

BAB V

KONTRIBUSI *TRUSTMARK* DALAM MENINGKATKAN KETERPERCAYAAN DALAM DUNIA BISNIS DAN MELINDUNGI KONSUMEN PENGGUNA *E COMMERCE*

A. *Trustmark* untuk Meningkatkan Keterpercayaan dalam *E Commerce*

Trustmark merupakan label elektronik yang menunjukkan bahwa *e-mearchant* atau pedagang *online* telah menunjukkan kesesuaian terhadap standar keamanan, privasi, dan praktik bisnis.²¹¹ TMOS atau *Trustmark* Organisasi didefinisikan sebagai Pihak Ketiga Terpercaya, *Trustmark* Organisasi ini merupakan pihak-pihak yang bisa dipercaya dan diandalkan. Organisasi ini merupakan pihak independen (pihak ketiga) dan memberikan *Trustmarks* (label atau representasi visual yang menunjukkan bahwa produk, proses atau jasa sesuai dengan karakteristik kualitas tertentu) untuk pedagang *online* (*emerchants*).²¹²

Kepercayaan adalah proses dinamis yang dapat memperdalam atau mundur dari waktu ke waktu berdasarkan pengalaman. Jenis kepercayaan juga berkembang dari waktu ke waktu. Pada bisnis *online*, kepercayaan vendor *e-commerce* diperdalam dengan melewati tahap pembangunan, konfirmasi dan pemeliharaan.²¹³ Instrumen penting untuk meningkatkan kepercayaan konsumen adalah melalui kode etik dan kualitas segel atau tanda kepercayaan (*Trustmark*). Berbagai organisasi konsumen di negara-negara Eropa meluncurkan *Trustmark* untuk situs web komersial yang didukung oleh kode etik. Sebuah penyedia layanan elektronik yang mempergunakan *Trustmark* menyanggupi untuk mengawai kondisi yang menjadi hak organisasi konsumen

²¹¹Electronic labels or visual representations indicating that an e-mearchant has demonstrated its conformity to standards regarding, e.g., security, privacy, and business practice. Paolo Balboni, Partner at ICT Legal Consulting & Director of the European Privacy Association, *Trustmark in e commerce scheme, The Book Trustmark in E Commerce*.

²¹²TMOs – also defined as Trusted Third Parties, parties that can be trusted and relied on – are organizations which present themselves as independent parties (third parties) and provide trustmarks (a label or visual representation indicating that a product, process or service conforms to specific quality characteristics) to online merchants (*emerchants*). Ibid. PP. 6

²¹³Head, M., and Hassanein, K. (2002). "Trust in e-Commerce: Evaluating the Impact of Third-Party Seals", *Quarterly Journal of Electronic Commerce*, 3(3), 307-325.

atau kelompok kepentingan tertentu. Di negara Uni Eropa asosiasi konsumen di delapan negara anggota mengembangkan *Trustmark* nasional untuk penjualan yang dilakukan melalui Internet.²¹⁴

Pada penelitian Xianguang Sheng & Lorrie Faith Cranor mengatakan bahwa,

*The US Federal Trade Commission's online privacy activities in the mid 1990s led to several self-regulatory initiatives to improve data privacy practices, including the BBBOnline and TRUSTe privacy seal programs. Each of these initiatives requires participating entities to post privacy notices that conform to guidelines based on the Fair Information Practice Principles. TRUSTe was founded in 1997 by the Electronic Frontier Foundation and the CommerceNet Consortium. The TRUSTe program evolved over time, going through a number of major revisions. TRUSTe awards a "trustmark" to Web sites that agree to adhere to a set of privacy principles and agree to comply with ongoing TRUSTe oversight and consumer complaint resolution procedures. About 2000 Web sites had TRUSTe seals in 2005. The BBBOnline privacy program is operated by the Council of Better Business Bureaus and is similar to the TRUSTe program. As of January 2005, 630 Web sites had BBBOnline privacy seals. As every trust mark has its own criteria and code of conduct, a complete list of aspects will not be published in this report. However, the working group has chosen to highlight a number of criteria that illustrates the differences and individual composition of some trust marks.*²¹⁵

Penelitian tersebut mengatakan bahwa kegiatan privasi *online US Federal Trade Commission* pada pertengahan 1990 membuat beberapa inisiatif *self-regulatory* untuk meningkatkan praktik privasi data, termasuk privasi Trustmark BBBOnline dan TRUSTe. Masing-masing inisiatif ini membutuhkan entitas yang berpartisipasi untuk mengirim pemberitahuan privasi yang sesuai dengan pedoman berdasarkan Prinsip Praktek Informasi *Fair*. TRUSTe didirikan pada tahun 1997 oleh *Frontier Foundation Elektronik* dan *Konsorsium CommerceNet*. Program TRUSTe berkembang dari waktu ke waktu, akan melalui beberapa revisi utama. TRUSTe penghargaan sebagai

²¹⁴J. E. J. PRINS, Consumers, Liability, and the Online World. *Information & Communication Technology Law* Vol. 12, No. 2, June 2003. Pp. 159

²¹⁵ Xianguang Sheng & Lorrie Faith Cranor An Evaluation of the Effect of US Financial Privacy Legislation Through the Analysis of Privacy Policies. *I/S: A Journal of Law and Policy* [Vol. 2:3]

Trustmark ke situs *Web* yang setuju untuk mematuhi seperangkat prinsip privasi dan setuju untuk mematuhi TRUSTe pengawasan dan prosedur penyelesaian pengaduan konsumen yang sedang berlangsung. Sekitar 2000 situs web telah TRUSTe segel pada tahun 2005. Program privasi BBBOnline dioperasikan oleh Dewan *Better Business Biro* dan mirip dengan program TRUSTe. Pada Januari 2005, 630 situs web memiliki segel privasi BBBOnline. Setiap *Trustmark* memiliki kriteria dan kode etik tersendiri.

Trustmark memiliki kriteria dan kode etik tersendiri, sebagai contoh pada pengaturan *Trustmark* yang terdapat pada negara-negara berikut:

1. Eropa

Sebagai upaya untuk membangun *Trust* pada lingkungan *Online* yang merupakan kunci perkembangan ekonomi dan sosial maka di buat Regulasi (EU) Nomor 910/2014 tentang identitas elektronik dan pelayanan *Trust* untuk transaksi elektronik. Regulasi ini bertujuan membangun kepercayaan konsumen, bisnis dan masyarakat terhadap pelayanan melalui transaksi elektronik.

2. Austria.

Keluhan (dan pertanyaan) harus dijawab dalam waktu dua hari kerja. (*Osterreichisches E-Commerce-Gutezeichen*). Syarat dan ketentuan yang dibuat pelaku usaha harus mudah dimengerti (*E-Commerce* dan *M-Commerce*).

3. Belgia:

Pedagang tidak akan mendorong anak-anak untuk memesan produk / jasa, keluhan anggota dianggap sah, tanda kepercayaan bisa memaksakan satu (atau beberapa hukuman sebagai berikut: Peringatan, Menyalahkan Baik (minimal 1.000 Euro dan maksimum 50 000 Euro), Suspensi keanggotaan, Pengecualian (*BeCommerce*).

4. Republik Ceko:

Informasi kepada konsumen mengenai pelaku usaha melebihi hukum nasional.

5. Jerman.

Keamanan Data: rencana yang konsisten untuk menangani gangguan dan keadaan darurat operasional telah ditetapkan. Rencana ini termasuk nama-nama orang yang bertanggung jawab dan / atau peran dan kewenangan mereka. Dalam kasus pencabutan atau mengembalikan semua pembayaran yang dilakukan harus dikembalikan dalam waktu 30 hari. Ada aturan untuk yang menimbulkan biaya pengiriman kembali. *Trustmark* akan memastikan melalui kriteria yang aturan spesifik negara tentang periode pengembalian yang diikuti.

6. Denmark:

Toko *online* harus dirancang agar mudah dan mudah untuk membatalkan kontrak anak-anak dan remaja. Pada saat yang sama anak-anak dan orang muda tidak akan diminta untuk memberikan informasi pribadi tanpa persetujuan orang tua. (*E-market*).

7. Estonia

Website harus beroperasi selama setidaknya satu tahun.

8. Spanyol:

Menjamin adanya bagian terpisah tentang perlindungan anak di bawah umur dan persyaratan untuk memastikan bahwa penyandang cacat dapat menggunakan situs pedagang. Kode etik ditinjau kembali setiap tahun ke-4.

9. Finlandia:

Kontak digital dengan pedagang harus dijawab dalam waktu satu hari kerja. Syarat dan ketentuan mengenai garansi komersial harus selalu menyatakan bahwa konsumen juga memiliki hak hukum sesuai dengan undang-undang perlindungan konsumen.

10. Prancis:

Konsumen berhak "mengevaluasi" pemenuhan kepercayaan atas pedagang dan menandai kriteria setelah pembelian. Evaluasi tersebut kemudian ditindaklanjuti oleh tanda *Trustmark* dalam rangka untuk memastikan kepatuhan. *commit to user*

11. Yunani:

Trustmark menawarkan pemutusan kontrak jika barang yang dipesan tidak tersedia, *Trustmark* juga menawarkan jaminan uang kembali.

12. Belanda:

Anggota *Trustmark* menawarkan diperpanjang *cooling period* dibandingkan dengan hukum nasional. Jaminan Cek keuangan tahunan anggota. *Trustmark* menjamin bahwa konsumen akan diganti jika anggota tersebut bangkrut. Konsumen selalu dapat beralih ke pelaku usaha untuk keluhan atau bantuan, bahkan jika pelaku usaha tidak menyediakan barang atau jasa. Pelaku usaha tidak menjual kepada anak di bawah umur tanpa persetujuan dari orang tua.

13. Singapore

Singapore memiliki tiga sistem *Trustmark* yaitu *TrustSg*, *CASETRUST* and *CONSUMERTRUST*. *TrustSg* dikembangkan oleh *National Trust Council* (NTC). *CASETRUST* dikelola oleh *Consumers Association of Singapore* (CASE). *CONSUMERTRUST* dibentuk dan dioperasikan oleh *CommerceNet Singapore*²¹⁶

National Internet Advisory Committee membentuk aturan khusus mengenai *E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce*" (Code). Kode ini bertujuan untuk memberikan keyakinan dan kepercayaan konsumen atas bisnis dan informasi data pribadi pengguna. *Info-Communications Development Authority* (IDA), merupakan agen pertama yang membuat regulasi *e commerce* dan menggunakan sistem *TRUSTe* sebagai industri penjamin *website*²¹⁷

²¹⁶Background Report For Mutual Understandings On B2C Legal Framework In Asia-Pacific Countries, Japan External Trade Organization Industry and Technology Department, 2002. PP. 19

²¹⁷EPIC Privacy and Human Rights Report 2006
<http://www.worldlii.org/int/journals/EPICPHR/2006/PHR2006-Republic-24.html>, Diakses 30 Maret 2015 Jam 10.32 WIB

14. Malaysia

Sebanyak 92 perusahaan di Malaysia telah memiliki sertifikat penjamin keamanan dari *CyberSecurity Malaysia (CSM)*. CSM's telah melakukan sertifikasi atas 41 produk ICT dan 29 *website e bisnis* yang telah di validasi *Malaysia Trustmark Service*. Malaysia ranking ke tiga diantara 193 anggota ITU (*International Telecommunications Union*) yang memiliki komitmen tinggi terhadap keamanan di internet.²¹⁸ CSM telah meluncurkan MyTrustSEAL, merupakan pelayanan atas audit dan validitas *website e commerce* dan pelaku usaha sehingga dapat dengan mudah diidentifikasi oleh pengguna internet. Perusahaan yang telah mampu melewati kriteria memberikan kepuasan kepada konsumen akan menerima *Malaysia Trustmark certificate* yang dapat diupload pada *website e commerce*.²¹⁹

15. Indonesia

Di Indonesia Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik juga mengatur agar pelaku usaha yang menyelenggarakan sistem elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan (Pasal 10 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik). Pasal 41 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggara sistem dan Transaksi elektronik juga dijelaskan bahwa Penyelenggaraan Transaksi Elektronik dalam lingkup publik atau privat yang menggunakan Sistem Elektronik untuk kepentingan pelayanan publik wajib menggunakan Sertifikat keandalan. Salah satu standar yang diperlukan untuk memfasilitasi sistem transaksi elektronik adalah adanya standar sertifikasi keandalan (*trustmark*). Sertifikat keandalan akan dimiliki pelaku usaha jika memenuhi beberapa persyaratan. Seperti lolos standar perangkat keras, perangkat lunak, standar tenaga ahli, keamanan data, dan pengelola data. Terkait hal ini, sertifikasi

²¹⁸Malaysian organisations get international accreditation via CSM
<https://www.digitalnewsasia.com/security/92-malaysian-organisations-get-international-accreditation-via-csm> Diakses Tanggal 30 Maret 2015 Jam 11.10 WIB

²¹⁹CSM rolls out MyTrustSEAL to reduce online fraud Digital News AsiaDec 12, 2014.
<https://www.digitalnewsasia.com/security/csm-rolls-out-mytrustseal-to-reduce-online-fraud>

bagi pelaku usaha dapat diperoleh dari lembaga sertifikasi keandalan Indonesia dan asing. Terkait dengan kegiatan transaksi elektronik yang lebih luas, saat ini pemerintah Indonesia belum memiliki standar yang dapat digunakan sebagai arahan yang spesifik untuk kegiatan transaksi elektronik.

