat (2)

Cukup jelas.

Ayat (3)

Huruf a

Cukup jelas.

Huruf b

Data Pembuatan Tanda Tangan Elektronik yang dihasilkan dengan teknik kriptografi pada umumnya memiliki korelasi matematis berbasis probabilitas dengan data verifikasi Tanda Tangan Elektronik. Oleh sebab itu

pemilihan kode kriptografi yang akan digunakan harus mempertimbangkan kecukupan tingkat kesulitan yang dihadapi dan sumber daya yang harus disiapkan oleh pihak yang mencoba memalsukan Data Pembuatan Tanda Tangan Elektronik.

Huruf c

Yang dimaksud dengan "media elektronik" adalah fasilitas, sarana, atau perangkat yang digunakan untuk mengumpulkan, menyimpan, memproses, dan/atau menyebarkan Informasi Elektronik yang digunakan untuk sementara atau permanen.

Huruf d

Yang dimaksud dengan "data yang terkait dengan Penanda Tangan" adalah semua data yang dapat digunakan untuk mengidentifikasi jati diri Penanda Tangan seperti nama, alamat, tempat dan tanggal lahir, serta kode spesimen tanda tangan manual.

Yang dimaksud dengan "sistem terpercaya" adalah sistem yang mengikuti prosedur penggunaan Tanda Tangan Elektronik yang memastikan autentitas dan integritas Informasi Elektronik. Hal tersebut dapat dilihat dengan memperhatikan beberapa faktor, antara lain:

1. keuangan dan sumber daya;
2. kualitas Perangkat Keras dan Perangkat Lunak;
3. prosedur sertifikat dan aplikasi serta retensi data;
4. ketersediaan Data Pembuatan Tanda Tangan Elektronik; dan
5. audit oleh lembaga independen.

Ayat (4)

Cukup jelas.

Pasal 56

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Keharusan adanya 3 (tiga) unsur yang menjadi masukan pada saat terjadinya proses penandatanganan dan memiliki pengaruh terhadap Tanda Tangan Elektronik yang dihasilkan pada proses tersebut akan menjamin keautentikan Tanda Tanda Elektronik, Informasi Elektronik yang ditandatangani serta waktu penandatanganan.

Ayat (5)

Contoh dari ketentuan ini adalah sebagai berikut:

a. Perubahan terhadap Tanda Tangan Elektronik setelah waktu penandatanganan harus mengakibatkan Informasi Elektronik yang dilekatinya tidak berfungsi sebagaimana mestinya, rusak, atau tidak dapat ditampilkan jika Tanda Tangan Elektronik dilekatkan dan/atau terkait pada Informasi Elektronik yang ditandatangani.

   Teknik melekatkan dan mengaitkan Tanda Tangan Elektronik pada Informasi Elektronik yang ditandatangani dapat menimbulkan terjadinya Informasi Elektronik atau Dokumen Elektronik baru yang:

   1. terlihat sebagai satu kesatuan yang tidak dapat dipisahkan; atau
   2. tampak terpisah dan Informasi Elektronik yang ditandatangani dapat dibaca oleh orang awam sementara Tanda Tangan Elektronik berupa kode dan/atau gambar.

b. Perubahan terhadap Tanda Tangan Elektronik setelah waktu Penandatanganan harus mengakibatkan sebagian atau seluruh Informasi Elektronik tidak valid atau tidak berlaku jika Tanda Tangan Elektronik terasosiasi logis dengan Informasi Elektronik yang ditandatanganinya.

   Perubahan yang terjadi terhadap Informasi Elektronik yang ditandatangani harus menyebabkan ketidaksesuaian antara Tanda Tangan Elektronik dengan Informasi Elektronik terkait yang dapat dilihat dengan jelas melalui mekanisme verifikasi.

Pasal 57

Ayat (1)

Yang dimaksud dengan “bertanggung jawab atas penggunaan Data Pembuatan Tanda Tangan Elektronik atau alat pembuat Tanda Tangan Elektronik” adalah Penyelenggara Tanda

Tangan Elektronik atau Pendukung Layanan Tanda Tangan Elektronik harus dapat menyediakan sistem penelusuran yang dapat membuktikan ada atau tidaknya penyalahgunaan Data Pembuatan Tanda Tangan Elektronik dan/atau alat pembuat Tanda Tangan Elektronik.