Dari hasil penelitian yang telah penulis lakukan pada konsumen *pengguna e commerce* dikatakan bahwa,

“Saya sering melakukan pembelian melalui online, sebelum saya memutuskan untuk membeli barang yang ditawarkan pada website, saya hanya membandingkan barang sejenis pada website lain atau toko konvensional, kemudian saya akan mencoba menghubungi penjual melalui telepon untuk mengetahui detail kondisi barang bila ada nomor telepon yang bisa dihubungi, namun bila tidak ada yang tidak bisa dihubungi, bila saya sudah suka dengan barang tersebut saya akan segera melakukan pembayaran melalui transfer. Kebetulan selama ini tidak pernah ada masalah dengan barang yang saya order baik jenis barangnya maupun waktu pengirimannya”²²⁰

Lain halnya dengan yang dikatakan Khabib mengenai pembelian melalui *e commerce*,

“pada awalnya saya *browsing* pada situs lazada yang lumayan terkenal di Indonesia. Saya percaya saja karena karena yang saya tahu situs tersebut profesional dalam melakukan transaksi elektronik dan banyak orang berbelanja pada situs tersebut. Pada suatu saat saya melakukan transaksi pembelian barang elektronik seharga Rp.500.000,- pada bulan November 2015 namun barang yang saya pesan tersebut hingga saat ini Februari 2016 masih juga belum saya terima. Saya sudah berusaha menghubungi nomor telepon yang katanya *customer service* atas situs tersebut, namun yang menjawab hanya mesin penjawab otomatis. Kemudian saya juga mencoba mengirim email namun balasan emailnya sama hanya berupa step-step komplain tanpa ada solusi hingga saat ini”²²¹

Permasalahan senada juga di hadapi oleh konsumen Lazada khususnya dalam hal kasus refund untuk pembatalan sepihak oleh Lazada,

“Saya membeli HP ZTE Blade A711 di Lazada Indonesia dengan nomor pesanan: 392372329 tanggal 21 Desember 2015 seharga Rp. 1.900.000,- Handphone yang saya beli bermasalah dan tidak normal dan setelah chat

²²⁰Wawancara langsung dengan Abi buana jaya selaku konsumen *pengguna e commerce* di Surakarta pada 5 Februari 2016 jam 16.10 WIB

²²¹Wawancara langsung dengan Khabib Aliya selaku konsumen *pengguna e commerce* di Surakarta 15 Februari 2016 jam 10.00 WIB

dengan CS lazada sepakat dikembalikan. Tanggal 28 Desember 2015, unit saya kembalikan ke lazada dan sudah terverifikasi bahwa retur unit sudah diterima oleh lazada. Tanggal 4 Januari 2016 saya mendapatkan email bahwa refund dana yang sudah saya ajukan. Aturan dari lazada bahwa karena saya menggunakan BCAklikpay maka perlu 14 hari kerja maksimum. Maka kita hitung kapan uangnya harus masuk kalau email saya terima tanggal 4 Januari 2016 dan anggaplah di proses tanggal 5 Januari 2016, maka 14 hari kerja adalah tanggal 22 Januari 2016. Sampai dengan hari ini saya bolak balik email dan telpon ke lazada selalu dijawab untuk di tunggu refundnya. Saya sangat kecewa dan saat ditanya ke fanpage lazada dijawabnya silahkan konfirmasi ke bank. Nah, apa yang mau saya konfirmasi? Bukti refund saja tidak ada. Yang paling parah lazada bilang uang saya sudah di refund tanggal 5 Januari 2016 saya minta bukti refund sampai dengan hari ini tidak ada. Yang jelas sudah lebih dari 14 hari kerja uang belum ada di rekening saya. Harus bagaimana ? bawa golok ke kantor lazada gitu ?”²²²

Lebih lanjut tidak hanya konsumen akhir yang merasa di rugikan oleh manajemen lazada.co.id, namun seller pada lazada.co.id juga mengatakan,

“Sebagai salah satu *seller* di lazada.co.id saya sudah berjualan selama 1 tahun lebih. Saya tidak tahu lagi mau menulis email komplain kemana karena setiap kali email ke support lazada selalu tidak pernah terselesaikan dan tidak jelas. Katanya Lazada di support dengan sistem tapi pertanyaan saya kenapa untuk ongkos kirim saja selalu kurang dan kami para *seller* di suruh tetap mengirim kan produk tersebut atau kami akan dikenakan penalty Rp. 100.000. Contoh aktual pengiriman JNE dari Surabaya-Bekasi Rp. 18.000 tetapi lazada hanya membayar ke *seller* hanya Rp. 1.384. Kalian bisa bayangkan ongkir manasih yang Cuma Rp. 1.384. Alasan dari pihak lazada bilang suruh klaim ke mereka dan akan mengganti ongkir tersebut”²²³

Lebih lanjut berdasarkan hasil wawancara yang telah penulis lakukan dengan pelaku usaha yang tergabung di UKM Kota Surakarta mengatakan bahwa,

Ada salah satu market place yang terkenal, namun membawa banyak kerugian bagi kami selaku seller sebagai contoh bagi *website* yang berbasiskan *e commerce* seharusnya *seller* adalah mitra penting, namun bagi *lazada seller* harus dipersulit hidupnya. Sebagai contoh dalam

²²²Surat terbuka untuk lazada.co.id Agungz <http://www.kaskus.co.id/thread/> diakses pada 24 Feruari 2016 jam 04.33 WIB

²²³Surat terbuka untuk lazada.co.id tidak masuk akal yang terdapat dalam <https://trustedcompany.com> diakses pada 24 Februari 2016 Jam 05.23 WIB

membuka account verifikasi KTP, tabungan bank, alamat dan lain-lain. Kesulitan mengedit gambar dengan latarbelakang putih, kesulitan disetujui produknya dan banyak kesulitan lain. Belum lagi kegemaran lazada memberikan promo palsu misalnya *harbolnas*, promo *free ongkir* jabodetabek yang pada akhirnya harus ditanggung oleh seller secara sepihak dan janji lazada untuk mengganti rugi ongkir adalah bohong. Lazada tidak mendukung UKM di Indonesia banyak teman saya yang berjualan di lazada mengeluhkan produknya tergilas oleh serbuan produk asing yang harganya sangat miring. Selain itu di lazada bila seller mendapatkan order sama sekali tidak ada notifikasi baik notifikasi email maupun notifikasi melalui aplikasi mobile, berbeda dengan sistem yang ada di bukalapak dan tokopedia. Perlu dipikirkan lagi bahwa seller dan buyer adalah mitra sejati sehingga market place seperti lazada perlu membenahi sistem bila tidak ingin di tinggalkan oleh konsumennya”²²⁴

Berdasarkan hasil penelitian yang penulis lakukan dengan konsumen yang sering menggunakan *e commerce* mengenai *Trustmark* dikatakan bahwa,²²⁵

“*Trustmark.. apa ya.. saya tidak tahu apa itu Trustmark*”

Hal senada juga dikatakan oleh konsumen pengguna *e commerce* mengenai *Trustmark*,²²⁶

“Kalau Norton, Paypal saya tahu.. tetapi *Trustmark* saya kurang tahu, Lembaga Sertifikasi Keandalan saya juga tidak paham, apa semacam sertifikat halal yang dikeluarkan oleh MUI mungkin ya”

Dari hasil wawancara yang telah penulis lakukan di Kementerian Perdagangan RI, dikatakan bahwa:²²⁷

“Mengenai perlindungan pengguna *website* nanti arahnya kesana, jadi nanti kita mengatur informasi apa yg ada dalam Undang-Undang, untuk yg disampaikan kepada konsumen ketika melakukan perdagangan sistem elektronik, nah ini nantinya dalam RPP akan dijabarkan lebih detail lagi apa yang menjadi hak dan kewajiban pelaku usaha serta konsumen, diatur mulai dari informasi apa saja yg harus dicantumkan kemudian

²²⁴Wawancara langsung dengan Witri widhoyoko pelaku usaha kecil menengah Kota Surakarta sebagai pemilik usaha di www.tardjotea.com pada 5 Januari 2016 Jam 10.00 WIB

²²⁵Wawancara langsung dengan Ibu Dhany Hidayati selaku konsumen pengguna *e commerce* di BPK RI Jakarta pada 20 Januari 2015 Jam 13.22 WIB

²²⁶Wawancara langsung dengan Ibu Riana Fatmawati selaku konsumen pengguna *e commerce* di Poltekpel Surabaya pada 12 Februari 2015 Jam 16.15 WIB

²²⁷Wawancara langsung dengan Ibu Ria selaku Subbag e bisnis Kemertian Perdagangan RI Jakarta pada 15 Januari 2015 Jam 14.25 WIB

kewajiban pelaku usaha harus melakukan jaminan bahwa harus berijin. Ijin disini bukan harus ijin baru, ijin disini kan sekarang ada ijin besar, secara online, dan produknya harus ada jaminan. Itu nanti lebih di detailkan di PP. Kemudian juga nantinya akan di atur juga mengenai kontraknya. Bagaimana sih kontrak dlm penawaran kontrak terus dalam buat kontrak sampai dengan ketika nanti seperti pelayanan nilai jualnya seperti apa. Sebenarnya ini juga banyak yang mengadu, kita juga tidak hanya dari Undang-Undang perlindungan konsumen, kita coba kolaborasi disini. Untuk meningkatkan kepercayaan konsumen di internet, saya rasa bisa menggunakan *trustmark* namun lembaga yg memberikan *trustmark* harus terdaftar di Kementrian Kominfo, tetap di bawah pengawasan kominfo, seperti halnya domain, masih di bawah pengawasan kominfo”

Lebih lanjut di jelaskan oleh Ferdinandus Setu selaku Kepala Subbag Penyusunan Rancangan Peraturan Direktorat Jendral Aplikasi Informatika Kementrian Kominfo,

“Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik mengatur pelaku bisnis dengan menganjurkan untuk menggunakan Sertifikat keandalan juga elektronik yang disertifikasi oleh penyelenggara sertifikasi elektronik, jadi Undang-Undang itu sudah mulai masuk di 2 hal yaitu Sertifikat keandalan yang merupakan sebuah sarana yang dipasang disebuah *website*. Misalnya mandiri, bca, ada semacam *trustmark*. Dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik disebut Sertifikat keandalan. Sertifikat keandalan dikeluarkan oleh lembaga Sertifikat keandalan (LSK) di Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik. Sertifikat Elektronik, dikeluarkan oleh penyelenggara sertifikasi elektronik, tujuannya untuk memberi sertifikasi tanda tangan elektronik. Jadi untuk hubungan bisnis antara seseorang dengan pihak lain di dunia maya. Itu dibutuhkan pihak ketiga. Pihak ketiga terpercaya disebut penyelenggara sertifikasi elektronik yang nanti yang melakukan sertifikasi terhadap tanda tangan kita. Itu yang disebut dengan sertifikat elektronik”²²⁸

Dari hasil wawancara yang telah peneliti lakukan dengan Ricky di Ditjen Aptika Kementrian Kominfo dikatakan bahwa,

“Kominfo ini mengoperasikan *Root CA*, nanti kedepannya kalau liat di PP nya karena layanan publik, namun semuanya harus bertahap, kita

²²⁸Wawancara dengan Ferdinandus Setu selaku Kepala Subbag Penyusunan Rancangan Peraturan Direktorat Jendral Aplikasi Informatika Kementrian Kominfo Jakarta Pada 10 Februari 2014

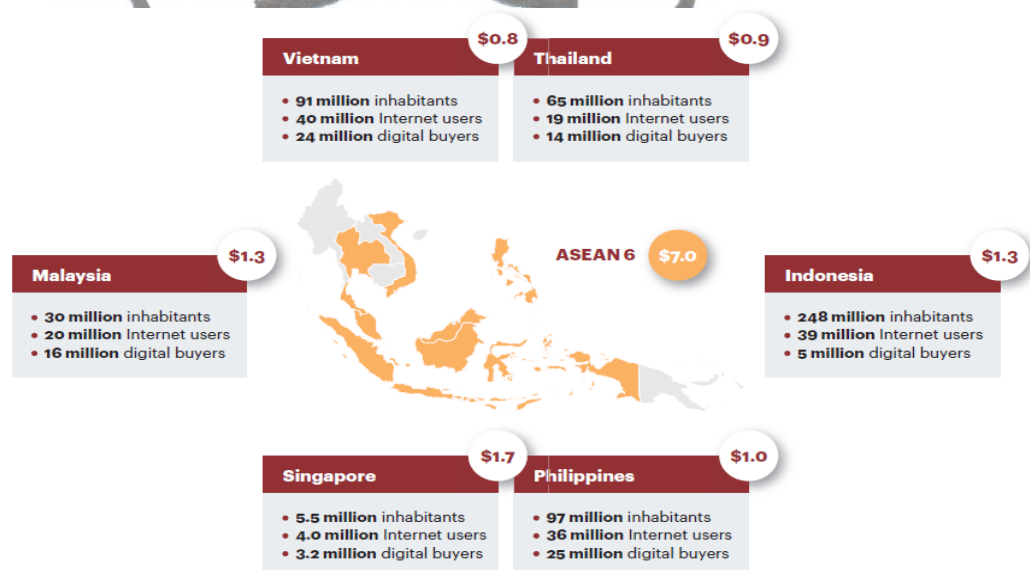
terkena kendala teknis. Teknisnya ini kan warna hijau tidak ada masalah karena secara teknis sertifikat di dlm browsernya, kalau merah ada masalah Rootnya blum dipercaya. Ada daftar *Root CA* yang sudah dipercaya oleh mozilla. Sertifikasi internasional, kita harus manggil auditor untuk trustmark kita, jadi kita harus dpt *trustmark* (logo), namanya webtrust. Begitu kita dapat sertifikat webtrust. Kominfo sudah dipercaya, kemudian kita Kirim ke explorer, mozilla, baru mereka secara teknis baru dimasukkan ke daftar itu. Ini prosesnya lama tidak bisa cepat. Misal hari ini kita dapat sertifikat *webtrust* kita ngajuin ke mozilla besok, paling 1 tahun lagi baru ada disini. Paling cepat itu 18 bulan, itu untuk mozilla, itu d sistem operasinya. Dari sisi goverment kita msh bisa mentolerir itu, akan menjadi sulit bila itu adalah *bussiness to bussiness*”²²⁹

Dari hasil penelitian yang telah penulis lakukan konsumen dalam transaksi elektronik terbagi menjadi dua yaitu konsumen akhir pengguna barang dan jasa dan *seller* sebagai konsumen penyedia sistem elektronik. Meskipun pemerintah telah membuat Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta turunannya Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, namun hingga saat ini banyak konsumen *e commerce* yang belum terlindungi hak-haknya. Peran pemerintah masih terbatas pada pembuatan Undang-Undang dan belum secara teknis ikut aktif dalam menumbuhkan iklim usaha yang sehat melalui *e commerce* secara lebih nyata. Hal ini berbeda dengan upaya yang telah dilakukan oleh beberapa negara yang secara geografis berdekatan dengan Indonesia yaitu Malaysia dan Singapura yang telah terlebih dahulu masuk tergabung menjadi anggota *Asian Trustmark Alliance* / ATA yang saat ini menjadi *World Trustmark Alliance*. Pemerintah kedua negara tersebut yang menginisiasi munculnya perlindungan konsumen *e commerce* dan cenderung otoriter dalam mengatur tentang perlindungan hukum bagi warga negaranya dalam transaksi elektronik.

²²⁹Wawancara langsung dengan Ricky Prajoyo dan Riko Rasota Rahmada selaku Subdit Teknologi Keamanan Informasi Ditjen Aptika Kementerian Kominfo Pada 21 Januari 2015 pada 14.10 WIB

B. Upaya pemerintah negara Singapore dan Malaysia dalam meningkatkan *E Commerce* melalui Penggunaan *Trustmark*

Masyarakat Ekonomi Asean pada dasarnya merupakan peluang bagi Indonesia karena salah satu pasar terbesar di asia tenggara berdasarkan jumlah penduduk. Namun hal ini perlu diukur pula dari kesiapan negara Indonesia atas masuknya arus barang dan jasa dari negara asing khususnya melalui *e commerce*. Ada lima hal yang perlu dibenahi untuk mengatasi hambatan pertumbuhan *e commerce* di Indonesia, 1) meningkatkan akses *broadband*, 2) mendukung munculnya pelaku usaha kecil dan menengah ditingkat lokal, 3) memperkuat keamanan *online*, 4) mempromosikan pembayaran elektronik dan 5) meningkatkan efisiensi logistik dan perdagangan. Beberapa hambatan khususnya keamanan dalam transaksi *e commerce* apabila dibandingkan dengan enam negara ASEAN utama yaitu Malaysia, Philipina, Singapura, Thailand dan Vietnam, Indonesia masih jauh tertinggal.



Sumber, AT Kearney analysis, 2015

Gambar 9 Penggunaan *e commerce* dibandingkan dengan jumlah populasi di negara ASEAN

commit to user

Berdasarkan gambar tersebut diatas, maka dapat ditunjukkan bahwa Singapura dan Malaysia lebih dari 50% jumlah penduduknya telah menggunakan *e commerce*. Hal ini dikarenakan dukungan pemerintah negara Singapura dan Malaysia yang selalu otoriter dan konsisten untuk melindungi warga negaranya pada saat menggunakan *e commerce*. Atas dasar tersebut maka peneliti ingin membandingkan bagaimana regulasi Singapura dan Malaysia dalam memberikan perlindungan terhadap konsumen pengguna *e commerce* khususnya dalam menggunakan *Trustmark*.

1. Deskripsi Peran ATA (*Asia-Pacific Trustmark Alliance*) dalam mewadahi anggotanya pengguna *Trustmark* di Asia Pasifik WTA.

The Asia Trustmark Alliance (ATA), salah satu aliansi *trustmark* di tingkat regional, didirikan pada tahun 2003. Pada tahun 2006, ATA memiliki anggota antara lain dari Singapore: CNSG (*Commerce Net Singapore*), CASE (*Consumer Association Singapore*), Jepang: EC Jaringan, Aman Perdagangan, Vietnam: *EcomViet*, Korea Selatan: LAN, Filipina: *Qartas Corporation*, Taiwan: SOSA, USA: TRUSTe. Asosiasi aman Belanja Online (SOSA),

Pada tahun 2010, ATA asli berganti nama WTA (*World Trustmark Alliance*). WTA tetap menjadi organisasi berbasis keanggotaan sebagai ATA, perbedaan antara ATA dan WTA adalah bahwa keanggotaan asosiasi ini tidak lagi terbatas pada wilayah Asia-Pasifik, tapi untuk dunia, dan WTA dapat menangani masalah yang lebih luas. Ini menjadi besar, organisasi di seluruh dunia dengan 37 operator bisnis dari 30 negara. Dalam gerakan mengembangkan kerangka Asia ke dalam skala global dengan GTA (*Global Trustmark Alliance*) dan WTA (*World Trustmark Alliance*), memiliki anggota EC dari perusahaan kelas atas seluruh dunia. ATA mampu berkolaborasi dengan APEC (*Asia-Pacific Economic Cooperation*), Eropa, Amerika. SOSA yang perusahaan *Trustmark* di Taiwan, menjadi ketua organisasi.

commit to user

Dengan penyebaran broadband dan perangkat mobile seperti ponsel pintar dan tablet PC, *e-commerce* transaksi diperkirakan akan terus berkembang. Tentu, jaringan trustmark dan penanganan sengketa akan memainkan peran yang lebih besar. Sejak negara memiliki standar yang berbeda, operasi ini akan menjadi sangat penting dalam rangka untuk melakukan transaksi lintas batas yang sukses. Diskusi dan pengaturan di organisasi seperti WTA dengan banyak peserta perusahaan akan semakin penting.

Anggota dari WTA di wilayah Asia Pasifik antara lain:

- a. *EC Network*, Jepang



Gambar 10. Trustmark EC Network Jepang

EC Network didirikan pada April 2006, Tokyo. Direksi perusahaan ini adalah Toshiko Sawada dan Yuri Harada. *EC Network* ini merupakan Organisasi swasta Non-profit yang memiliki tujuan antara lain, Mempromosikan lingkungan *e-commerce* yang handal dan aman untuk bisnis dan konsumen, Mendorong praktik yang baik untuk bisnis *e-commerce*, Menyediakan layanan konsultasi dan ADR via *online* dan Menangani keluhan domestik dan lintas batas tentang transaksi Internet.

b. *Trade Safe*, Jepang

Japan

Gambar 11. *Trustmark Trade Safe* Jepang

Penanganan utama yang dilakukan *Trade Safe* adalah penanganan masalah bagi pembeli dan penjual di Importers.com dan situs perdagangan *online* lainnya yang memerlukan peningkatan kredibilitas dan profesionalisme anggotanya. Untuk membantu importir dan eksportir mendapatkan kepercayaan anggota lain, penghargaan Importers.com *TradeSafe Verifikasi* telah membuktikan profesionalisme bisnis mereka. Semua anggota yang *TradeSafe Verified* menerima ikon ini.

c. CNSG, Singapore

Singapore

Gambar 12. *Trustmark CNSG* Singapore

CNSG *Consulting* Group saat ini adalah salah satu inkubator paling agresif di kawasan ASEAN. Namun, juga mengambil proyek-proyek di luar ASEAN, ke Cina, Korea, Jepang, Timur Tengah, India, Pakistan dan

Afrika. Fokus dari lembaga *Trustmark* ini adalah untuk mengidentifikasi perusahaan dan proyek-proyek yang *bankable* internasional dan untuk lebih mengembangkan mereka dengan solusi nilai tambah tinggi dan proposisi bisnis. Dalam prosesnya, *incubatees* harus berasal penilaian maksimum dan keuntungan finansial, yang memungkinkan mereka untuk dengan mudah keluar di pasar siap dengan likuiditas yang tinggi.

d. Malaysia *Trustmark*, Malaysia



Gambar 13. Malaysia *Trustmark*, Malaysia

Malaysia *Trustmark* diprakarsai oleh Pemerintah Malaysia sebagai sarana memvalidasi kontrol keamanan *web* dari situs organisasi yang terlibat dalam *e-bisnis*. *website* divalidasi kemudian diberikan dengan Malaysia *Trustmark seal* sebagai pengakuan bahwa situs *web* tertentu dioperasikan oleh organisasi yang terpercaya. Malaysia *Trustmark* bertujuan untuk mempromosikan praktik *e-bisnis* yang baik di Malaysia dan sekaligus meningkatkan tingkat kepercayaan di kalangan konsumen.

Malaysia *Trustmark* untuk Sektor Swasta (MTPS) adalah layanan dengan *CyberSecurity* Malaysia untuk meningkatkan kepercayaan dalam *e-bisnis* untuk Malaysia. organisasi akan dinilai berdasarkan legalitas perusahaan dan keamanan kontrol dari situs *e-bisnis* dan transaksi.

e. *CyberSecurity* Malaysia



Gambar 14. *CyberSecurity* Malaysia

CyberSecurity Malaysia (www.cybersecurity.my) adalah lembaga spesialis keamanan *cyber* nasional di bawah Kementerian Sains, Teknologi dan Inovasi (MOSTI) (www.mosti.gov.my). *CyberSecurity* Malaysia telah ditunjuk sebagai Malaysia *Trustmark* untuk Sektor Swasta (MTPS) operator dan sertifikasi oleh Pemerintah Malaysia. Sebelumnya dikenal sebagai Keamanan TIK Nasional dan Pusat Tanggap Darurat (NISER), *CyberSecurity* Malaysia menjadi agen di bawah lingkup MOSTI pada tahun 2005 sebagai badan nasional untuk memantau aspek National *e-Security*. Pada dasarnya, peran *CyberSecurity* Malaysia adalah untuk memberikan layanan keamanan *cyber* khusus seperti, keamanan *Cyber* tanggap darurat, penanganan insiden, dan forensik digital, manajemen mutu keamanan *Cyber*, kemampuan keamanan *Cyber* dan pembangunan kapasitas, keamanan *Cyber* penjangkauan dan akulturasi, penelitian keamanan *Cyber* dan penilaian risiko dan evaluasi keamanan *Cyber* dan sertifikasi.

f. *CASE Trust*, SingaporeGambar 15. *CASE Trust*, Singapore

Asosiasi Konsumen Singapura (CASE) adalah non-profit, organisasi non-pemerintah yang berkomitmen untuk melindungi kepentingan konsumen melalui informasi dan pendidikan, dan mempromosikan lingkungan praktik perdagangan yang adil dan etis. Salah satu prestasi utama *Case Trust* adalah di lobi Perlindungan Konsumen (*Fair Trading*) Undang-Undang (CPFTA) yang mulai berlaku pada 1 Maret 2004

g. *Secure Online Shopping Association* (SOSA), Taiwan, R.O.CGambar 16. *Trustmark* SOSA, Taiwan, R.O.C

Secure Online Asosiasi Belanja (SOSA) adalah tidak terdaftar untuk organisasi nirlaba di Taiwan. SOSA adalah penyedia *trustmark* pertama

dan terbesar, didirikan pada September 1999. anggota pendiri meliputi HP, China Airlines, China Information Credit Service Inc and lain-lain. Tujuan SOSA adalah untuk mempromosikan, lingkungan *e-commerce* tertib *self-regulatory* memfasilitasi aplikasi *e-commerce*. SOSA akan membantu dalam menyelesaikan sengketa antara konsumen dan anggota SOSA. Misi SOSA adalah untuk, merekomendasikan standar dan kebijakan, melakukan evaluasi mengotentikasi dan penghargaan segel untuk pedagang *online*, berkomunikasi melalui topik yang muncul diberbagai seminar dan acara serta menyediakan *Platform-online* untuk menyelesaikan sengketa.