Ayat (2)

Keharusan penerapan teknik kriptografi untuk mengamankan proses pengiriman dan penyimpanan Tanda Tangan Elektronik dimaksudkan untuk menjamin integritas Tanda Tangan Elektronik. Pemilihan teknik kriptografi yang diterapkan untuk keperluan tersebut harus mengacu pada ketentuan atau standar kriptografi yang berlaku sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 58

Ayat (1)

Cukup jelas.

Ayat (2)

Faktor autentikasi yang dapat dipilih untuk dikombinasikan dapat dibedakan dalam 3 (tiga) jenis, yakni:

a. sesuatu yang dimiliki secara individu (*what you have*) misalnya kartu ATM atau *smart card*;

b. sesuatu yang diketahui secara individu (*what you know*) misalnya *PIN*/*password* atau kunci kriptografi; dan

c. sesuatu yang merupakan ciri/karakteristik seorang individu (*what you are*) misalnya pola suara (*voice pattern*), dinamika tulisan tangan (*handwriting dynamics*), atau sidik jari (*fingerprint*).

Ayat (3)

Cukup jelas.

Pasal 59

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Kepemilikan Sertifikat Elektronik merupakan salah satu upaya untuk meningkatkan keamanan penyelenggaraan Sistem Elektronik selain upaya keamanan lainnya.

Kepemilikan Sertifikat Elektronik berfungsi mendukung keamanan penyelenggaraan Sistem Elektronik yang mencakup antara lain kerahasiaan, keautentikan, integritas, dan kenirsangkalan (*non-repudiation*).

Ayat (4)

Cukup jelas.

Ayat (5)

Peraturan Menteri memuat antara lain pengaturan mengenai tata cara mengajukan permohonan sertifikasi elektronik yang dapat disampaikan melalui notaris.

Pasal 60

Huruf a

Yang dimaksud dengan pemeriksaan calon pemilik dan/atau pemegang Sertifikat Elektronik adalah pemeriksaan keberadaan fisik calon pemilik dan/atau pemegang Sertifikat Elektronik.

Huruf b

Cukup jelas.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Huruf f

Cukup jelas.

Pasal 61

Ayat (1)

Cukup jelas.

Ayat (2)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Yang dimaksud dengan "penyelenggara sertifikasi elektronik yang memperoleh pengakuan status berinduk" adalah penyelenggara sertifikasi elektronik yang menerbitkan Sertifikat Elektronik dengan menggunakan Tanda Tangan Elektronik *Root Certification Authority* yang dikeluarkan oleh Menteri.

Pasal 62

Cukup jelas.

Pasal 63

Cukup jelas.

Pasal 64

Cukup jelas.

Pasal 65

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Terhadap Sertifikat Keandalan yang dikeluarkan oleh Lembaga Sertifikasi Keandalan asing yang tidak terdaftar, tidak memiliki kekuatan pembuktian yang sempurna.

Pasal 66

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Huruf a

Cukup jelas.

Huruf b

Contoh “status dan kompetensi subjek hukum” adalah kedudukan Pelaku Usaha sebagai produsen, pemasok, atau penyelenggara maupun perantara.

Huruf c

Cukup jelas.

Huruf d

Cukup jelas.

Pasal 67

Cukup jelas.

Pasal 68

Ayat (1)

Huruf a

Pengamanan terhadap identitas (*identity seal*) merupakan Sertifikat Keandalan yang jaminan keandalannya sebatas pengamanan bahwa identitas Pelaku Usaha adalah benar. Validasi yang dilakukan oleh Lembaga Sertifikasi Keandalan hanya terhadap identitas Pelaku Usaha yang paling sedikit memuat nama subjek hukum, status subjek hukum, alamat atau kedudukan, nomor telepon, alamat email, izin usaha, dan Nomor Pokok Wajib Pajak (NPWP).

Lembaga Sertifikasi Keandalan yang menerbitkan Sertifikat Keandalan ini memberikan kepastian penelusuran bahwa identitas Pelaku Usaha adalah benar.

Huruf b

Pengamanan terhadap pertukaran data (*security seal*) merupakan Sertifikat Keandalan yang jaminan keandalannya memberikan kepastian bahwa proses penyampaian atau pertukaran data melalui website Pelaku Usaha dilindungi keamanannya dengan menggunakan teknologi pengamanan proses pertukaran data (contoh: protokol SSL/*secure socket layer*).

Sertifikat Keandalan ini menjamin bahwa terdapat sistem pengamanan dalam proses pertukaran data yang telah teruji.