SOSA memiliki keterlibatan dalam organisasi internasional termasuk APEC, GBDe, ATA / WTA, dan terpilih sebagai ketua WTA pada tahun 2011-2012. SOSA juga membantu dalam menyelesaikan masalah antara konsumen dan anggota, perusahaan dan pemerintah, teknologi yang baru peraturan baru.

h. *Dept. Of Business Development, Ministry of Commerce, Thailand*



Gambar 17. *Trustmark DBS Thailand*

Di bawah reformasi birokrasi pada bulan Oktober 2002. "Departemen Pendaftaran Komersial" telah berubah nama menjadi "Departemen Pengembangan Bisnis (DBD)", dan juga meningkatkan

fungsi pekerjaan. Salah satu peran utama baru promosi *e-commerce* untuk Usaha Kecil dan Menengah (UKM). Divisi *E-commerce* telah dibentuk dengan tujuan sebagai berikut, memberikan pemahaman yang lebih luas dari *e-Commerce* dan membangun kesadaran penggunaan *e-Commerce*, Mempromosikan kepercayaan dan keyakinan dalam transaksi *e-Commerce*, mengembangkan dan memperkuat keterampilan perusahaan dalam *e-Commerce* untuk meningkatkan kemampuan bisnis, mengumpulkan dan menganalisis statistik perusahaan *e-Commerce*, dan menyiapkan kebijakan untuk menjamin bahwa kegiatan *e-Commerce* konsisten dengan pasar saat ini.

i. EBS, China



Gambar 18. Trustmark EBS China

Sebagai upaya untuk meningkatkan layanan *E-commerce* yang lebih baik (www.ebs.org.cn) disahkan oleh hukum dan didukung oleh pemerintah. www.ebs.org.cn merupakan lembaga pihak ketiga *non-profit* yang memberikan kontribusi untuk membangun keterpercayaan lingkungan transaksi *e-commerce* dan keuntungan dalam memiliki kedua otoritas pemerintah dan fleksibilitas pasar. Berkomitmen untuk nilai "Keadilan, Integritas, Kepercayaan, *Corporation* dan Interdependensi", EBS menetapkan standar untuk kompetisi yang adil dalam *e-commerce*, bertujuan untuk membangun kredibel, terpercaya, dan aman dipasar

Commit to user

e-commerce dan akhirnya mendorong sehat dan perkembangan pesat dalam layanan *e-commerce*. Tujuan ebs adalah melakukan,

- 1, *Identity Authentication* untuk entitas perusahaan *E-commerce*
Berdasarkan data resmi pemerintah dengan melakukan pengawasan pemasaran, EBS mengevaluasi identitas dan kualifikasi entitas *e-commerce* perusahaan dengan mencocokkan identitas virtual mereka dengan identitas fisik. Mereka yang diverifikasi akan diberikan EBS *Trustmark* resmi, membantu konsumen untuk secara cepat mengidentifikasi keaslian entitas pasar *online*. .
2. Pemeriksaan untuk produk secara *online* dan komoditas
dengan mendasarkan pada standar sistem berbagi informasi produk, EBS meneliti dan memverifikasi keaslian produk secara *online* dan komoditas; memberikan kepada konsumen layanan keaslian produk secara *online* memeriksa dan akses untuk pelacakan sumber produk.
3. Pemeriksaan untuk voucher elektronik
EBS memberikan kepada badan *e-commerce* dan layanan konsumen dokumen pelestarian dan pemeriksaan transaksi *online*, untuk membuktikan keaslian transaksi *online* dengan memastikan *voucher* yang relevan terjadi melalui transaksi online yang efektif dan dapat dilacak.
4. Penyelesaian Sengketa *Online*
Dengan membangun sistem pengolahan sengketa secara *online*, di perusahaan dengan lembaga hukum yang profesional dan ahli dari dalam dan luar negeri, EBS menyediakan kepada konsumen layanan konsultasi hukum, serta layanan penyelesaian sengketa secara *online* yang mudah dan cepat.
5. Standar dan Promosi
Mendasarkan pada *E-commerce Standar Alliance*, EBS menetapkan sistem standar untuk *e-commerce* *commit to user* dipercaya transaksi, memimpin

dalam pengaturan standar penting dalam bidang-bidang seperti produk *e-commerce*, transaksi, kredit, perlindungan hak, dll, sehingga untuk mengembangkan dan mempromosikan lingkungan pasar secara *online* hukum dan standar, juga untuk membantu entitas *e-commerce* menjadi lebih kompetitif di seluruh mitra dunia.

Sebagai mitra strategis, perusahaan terkemuka *e-commerce* seperti Alibaba Group, Tencent, eBay, HuaqiangNorth Online, Made-in-China, Telah menandatangani nota kerja sama dengan EBS, melakukan untuk berusaha bersama-sama dengan EBS untuk tidak hanya mempopulerkan penerapan "*Identity Authentication untuk Enterprise Entity* ", tetapi juga membawa ke depan semua layanan lainnya.

Menyediakan layanan *Identity Authentication* untuk *Enterprise Entity*
Membangun Keterpercayaan perusahaan *ecommerce* serta menetapkan standar dasar *e-commerce* .

Membangun Identitas sistem bi-otentikasi untuk *Enterprise Entity* demonstrasi aplikasi dalam perusahaan *e-commerce*. Memberikan subsidi dan dukungan, budidaya entitas perusahaan *E-commerce*. Menetapkan standar dan peraturan *E-commerce*. menumbuhkan *E-commerce* perusahaan entitas, membangun dan mempromosikan transaksi *E-commerce* yang dipercaya ekosfer. Menetapkan dan menerapkan standar *e-commerce*, menumbuhkan *e-commerce* perusahaan entitas, menyediakan layanan *Identity Authentication* untuk *Enterprise Entity*.



Gambar 19 Mitra EBS, Alibaba Group, Tencent, eBay, HuaqiangNorth Online, Made-in-China

j. SOSA Secure, Taiwan



Gambar 20. Trustmark SOSA Secure Taiwan

SOSA *secure* berupaya membangun lintas batas lingkungan transaksi *e-commerce* yang terpercaya, mengaktualisasikan dan mengembangkan *Trustmark*. Membuat akses pengaduan untuk pelanggan dan pemasok dari baik dari Taiwan maupun diluar Taiwan. Mempromosikan komunikasi lintas-perbatasan dan diskusi tentang *E-commerce*.

E-Commerce Standards Alliance (ECSA) *E-Commerce Standards Alliance* (ECSA) didirikan pada bulan Juli 2010, oleh 18 raksasa *E-commerce* antara lain Xiu.com, Seg, Global Resources, dan kantor Sekretariat terletak di EBS. Dengan tahun pembangunan, keanggotaan

ECSA mencakup berbagai bidang dan industri, mengatakan organisasi seperti B2C dan *platform trading* pihak ketiga, yang berada di bidang perdagangan luar negeri, pembayaran, kredit, dalam industri *Garment, Luxuries, Jewelry*, 3C, Komponen Elektronik, Ticketing dan sebagainya.

k. NIPA, Korea



Gambar 21. Trustmark NIPA, Korea

Tujuan pendirian LAN (Badan IT *Industry Promotion*) mengabdikan dirinya untuk memperkuat daya saing industri TI dan memberikan kontribusi terhadap pertumbuhan ekonomi melalui dukungan yang efisien dan meletakkan dasar untuk promosi teknologi industri oleh Kementerian Sains, ICT dan Perencanaan Masa Depan.

Pada Bisnis secara umum melakukan penelitian kebijakan dan dukungan pengembangan untuk industri TI, membantu membangun fondasi industri TI dan mengolah sumber daya manusia, menghidupkan pasar distribusi untuk pengembangan industri TI dan dukungan pemasaran, mempromosikan bisnis terkait dengan konvergensi dan pemanfaatan teknologi IT, mendukung pertukaran internasional, kerjasama dan ekspansi ke luar negeri terkait dengan industri TI ECMC (*e-Commerce Committee Mediasi*)

Tujuan dan Dasar-dasar dari Pendirian ECMC (*e-Commerce Komite Mediasi*) adalah untuk menciptakan sebuah dunia maya yang aman, mempromosikan bisnis yang melakukan *e-commerce*, dan melindungi hak-hak konsumen dengan *commit to user* jaminan terhadap kerusakan dan pembentukan

transaksi yang adil yang timbul dari cepat dan resolusi sengketa yang adil. pencegahan sengketa: Pendidikan dan komunikasi publik untuk pencegahan sengketa *e-commerce*, penyelesaian sengketa: Menawarkan layanan mediasi dan konsultasi untuk memecahkan sengketa *e-commerce* Membangun lingkungan pasar *e-commerce* yang sehat: Bekerja sama dengan organ terkait dan bisnis untuk mewujudkan dunia *cyber* yang sehat.

Pada pelaksanaan sertifikasi, Departemen Ilmu, ICT dan Perencanaan Masa Depan dan Badan IT Industri Nasional mengevaluasi perlindungan situs konsumen dan perlindungan informasi pribadi kebijakan, serta proses pembelian seluruh adil dan ketat dan pemberian tanda kepada bisnis *e-commerce* yang unggul untuk menunjukkan kepada bahwa bisnis *e-commerce* tersebut dapat dipercaya.

Kontribusi Sertifikasi *eTrust* adalah untuk pembangunan lingkungan yang aman untuk transaksi *online* dan menjamin kepercayaan konsumen melalui manajemen yang ketat melalui tanda sertifikasi untuk bisnis transaksi *online*. Persiapan jangka panjang yang sistematis di desain untuk keamanan dan kenyamanan transaksi *online* melalui penyediaan sertifikasi *eTrust* kepada konsumen dan menawarkan kesempatan untuk mengembangkan bisnis melalui penggunaan tanda *eTrust* untuk perusahaan *cybermall internet*.

1. *SURESEAL*, Philippines



Gambar 22 Trustmark *SURESEAL*, Philipina

Sure Seal dijalankan oleh *Qartas Corporation*, sekelompok praktisi *e-commerce* yang sangat dihormati dengan tahun pengalaman di Filipina. Menggabungkan pengetahuan internet dan keahlian teknis dengan standar otentikasi yang telah teruji, *Qartas Corporation* bertujuan untuk menciptakan komunitas terbesar dari bisnis Filipina terpercaya yang sesuai dengan standar tertinggi integritas, etika, dan kehandalan. Tujuan utama adalah untuk muncul dalam setiap bisnis *online* yang sah di Filipina mempromosikan kepercayaan dan *goodwill* antara bisnis dan pelanggan.

m. *SafeWeb*, Vietnam



Gambar 23. *Trustmark SafeWeb Vietnam*

SafeWeb, *trustmark* Vietnam berhak dengan "Sistem kriteria transaksi secara *online* di *e-commerce*" di alamat www.safeweb.vn. Itu dibangun untuk menggantikan untuk *Trust In*, *Trustmark* sebelumnya, yang merupakan singkatan dari segel privasi. *Trustmark* *SafeWeb* adalah untuk menciptakan standar pada syarat dan kondisi dari transaksi di *website e-commerce*. Vietnam *E-commerce Development Center* milik Vietnam *E-commerce* dan Agen IT, Departemen Perindustrian dan Perdagangan adalah entitas *SafeWeb*. *SafeWeb* terdiri dengan 5 prinsip sebagai berikut, keyakinan membangun perlindungan, Informasi Pribadi, E-kontraktor, *Advertising* yang Jujur dan Klaim. Kelima prinsip dinyatakan dalam 32

kriteria rinci, di mana prinsip kedua dan ketiga mengambil sebagian. Pertama dan tertinggi prioritas *SafeWeb* adalah untuk mengamankan hak-hak konsumen dan menuju pengembangan *e-commerce* yang sehat di Vietnam.

2. Perbandingan Penggunaan *Trustmark* di Singapore dan Malaysia

Pemerintah Singapore telah berupaya meningkatkan penggunaan *e-commerce* yang diwujudkan dengan membentuk lembaga Skema Akreditasi *CaseTrust* dan Malaysia *Trustmark*. Adanya *CaseTrust* maupun Malaysia *Trustmark* dapat mengikis proporsi monopoli pelaku usaha. Kehadiran lembaga ini merupakan pagar yang kuat untuk melawan potensi praktek-praktek usaha yang sering merugikan konsumen.

a. *Trustmark* di Singapore

1). *CaseTrust* Singapura

Lembaga *CaseTrust* dibentuk atas inisiatif Asosiasi Konsumen Singapura (CASE). Lembaga ini menargetkan akreditasi layanan dan industri ritel untuk memelopori usaha menuju keunggulan dengan cara mengadopsi praktek bisnis yang adil. Sebuah toko online yang menampilkan Logo *CaseTrust* akan menunjukkan keadilan dan kejujuran terhadap konsumen.

Sejak diluncurkan, *CaseTrust* telah diterima oleh pelaku industri. Hal ini karena standar *CaseTrust* diselenggarakan dengan cara yang jelas dan menunjukkan bahwa bisnis yang telah terakreditasi dapat terus mengikuti tren konsumen dan perkembangan baru dalam industri. Personal Lembaga *CaseTrust* merupakan perwakilan dari STB, SPRING Singapura, IDA, NATAS, dan relawan CASE semua anggota Dewan Penasehat *CaseTrust*, membantu lembaga dalam mewujudkan visi kedepan.

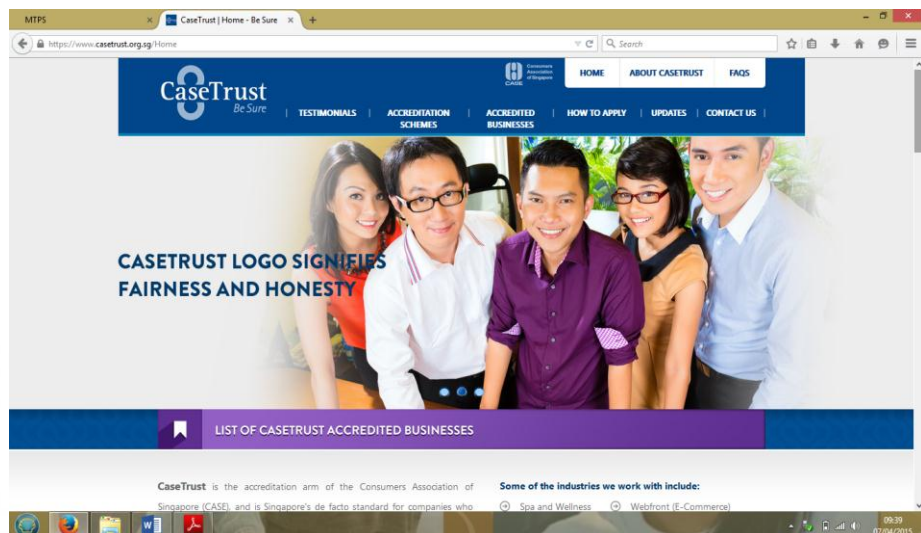
Tanggal 18 Mei 2004, *CaseTrust* diluncurkan kembali dengan merek baru logo *CaseTrust*. Logo menyajikan *CaseTrust* sebagai perantara *commit to user* konsumen dan pedagang, yang

terlibat dalam transaksi bisnis yang saling menguntungkan. Ketika semua elemen bergabung bersama-sama, mereka membentuk kunci kokoh, yang merupakan simbol universal kepercayaan dan keyakinan. 'CaseTrust' membuat kerangka minimum kunci, melambangkan dasar yang kuat untuk praktek bisnis yang baik.

Upaya Singapura membangkitkan kepercayaan pada *e commerce* melalui skema *CaseTrust* yang diluncurkan pada tahun 1999 oleh *Commerce Net* Singapura, Pusat Promosi Perdagangan (*Retail Promotion Centre*) dan Asosiasi Konsumen Singapura (*CASE, Consumer Association of Singapura*).

CaseTrust bertujuan untuk memberikan sertifikasi kepada pedagang yang mematuhi aturan praktik bisnis yang telah ditetapkan oleh asosiasi perdagangan dan memberikan hak kepada mereka untuk menggunakan segel tanda persetujuan yang dikenal sebagai *Trustmark*. *Trustmark* tersebut tidak membedakan antara perdagangan *online* maupun *offline*. *Trustmark* tersebut bertujuan untuk memberikan sertifikasi pada kedua bentuk bisnis. Bisnis *offline* akan menjadi subjek dari sertifikasi fisik sedangkan bisnis *online* akan menjalani sertifikasi *web*.²³⁰

²³⁰ Assafa Endeshaw, *Hukum E Commerce dan Internet dengan Fokus di Asia Pasific.*, Pustaka Pelajar, Yogyakarta, 2007, hlm. 286



Gambar 24. Casetrust merupakan Trustmark yang dimiliki Singapura

2) Regulasi CaseTrust Singapura

Berdasarkan hasil penelitian yang telah penulis lakukan, dasar hukum dibentuknya *Case Trust Singapura* berdasarkan *The Statutes of The Republic of Singapore Trust Companies Act (Chapter 336)*. Atas dasar regulasi tersebut maka *Case Trust Departement* membentuk *Code of Practice* sebagai aturan yang digunakan oleh pelaku usaha *e commerce* agar melakukan praktik bisnis yang baik dan adil. Isi dari *Code of Practice* yang dibuat oleh *Case Trust Departement* adalah sebagai berikut:

Code of Practice CaseTrust Accreditation Scheme

1 INTRODUCTION

*1.1 All accredited businesses agree to comply at all times with this Code which sets out, among other things, good and fair business practices to be used by CaseTrust accredited businesses. This Code also provides a framework for resolving disputes between the accredited business and their customer, or between accredited businesses themselves as may be the case.*²³¹

commit to user

²³¹ CaseTrust Accreditation Scheme *Code of Practice*. 2014 CaseTrust Department. Hlm. 1

- 1.2 This Code aims to promote all business transactions arising out of or in connection with a CaseTrust accredited business will be conducted with honesty, integrity and transparency. In the interpretation of this Code, regard should be had to:*
- (a) The objective of this Code; and*
 - (b) The principles of good and fair business practices.*
- 1.3 This Code is intended to provide the general principles to be followed by CaseTrust accredited businesses when conducting their business and if applicable, supplements the various agreements, which the accredited business has entered into with CASE, including but not limited to the full set of terms and conditions of accreditation.²³²*

Berdasarkan kutipan dari *Code of Conduct* tersebut maka dapat penulis terjemahkan secara bebas bahwa dalam point 1.1 menegaskan bahwa semua bisnis yang terakreditasi oleh *Case Trust* setuju untuk melakukan praktik bisnis yang baik dan adil. Kode etik ini juga merupakan kerangka untuk menyelesaikan sengketa yang mungkin terjadi. Point 1.2 menyatakan bahwa Kode ini bertujuan untuk mempromosikan bahwa semua transaksi bisnis yang timbul dari atau sehubungan dengan bisnis *CaseTrust* terakreditasi akan dilakukan dengan kejujuran, integritas dan transparansi. Kode Etik ini memiliki bertujuan untuk mewujudkan prinsip-prinsip praktek bisnis yang baik dan adil. Point 1.3 Kode etik ini dimaksudkan untuk memberikan prinsip-prinsip umum yang harus diikuti oleh *CaseTrust* bisnis terakreditasi ketika melakukan bisnis dan telah menandatangani perjanjian sebagai bisnis terakreditasi dan disetujui oleh CASE termasuk kelengkapan persyaratan dan ketentuan akreditasi.

2 PRINCIPLES OF GOOD AND FAIR BUSINESS PRACTICES

- 2.1 Accredited businesses are obliged to and undertake to implement principles of good and fair business practices, which include but are not limited to the following:²³³*
- (a) Accredited businesses shall ensure that the terms and conditions governing the relationship between the accredited*

²³² *Ibid.*

²³³ *Ibid.*

- businesses and their customers are provided or made available to the customers at the point of sale;*
- (b) Accredited businesses shall not use methods of sale, advertisement and promotion which are inconsistent with that laid down by the Code, but should be consistent with the highest standards of honesty, fairness, integrity and transparency;*
 - (c) Accredited businesses shall not make claims, warranties, representations or statements which may be false, untrue, misleading, inaccurate or fraudulent in the course of business or to induce a customer to purchase their goods and/or use their services through such means;*
 - (d) Accredited businesses must apply principles of good and fair trading in their business like not engaging in high-pressure sales tactics, “bait and switch” advertising and the like; and*
 - (e) Accredited businesses shall comply with all applicable laws and regulations including but not limited to the Personal Data Protection Act 2012, so that the personal data protection obligations for the collection, use and disclosure of personal data as well as the Do Not Call Registry obligations are satisfied at all times.²³⁴*

Kutipan nomor 2 membahas mengenai prinsip dan praktik bisnis yang baik serta adil. Pada pasal ini ditekankan bahwa bisnis terakreditasi wajib melaksanakan prinsip-prinsip bisnis yang baik dan adil tetapi tidak terbatas pada hal-hal yang mengatur mengenai adanya persyaratan atau ketentuan yang jelas mengenai hubungan antara bisnis terakreditasi dengan konsumen. Bisnis terakreditasi disini harus senantiasa menjunjung tinggi konsistensi dengan standar tertinggi kejujuran, keadilan, integritas dan transparansi; selain itu pelaku bisnis yang terakreditasi dilarang membuat klaim, jaminan, representasi atau pernyataan palsu, tidak benar, menyesatkan, tidak akurat atau penipuan di kegiatan usaha atau untuk mendorong pelanggan untuk membeli barang-barang mereka dan / atau menggunakan jasa mereka. Bisnis Terakreditasi harus menerapkan prinsip-prinsip perdagangan yang baik dan adil dalam melakukan

²³⁴ CaseTrust Accreditation Scheme *Code of Practice*. 2014 CaseTrust Department. hlm. 2

praktik bisnis tanpa menggunakan taktik penjualan. Bisnis yang telah terakreditasi harus mematuhi semua hukum dan peraturan yang berlaku termasuk namun tidak terbatas pada Undang-Undang Perlindungan Data Pribadi 2012, untuk melindungi data pribadi konsumen.

3 PRINCIPLES OF GOOD ADVERTISING AND PROMOTIONS

3.1 Accredited businesses undertake to comply with the principles of good advertising and promotions, which include, but are not limited to, the following:

- (a) Accredited businesses shall ensure that all advertisements and promotions are clear, unambiguous, truthful, accurate and not misleading;*
- (b) Accredited businesses shall not permit or allow advertisements or promotions which may contain false, untrue, misleading, inaccurate or fraudulent claims, warranties, representations or statements relating to the goods or services;*
- (c) Accredited businesses shall comply with the Singapore Code of Advertising Practice and such other code(s) as which may be drawn up to regulate advertising and marketing on the internet by any other regulator, or by the CaseTrust; and*
- (d) Any complaint on advertising shall be referred by the CaseTrust to the Advertising Standards Authority of Singapore or other body or bodies as deemed fit by the CaseTrust, for such recommendations and advice on the advertisement.²³⁵*

Kutipan tersebut diatas, apabila diterjemahkan pada nomor 3 mengatur tentang Prinsip Iklan dan promosi yang baik. Pada point ini di sebutkan bahwa bisnis terakreditasi melakukan untuk mematuhi prinsip-prinsip iklan dan promosi yang baik, yang meliputi jelas, tidak ambigu, jujur, akurat dan tidak menyesatkan. Bisnis terakreditasi melarang iklan atau promosi yang memiliki konten palsu, tidak benar, menyesatkan, tidak akurat atau penipuan klaim, jaminan, representasi atau pernyataan yang berkaitan dengan barang atau jasa; Bisnis terakreditasi wajib mematuhi Kode etik bisnis Singapore dan kode

commit to user

²³⁵ *ibid*

etik lain yang digunakan untuk mengatur iklan dan pemasaran di internet.

4 PRINCIPLES OF GOOD CUSTOMER SERVICE

4.1 Accredited businesses undertake to comply with the principles of good customer service, which include, but are not limited to, the following:

- (a) Accredited businesses shall deal promptly and effectively with all customer queries;*
- (b) Accredited businesses shall ensure that all customers will be treated with courtesy;*
- (c) Accredited businesses shall keep adequate records of orders received and ensure fulfilment of all orders for goods or services within the period stipulated in their store or web policies; and*
- (d) Where the goods or services ordered by the customer are unavailable for reasons beyond the control of the accredited business, such must be notified to the customer forthwith and the customer may cancel such order without any penalty whatsoever. This must not negate the accredited business' responsibility to update their records accordingly.²³⁶*

Berdasarkan kutipan tersebut diatas, dapat penulis terjemahkan bahwa pada angka empat mengatur tentang prinsip layanan pelanggan yang baik yang terdiri atas, adanya catatan yang memadai dari pesanan yang diterima dan memastikan pemenuhan semua pesanan untuk barang atau jasa dalam waktu yang ditentukan di toko atau web kebijakan mereka; dan dimana barang atau jasa yang dipesan oleh pelanggan yang tidak tersedia untuk alasan di luar kendali bisnis terakreditasi, seperti harus diberitahukan segera kepada pelanggan dan pelanggan dapat membatalkan pesanan tanpa sanksi apapun.

5 PRINCIPLES OF ELECTRONIC COMMERCE

5.1 Accredited businesses engaged in electronic commerce undertake to comply with the principles of electronic commerce include, but are not limited to the following:

²³⁶ CaseTrust Accreditation Scheme *Code of Practice*. 2014 CaseTrust Department. hlm. 2

- (a) *Displaying prominently on the e-commerce website the name of the trading entity;*
- (b) *Displaying prominently on the e-commerce website, the physical location of its business / operating office;*
- (c) *Displaying prominently on the e-commerce website, the contact information including all available modes of communication, but not limited to, telephone and facsimile numbers and their e-mail addresses;*
- (d) *The accredited business' has a responsibility to fulfil all obligations under the PDPA 2012 and its regulations on the collection, use and disclosure of personal data and also the Do Not Call Registry obligations.*
- (e) *Terms and conditions relating to the use of the website are provided by the CaseTrust, which may be varied from time to time;*
- (f) *The terms and conditions relating to the sale of goods or the provision of services shall be subject to the governing law and jurisdiction of the Republic of Singapore, whilst the refund and exchange policy of the business must be approved by the CaseTrust in writing;*
- (g) *The price of the goods and services, including delivery and all other costs must be set out clearly and*
- (h) *And a hyperlink to CaseTrust website on the e-commerce website.*²³⁷

Pada nomor lima berisi mengenai prinsip perdagangan elektronik diantaranya, bahwa pelaku usaha terakreditasi harus menampilkan nama usaha atau bisnisnya, menyebutkan lokasi atau alamat lengkap, memberikan kontak informasi baik melalui telepon, fax dan alamat email pada *website e commerce*. Pelaku usaha terakreditasi memiliki tanggungjawab untuk memenuhi syarat dan ketentuan yang berkaitan dengan penggunaan *website* yang disediakan oleh *Case Trust* yang dapat berubah dari waktu ke waktu. Syarat dan ketentuan yang berlaku harus tunduk dan patuh pada yuridiksi Republik Singapura sedangkan untuk pengembalian maupun pertukaran kebijakan bisnis harus disetujui *Case Trust* secara tertulis. Harga barang dan jasa termasuk biaya pengiriman dan biaya lain yang timbul dari

²³⁷ CaseTrust Accreditation Scheme *Code of Practice*. 2014 CaseTrust Department. hlm. 3

transaksi bisnis *e commerce* telah diatur dengan jelas dan di Hyperlink ke situs *Case Trust* dan situs *e commerce*.