Huruf c

Pengamanan terhadap kerawanan (*vulnerability seal*) merupakan Sertifikat Keandalan yang jaminan keandalannya adalah memberikan kepastian bahwa terdapat sistem manajemen keamanan informasi yang diterapkan oleh Pelaku Usaha dengan mengacu pada standar pengamanan Sistem Elektronik tertentu berdasarkan ketentuan peraturan perundang-undangan.

Huruf d

Pemeringkatan konsumen (*consumer rating seal*) merupakan Sertifikat Keandalan yang jaminan keandalannya memberikan peringkat tertentu bahwa berdasarkan penilaian subjektif kepuasan konsumen terhadap layanan Transaksi Elektronik yang diselenggarakan Pelaku Usaha telah memberikan kepuasan konsumen.

Sertifikat ini memberikan jaminan bahwa Pelaku Usaha telah mendapatkan pengakuan kepuasan konsumen berdasarkan pengalaman yang nyata dari konsumen meliputi proses pratransaksi, transaksi, dan pasca transaksi.

Huruf e

Pengamanan terhadap kerahasiaan Data Pribadi (*privacy seal*) merupakan Sertifikat Keandalan yang jaminan keandalannya adalah memberikan kepastian bahwa Data Pribadi konsumen dilindungi kerahasiaannya sebagaimana mestinya.

Ayat (2)

Cukup jelas.

Pasal 69

Ayat (1)

Cukup jelas.

Ayat (2)

Yang dimaksud dengan “profesi” adalah keahlian tertentu yang dimiliki oleh seseorang yang diakui atau disahkan oleh pemerintah.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Peraturan Menteri memuat antara lain, pendaftaran dan persyaratan untuk ditetapkan sebagai profesi dalam lingkup Teknologi Informasi yang dapat turut serta dalam pembentukan Lembaga Sertifikasi Keandalan.

Pasal 70

Cukup jelas.

Pasal 71

Cukup jelas.

Pasal 72

Cukup jelas.

Pasal 73

Ayat (1)

Cukup jelas.

Ayat (2)

Huruf a

Yang dimaksud dengan "Nama Domain tingkat tinggi generik" adalah Nama Domain tingkat tinggi yang terdiri atas tiga atau lebih karakter dalam hierarki sistem penamaan domain selain domain tingkat tinggi Negara (*country code Top Level Domain*). Contoh .nusantara atau .java.

Huruf b

Yang dimaksud dengan "Nama Domain tingkat tinggi Indonesia" adalah domain tingkat tinggi dalam hierarki sistem penamaan domain yang menunjukkan kode Indonesia (.id) sesuai daftar kode negara dalam ISO 3166-1 yang dikeluarkan oleh *Internet Assigned Numbers Authority* (IANA).

Huruf c

Contoh Nama Domain Indonesia tingkat kedua adalah co.id, go.id, ac.id, or.id, atau mil.id.

Huruf d

Contoh Nama Domain Indonesia tingkat turunan adalah kominfo.go.id.

Ayat (3)

Huruf a

Termasuk dalam lingkup pengertian Registri Nama Domain ialah fungsi dan peran ccTLD manager.

Huruf b

Cukup jelas.

Pasal 74

Cukup jelas.

Pasal 75

Cukup jelas.

Pasal 76

Cukup jelas.

Pasal 77

Cukup jelas.

Pasal 78

Cukup jelas.

Pasal 79

Cukup jelas.

Pasal 80

Cukup jelas.

Pasal 81

Cukup jelas.

Pasal 82

Cukup jelas.

Pasal 83

Cukup jelas.

Pasal 84

Ayat (1)

Pengenaan sanksi dalam ketentuan ini hanya ditujukan bagi pihak yang melakukan pelanggaran administratif, sedangkan mengenai pelanggaran yang bersifat moral atau keperdataan tidak dikenakan sanksi administratif.

Ayat (2)

Huruf a

Cukup jelas.

Huruf b

Cukup jelas.

Huruf c

Penghentian sementara dalam ketentuan ini berupa penghentian sebagian atau seluruh komponen atau layanan pada Sistem Elektronik yang bersangkutan untuk jangka waktu tertentu.

Huruf d

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat (5)

Cukup jelas.

Pasal 85

Cukup jelas.

Pasal 86

Cukup jelas.

Pasal 87

Cukup jelas.

Pasal 88

Cukup jelas.

Pasal 89

Cukup jelas.

Pasal 90

Cukup jelas.