6 COMPLAINT & DISPUTE RESOLUTION

- 6.1 *Accredited businesses shall maintain an adequate system for monitoring complaints so that appropriate action can be taken to rectify any breach of the principles of good business practice or resolve the customer's grievance.*
- 6.2 *Accredited businesses shall have a fair and effective procedure to handle customer complaints within a reasonable time and will investigate all grievances received from customers, or made on behalf of the customer promptly and diligently. If the grievance is complex and the investigation into the grievance cannot be completed within 21 working days of the receipt of the customer's complaint, a written acknowledgement should be sent to the customer by the business. Such acknowledgement should contain an indication of when a full investigation can be completed, of which should be within a reasonable time.*
- 6.3 *Where the accredited business' investigation reveals that there has been a breach of the principles of good business practice, the accredited business shall take all steps necessary to rectify the said breaches or resolve the grievance.*
- 6.5 *If the customer is not satisfied with the accredited business' efforts to rectify the breach of the principles of good business practice or resolve the grievance, the customer or the business may refer the complaint to CASE Mediation Centre for mediation. In such an instance, the accredited business must attend the mediation. For all intents and purposes, if a matter cannot be resolved for 4 months, then it is deemed that it cannot be resolved for the purpose of Clause 6.2.*
- 6.7 *If there is no settlement at the mediation session at CASE Mediation Centre, either party may refer the matter to CaseTrust Resolution Board within 14 working days after the mediation was concluded.*
- 6.8 *The CaseTrust Department reserves the right to re-investigate any complaint, while the accredited business shall render all necessary assistance for the purpose of such investigations, including but not limited to, the supply of documents related to the investigation or the interview of the accredited business.*²³⁸

Kutipan tersebut diatas, pada nomor 6 mengatur masalah pengaduan dan resolusi perselisihan. Bisnis Terakreditasi memiliki

commit to user

²³⁸*Ibid.* hlm 4

prosedur yang adil dan efektif untuk menangani keluhan pelanggan dalam waktu yang wajar. Jika keluhan tersebut adalah kompleks dan penyelidikan pengaduan tidak dapat diselesaikan dalam waktu 21 hari kerja sejak diterimanya pengaduan pelanggan, keterangan tertulis harus dikirim ke pelanggan yang berisi indikasi kapan penyelidikan penuh dapat diselesaikan, dalam waktu yang wajar. Bila terjadi pelanggaran prinsip-prinsip praktek bisnis yang baik, bisnis terakreditasi harus mengambil semua langkah diperlukan untuk memperbaiki pelanggaran atau mengatasi keluhan tersebut. Konsumen atau pelaku usaha bisnis dapat merujuk keluhan ke Pusat Negosiasi CASE untuk mediasi.

Pelaku usaha terakreditasi harus menghadiri mediasi. Untuk semua maksud dan tujuan, jika suatu hal tidak dapat diselesaikan selama 4 bulan, maka dianggap bahwa itu tidak bisa diselesaikan maka penyelesaian dapat dilanjutkan di sesi mediasi di Pusat Negosiasi CASE, baik pihak dapat merujuk hal tersebut kepada *CaseTrust* Resolusi Dewan dalam waktu 14 hari kerja setelah mediasi itu menyimpulkan.

Departement *CaseTrust* berhak untuk menyelidiki ulang keluhan apapun, sedangkan pelaku usaha harus memberikan semua bantuan yang diperlukan untuk tujuan penyelidikan, termasuk namun tidak terbatas pada, pasokan dokumen yang terkait dengan penyelidikan atau wawancara pada pelaku usaha.

7 MARKETING

7.1 Broadcast Media

Advertorial / Infomercial: Customers must be notified by a clear on-screen and spoken announcement before and after an advertorial/infomercial that it is a paid commercial message. The advertiser and the product or service on offer must be clearly identified. The video announcement must also appear before each ordering opportunity.

7.2 Internet and Other Electronic Media

Application: All forms of electronic media, including, but not limited to, the internet, electronic mail, WAP, interactive kiosks,

databases and computer-based information services, are covered by these guidelines.

7.3 Spamming

As a general rule, email 'spamming' (the process of unasked for mass marketing by email) is regarded as a poor business practice. Un-requested marketing communications must not be sent by email, unless there is an existing relationship between the customer and the business.

7.4 Reply

Every email message must clearly identify the business and provide the person receiving it with a simple and easy-to-use method of replying.

7.5 Email Opt-out

The business must have a system in place to make sure they do not send email communications to anyone who has notified the business that they do not wish to receive such electronic messages.

7.6 Disclosure

When information is being gathered from individual customers that could identify them, and which will be linked with 'click stream' data, they must be advised what information is being collected and how it will be used. This advice must be given before customers send data that could identify them.

7.7 Internet Opt-out

Customers must be given the chance to choose not to have information that identifies them made available to others for marketing purposes. This chance to choose must be offered in every location, site or page from which such data is being collected.²³⁹

Pada nomor 7 diatur mengenai marketing yang dilakukan pelaku usaha terakreditasi. Marketing menggunakan media *broadcast* harus dapat diidentifikasi secara jelas. Iklan yang menggunakan internet dan media elektronik lainnya harus mematuhi kode etik. Setiap pemasaran yang dilakukan menggunakan email harus jelas mengidentifikasi bisnis dan memberikan orang yang menerima dengan metode yang sederhana dan mudah untuk membalas.

8. BREACH OF THIS CODE

8.1 *Where the CaseTrust becomes aware that a breach of this Code or other terms and conditions of being an accredited business has taken place, CaseTrust will provide an opportunity for the accredited business to answer the allegations in writing within 7 working days from the date CaseTrust requested for the answer. Should the accredited business refuse or fail to answer the request in writing within the time specified by CaseTrust, CaseTrust shall proceed with its decision.*

8.2 *If CaseTrust concludes at the end of the time period provided herein that a breach of this Code has occurred, it may in the circumstance decide to issue warnings, suspensions and/or expulsions or a combination thereof. The decision may be brought to the public's attention through the media and CaseTrust's website. In this regard the accredited business will render full co-operation to CaseTrust in coming to its decision including access to information through documents and interviews with the accredited business staff.²⁴⁰*

Bila terjadi pelanggaran atas kode etik ini maka *Case Trust* akan memberikan waktu kepada pelaku usaha terakreditasi untuk menjawab tuduhan secara tertulis dalam waktu 7 hari kerja sejak *Case Trust* meminta jawaban. Jika *CaseTrust* menyimpulkan pada akhir periode waktu yang disediakan terjadi pelanggaran maka *Case Trust* mengeluarkan peringatan, hingga pemberitahuan kepada publik melalui media setelah ada keputusan dari *Case Trust*.

9. CASETRUST LOGO

9.1 Proprietorship

The Consumers Association of Singapore is the sole owner of the CaseTrust Logo and has the power to make all decisions about approval or the use of the said logo. CaseTrust and CASE will be used in the CaseTrust Accreditation Scheme as referring to the same entity.²⁴¹

²⁴⁰ *Ibid.*

10 TRUST SG

10.1 The Consumers Association of Singapore is the Authorised Code Owner (ACO) for the Trust Sg seal.

Pada kode etik nomor sembilan di jelaskan bahwa Asosiasi Konsumen Singapura merupakan pemilik tunggal dari logo *Case Trust* dan memiliki kekuatan untuk membuat semua keputusan tentang persetujuan atau penggunaan logo *CaseTrust* dan CASE akan digunakan dalam Skema *CaseTrust* Akreditasi sebagai petunjuk untuk entitas yang sama. Asosiasi Konsumen Singapura adalah pemilik Resmi Kode untuk segel Kepercayaan Sg.

11. DEFINITIONS & INTERPRETATION

11.1 Except where the context otherwise requires, the following expressions in this Code of Practice shall have the following meanings: "Business" means any business in which the accredited business is engaged in, which the CaseTrust Logo is used or displayed. "CASE" means the Consumers Association of Singapore. "CaseTrust" means the scheme for accrediting any corporation (whether incorporated or unincorporated), firm, organisation, association, person or other legal entity engaged in commerce in Singapore, which agrees to adopt and implement this Code and all other requisite terms and conditions of accreditation, through the adoption of acceptable minimum standards stipulated; also refers to any decision made by the CaseTrust Advisory Council.

"CaseTrust Logo" means such logo as may be from time to time issued by the CaseTrust Department. "DNC Register / Registry" refers to the Do Not Call Register / Registry of the Personal Data Protection Act 2012.

"Code" means this Code of Practice as time to time amended, modified or varied by the CaseTrust.

"Goods" means such goods that the accredited business may offer for sale.

"Accredited business" means any, corporation (whether incorporated or unincorporated), firm, organisation, association, person or other legal entity, which is an accredited business of CaseTrust.²⁴²

"Personal Data Protection Act" also refers as "PDPA" means the Personal Data Protection Act 2012 (Cap. 26) and all

commit to user

its regulations. "Personal details" includes any personal information that could be readily associated with the individual, including but not limited to, name, address, phone number, fax number, email address, personal profile, financial profile, identity card number and credit card information.

"Services" means such services, which the accredited business may offer. "Website" means the internet web page used by an accredited business in the conduct of his electronic commerce business.

11.2 References to any document or agreement include references to such document or agreement as amended, novated, supplemented or replaced from time to time.

11.3 In this Code, unless the context otherwise requires, headings are for ease of reference only and shall not affect the interpretation of this Code; words importing the singular include the plural and vice versa; and words importing a gender include every gender.²⁴³

Nomor 11 dari kode etik berisi mengenai definisi dan interpretasi istilah. "Bisnis" berarti setiap bisnis terakreditasi yang termasuk menggunakan yang Logo *CaseTrust*. "CASE" berarti Asosiasi Konsumen Singapura. "*CaseTrust*" berarti skema untuk akreditasi setiap perusahaan, organisasi perusahaan, asosiasi, orang atau badan hukum lainnya yang bergerak dalam perdagangan di Singapura, yang setuju untuk mengadopsi dan menerapkan Kode Etik ini dan semua hal yang diperlukan lainnya dan kondisi akreditasi, melalui adopsi diterima standar minimum yang ditetapkan; juga mengacu pada setiap keputusan yang dibuat oleh Dewan Penasihat *CaseTrust*.

3) Display *CaseTrust* Singapura

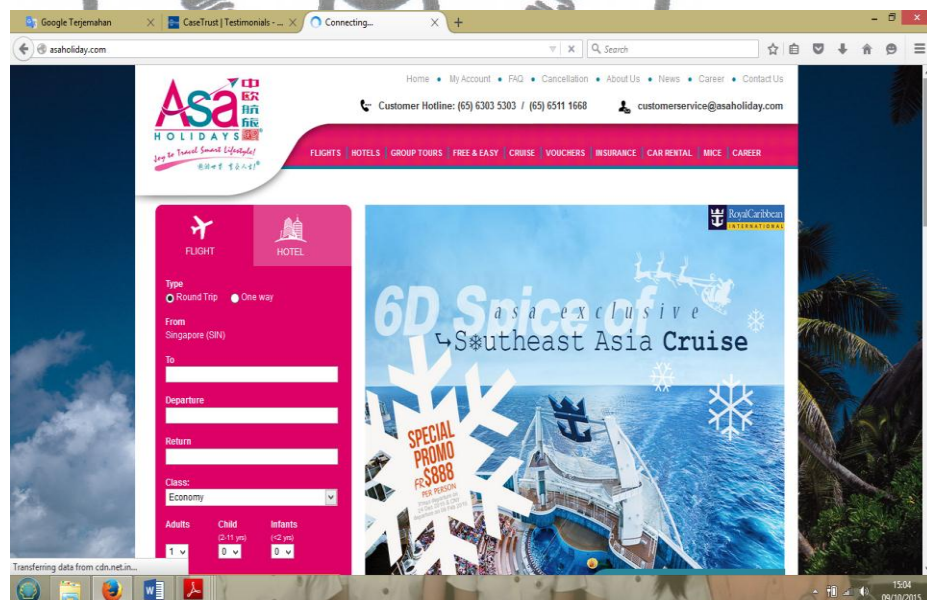
Salah satu Trustmark yang digunakan Singapura bernama *Case Trust* dengan display logo sebagai berikut:

²⁴³ CaseTrust Accreditation Scheme *Code of Practice*. 2014 CaseTrust Department. hlm. 6



Gambar 25. *Case Trust* Singapura²⁴⁴

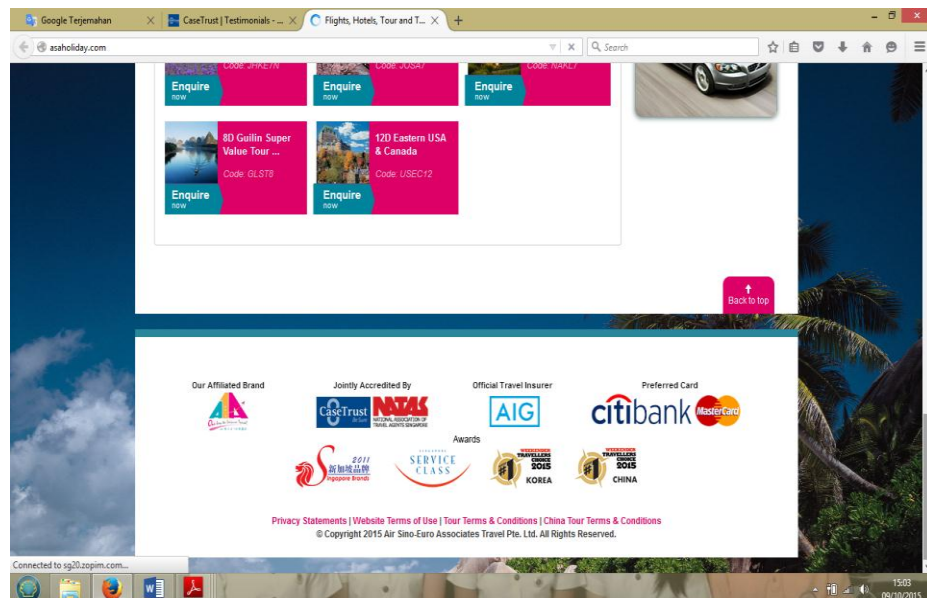
Gambar tersebut diatas merupakan *Trustmark Case Trust* Singapura.



Gambar 26. Salah satu Bisnis terakreditasi oleh *Case TRust*²⁴⁵

²⁴⁴ CaseTrust Accreditation Scheme for Spa & Wellness Business ses. 2015. Hlm. 17

²⁴⁵ *Ibid.*



Gambar 27. Logo *Case Trust* di display pada *website*

Pada gambar tersebut diatas, tampak logo *Trustmark* terdisplay pada *website* yang telah tersertifikasi oleh *Case Trust*. *Trustmark Case Trust* menjamin konsumen atas apa yang diperjanjikan oleh pelaku usaha.

4) Jaminan yang diberikan *CaseTrust* Singapura

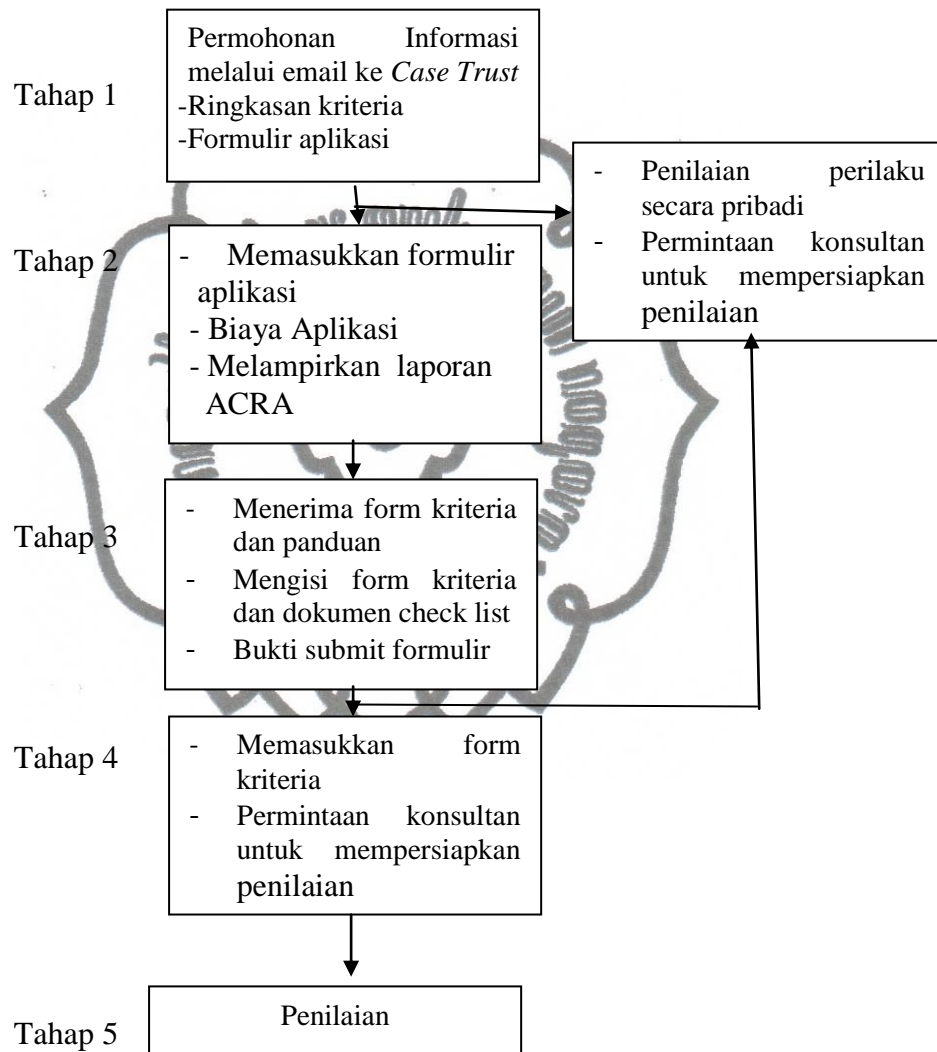
Jaminan yang diberikan oleh *Case Trust* Singapura tertuang di dalam form aplikasi permohonan bagi pelaku usaha. Jaminan tersebut antara lain:

- a) Dasar kebijakan yang mengatur mengenai barang dan jasa, syarat dan kondisi penjualan, harga dan pembayaran, keamanan.
- b) Komunikasi mengatur mengenai komunikasi eksternal serta iklan dan promosi
- c) Pelaksanaan dan sistem. Point ini mengatur tentang transaksi elektronik, setelah penjualan, respon manajemen, keamanan informasi, keamanan pembayaran, Ketersediaan dan Aksesibilitas dari *On-Line* Informasi, Pemantauan Keamanan, Privasi, Perlindungan Anak-anak dan Lansia, Barang dan Jasa

d) Personel mengatur tentang penampilan dan pengetahuan

5) Bagan Alir Prosedur Permohonan *Case Trust*

Alur prosedur permohonan untuk mendapatkan penilaian dari *Case Trust* adalah sebagai berikut:



Sumber: *Case Trust Accreditation Scheme*, 2013

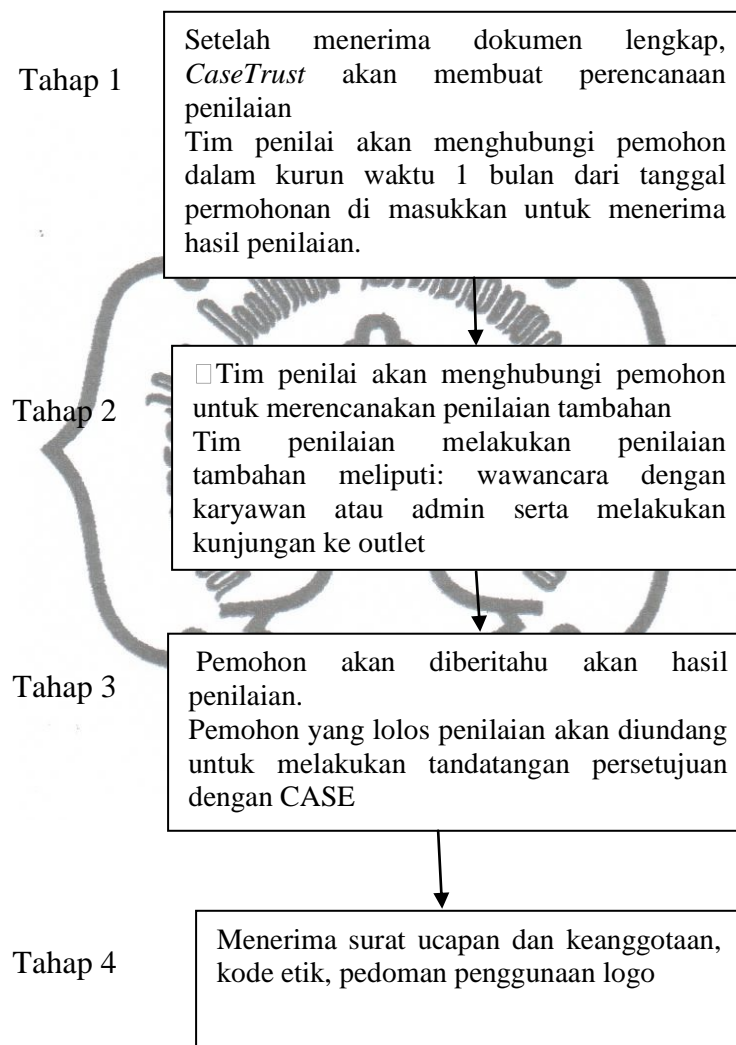
Bagan 2. Prosedur permohonan Penilaian *Case Trust*

Waktu yang digunakan dari mengajukan aplikasi hingga penilaian tergantung dari kelengkapan dokumen yang dikirim ke *Case Trust*. Proses memerlukan waktu antara 2-4 bulan untuk melengkapinya.

commit to user

6) Bagan Alir Prosedur Penilaian *Case Trust*

Proses penilaian yang dilakukan oleh *Case Trust* terhadap pelaku usaha di gambarkan pada bagan alir sebagai berikut:



Sumber : Sumber: *Case Trust Accreditation Scheme*, 2013

Bagan 3. Prosedur Penilaian Case Trust

Penilaian aplikasi *website* akan dilakukan melalui situs. Dilakukan *visitasi webfront* melalui server merupakan bagian dari penilaian situs.

commit to user

Ukuran dasar sertifikasi adalah pemenuhan aturan pelaksanaan yang telah diterapkan di industri yang spesifik, pernyataan praktik bisnis dan kemauan untuk tunduk pada audit oleh *trustmark* tersebut. Aspek lain dari *trustmark* adalah praktik bisnis yang baik dari pedagang yang akan dinilai agar dapat memenuhi syarat sertifikasi. Syarat sertifikasi ini berguna untuk meningkatkan integritas transaksi bisnis yang telah dijelaskan sebagai pengurangan resiko kerugian, kecurangan, dan harapan konsumen yang tidak terpuaskan. Inti dari tujuan *CaseTrust* adalah menghindari perselisihan. *CaseTrust* dapat dipergunakan untuk meminimalkan perselisihan. *CaseTrust* dapat memberikan manfaat dari ketaatannya dengan menyediakan cara penyelesaian perselisihan yang mudah, murah dan cepat ketika perselisihan tidak dapat dihindari dan memerlukan penyelesaian khususnya pada transaksi secara online mengingat persoalan hukum yang dapat digunakan, yuridiksi dan pelaksanaannya lebih kompleks.

g) Status Hukum *Trustmark*

Peraturan yang menetapkan penggunaan *Trustmark* harus terbuka terhadap pemeriksaan publik. *Trustmark* harus diakui sebagai anggota industri harus diuraikan dengan jelas. *Trustmark* organisasi harus terdaftar dalam sertifikasi merk dagang yang diijinkan menurut undang-undang. Pendaftaran *Trustmark* tersebut digunakan untuk melindungi peniruan dari bisnis yang serupa.²⁴⁶

b. *Trustmark* di Malaysia

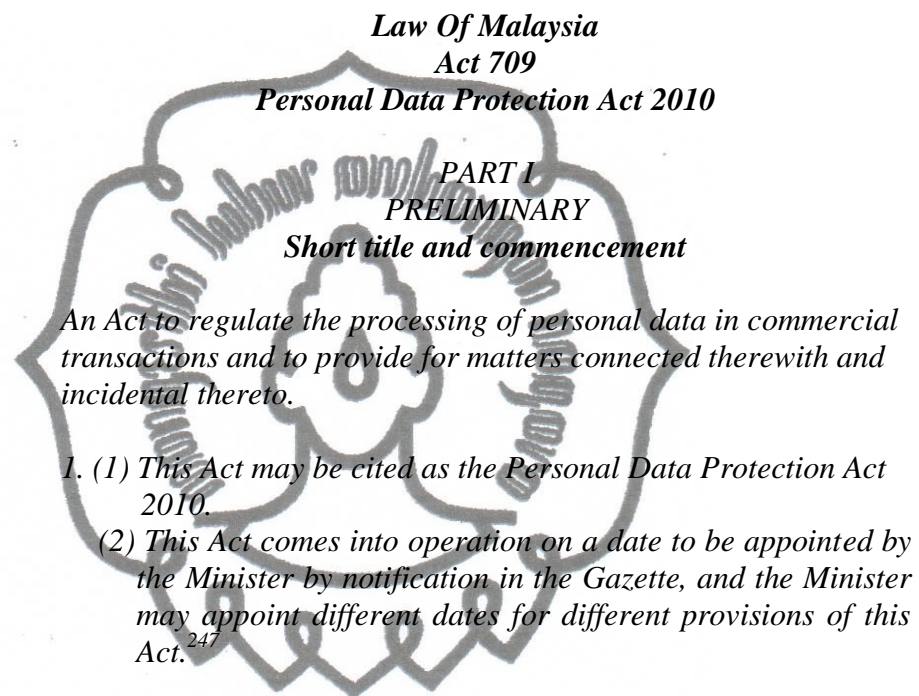
1) Regulasi Malaysia *Trustmark*

Malaysia *Trustmark* diprakarsai oleh Pemerintah Malaysia sebagai sarana memvalidasi legalitas organisasi yang terlibat dalam e-bisnis. Organisasi divalidasi kemudian diberikan dengan Malaysia *Trustmark* sebagai sertifikasi bahwa organisasi tertentu diakui sebagai

commit to user

²⁴⁶ *Ibid*, hlm. 292

operator e-bisnis yang dapat dipercaya. Oleh karena itu, Malaysia *Trustmark* akan membantu konsumen untuk mengidentifikasi situs milik operator e-bisnis yang dapat dipercaya. Dengan cara ini, konsumen dapat melanjutkan dengan pembelian / transaksi dengan keyakinan.



Pada bagian I menjelaskan bahwa Undang-Undang 709 Tahun 2010 merupakan Undang-Undang untuk mengatur data pribadi dalam transaksi bisnis dan untuk menyediakan hal-hal yang berhubungan dengan masalah insidental dalamnya. Pada Pasal 1 ayat (1) menjelaskan secara tegas bahwa Undang-Undang 2010 merupakan Undang-Undang Perlindungan Data Pribadi dan pada ayat (2) pelaksanaan undang-undang ditentukan oleh menteri dengan menunjuk tanggal pada aturan lain yang terpisah dari Undang-Undang ini.

Application

2. (1) *This Act applies to*
 - (a) *any person who processes; and*

commit to user

²⁴⁷ Law of Malaysia, Act 79, *Personal Data Act*, 2010

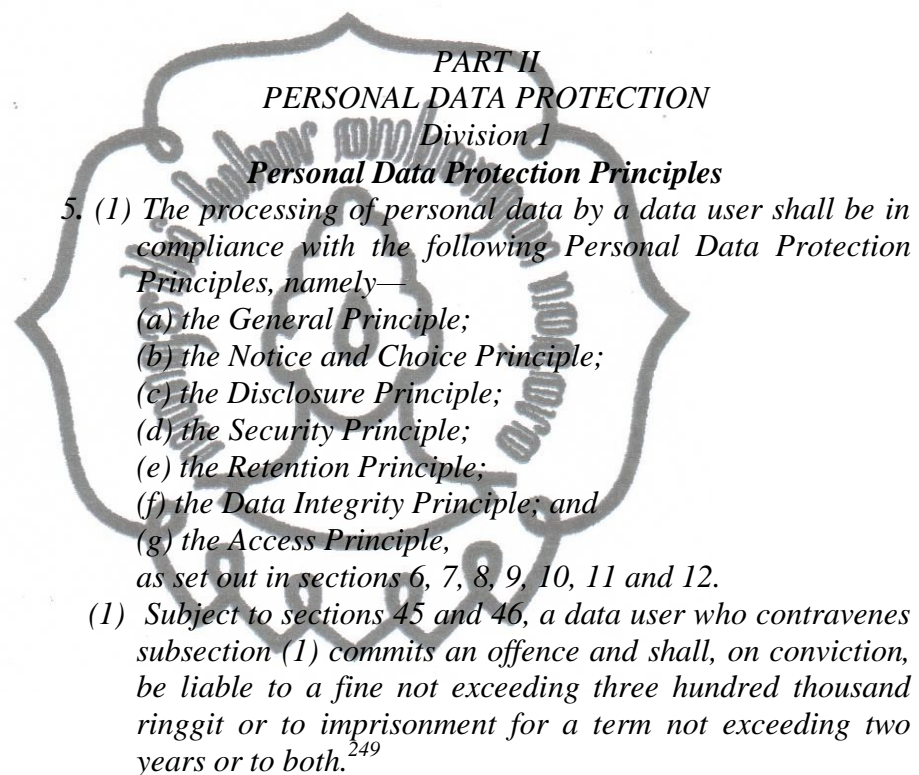
- (b) *any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions*
- (2) *Subject to subsection (1), this Act applies to a person in respect of personal data if—*
 - (a) *the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or*
 - (b) *the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia.*
- (3) *A person falling within paragraph (2)(b) shall nominate for the purposes of this Act a representative established in Malaysia.*
- (4) *For the purposes of subsections (2) and (3), each of the following is to be treated as established in Malaysia:*
 - (a) *an individual whose physical presence in Malaysia shall not be less than one hundred and eighty days in one calendar year;*
 - (b) *a body incorporated under the Companies Act 1965 [Act 125];*
 - (c) *a partnership or other unincorporated association formed under any written laws in Malaysia; and*
 - (d) *any person who does not fall within paragraph (a), (b) or (c) but maintains in Malaysia—*
 - (i) *an office, branch or agency through which he carries on any activity; or*
 - (ii) *a regular practice.*²⁴⁸

Pasal 2 memberikan penjelasan subjek hukum yang dimaksud dalam Undang-Undang Perlindungan Data pribadi, yaitu berlaku untuk setiap orang yang memproses, dan setiap orang yang memiliki kontrol atas kewenangan pengolahan data pribadi yang berhubungan dengan transaksi bisnis. Orang yang dimaksud baik berkedudukan di Malaysia selama 180 hari dalam satu tahun kalender maupun tidak berkedudukan di Malaysia tetapi menggunakan peralatan di Malaysia untuk memproses data pribadi meskipun hanya bertujuan sebagai transit data melalui Malaysia. Badan Hukum bisnis yang didikan berdasarkan

²⁴⁸ *Ibid.*

Company Act 1965, asosiasi yang dibentuk dibawah aturan hukum tertulis Malaysia dan orang yang berada di Malaysia namun menjalankan aktivitas di Malaysia.

Prinsip-prinsip yang diatur dalam Undang-Undang Perlindungan Data Pribadi ini diatur dalam Bagian II sebagai berikut:



Prinsip perlindungan data pribadi yang dimaksud adalah dalam pengolahan data pribadi harus memenuhi unsur sebagai mana yang disebutkan dalam prinsip umum, prinsip pemberitahuan, prinsip keamanan, prinsip retensi, prinsip keamanan, prinsip integritas data dan prinsip akses data yang harus tunduk pada peraturan nomor 6, 7, 8, 9, 10, 11 dan 12. Bagi yang melanggar adakan di kenai dengan maksimal 300 Ringgit atau penjara dalam jangka waktu dua tahun.

²⁴⁹ Law of Malaysia, Act 79, *Personal Data Act*, 2010

General Principle

6. (1) A data user shall not—

- (a) in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his consent to the processing of the personal data; or
- (b) in the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with the provisions of section 40.

(2) Notwithstanding paragraph (1)(a), a data user may process personal data about a data subject if the processing is necessary—

- (a) for the performance of a contract to which the data subject is a party;
- (b) for the taking of steps at the request of the data subject with a view to entering into a contract;
- (c) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;
- (d) in order to protect the vital interests of the data subject;
- (e) for the administration of justice; or
- (f) for the exercise of any functions conferred on any person by or under any law.

(3) Personal data shall not be processed unless—

- (a) the personal data is processed for a lawful purpose directly related to an activity of the data user;
- (b) the processing of the personal data is necessary for or directly related to that purpose; and
- (c) the personal data is adequate but not excessive in relation to that purpose.²⁵⁰

Prinsip umum terdapat dalam nomor 6 yang menjelaskan bahwa pengguna data tidak menggunakan data pribadi dan melakukan proses data pribadi kecuali jika subjek menyetujui. Penggunaan dan pemrosesan data pribadi dapat dilakukan jika merupakan data bersama, data yang diperlukan untuk pemenuhan draft kontrak atas permintaan subjek data serta untuk memenuhi kewajiban hukum subjek pengguna data yang berfungsi untuk melindungi kepentingan vital subjek data dan untuk memenuhi syarat administrasi peradilan atau fungsi-fungsi lain yang diberikan kepada seseorang atau badan hukum yang

commit to user

²⁵⁰ *Ibid.*

diatur dalam Undang-Undang. Data pribadi tidak akan diproses kecuali data pribadi tersebut untuk kepentingan hukum yang berkaitan langsung dengan kegiatan penggunaan data. Pengolahan data pribadi yang diperlukan untuk atau berkaitan langsung dengan dengan tujuan tersebut dan data pribadi yang diberikan tidak berlebihan dalam kaitannya dengan tujuan tersebut.

Notice and Choice Principle

7. (1) A data user shall by written notice inform a data subject—
- (a) that personal data of the data subject is being processed by or on behalf of the data user, and shall provide a description of the personal data to that data subject;
 - (b) the purposes for which the personal data is being or is to be collected and further processed;
 - (c) of any information available to the data user as to the source of that personal data;
 - (d) of the data subject's right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data;
 - (e) of the class of third parties to whom the data user discloses or may disclose the personal data;
 - (f) of the choices and means the data user offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;
 - (g) whether it is obligatory or voluntary for the data subject to supply the personal data; and
 - (h) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data.
- (2) The notice under subsection (1) shall be given as soon as practicable by the data user—
- (a) when the data subject is first asked by the data user to provide his personal data;
 - (b) when the data user first collects the personal data of the data subject; or
 - (c) in any other case, before the data user—
 - (i) uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected; or

commit to user

- (ii) discloses the personal data to a third party.²⁵¹
- (3) A notice under subsection (1) shall be in the national and English languages, and the individual shall be provided with a clear and readily accessible means to exercise his choice, where necessary, in the national and English languages.

Lebih lanjut pada nomor tujuh menjelaskan mengenai pilihan dan pemberitahuan. Seorang pengguna data harus dengan pemberitahuan tertulis menginformasikan subject data yang menerangkan bahwa data pribadi dari subject data sedang di proses atau atas nama pengguna data dan harus memberikan deskripsi data pribadi untuk subject data. Harus menerangkan mengenai tujuan data pribadi yang sedang dikumpulkan atau diproses. Hak subjek data untuk meminta akses dan meminta koreksi data pribadi serta menjelaskan cara menghubungi pengguna data sehubungan dengan pertanyaan dan keluhan atas data pribadi dari pihak ketiga pengguna data pribadi. Pilihan yang dimaksud dalam aturan ini adalah pengguna data menawarkan kepada subjek data untuk membatasi pengolahan data pribadi termasuk data yang berhubungan dengan orang lain yang dapat diidentifikasi dari data pribadi. Pilihan tersebut wajib atau sukarela bagi subjek data untuk memasukkan data pribadi.

Disclosure Principle

8. Subject to section 39, no personal data shall, without the consent of the data subject, be disclosed—
- (a) for any purpose other than—
- (i) the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or
 - (ii) a purpose directly related to the purpose referred to in subparagraph (i);
- (b) to any party other than a third party of the class of third parties as specified in paragraph 7(1)(e).²⁵²

Nomor delapan dalam Undang-Undang ini menyebutkan mengenai prinsip keterbukaan. Prinsip keterbukaan ini menjelaskan

²⁵¹ Law of Malaysia, Act 79, *Personal Data Act*, 2010

²⁵² *ibid*

bahwa subject data harus mengetahui adanya keterbukaan informasi dari tujuan dari pengumpulan data pribadi hingga tujuan pengumpulan data pribadi tersebut berhubungan dengan pihak ketiga.

Security Principle

9. (1) *A data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard—*
- (a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;*
 - (b) to the place or location where the personal data is stored;*
 - (c) to any security measures incorporated into any equipment in which the personal data is stored;*
 - (d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and*
 - (e) to the measures taken for ensuring the secure transfer of the personal data.*
- (2) *Where processing of personal data is carried out by a data processor on behalf of the data user, the data user shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, ensure that the data processor—*
- (a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and*
 - (b) takes reasonable steps to ensure compliance with those measures.*²⁵³

Prinsip keamanan dijelaskan dalam nomor sembilan yang mengatakan bahwa seorang pengguna data ketika memproses data pribadi, harus mengambil langkah-langkah praktis untuk melindungi data pribadi dari kerugian, penyalahgunaan, modifikasi, akses yang tidak sah atau tidak disengaja atau pengungkapan, perubahan atau

²⁵³ Law of Malaysia, Act 79, *Personal Data Act*, 2010

perusakan dengan memiliki pengamanan mengingat sifat data pribadi dan bahaya yang akan dihasilkan dari kerugian, penyalahgunaan, modifikasi, akses yang tidak sah atau tidak disengaja atau pengungkapan, perubahan atau perusakan. Pengamanana dalam hal tempat atau lokasi di mana data pribadi yang disimpan. Perlu mengambil langkah-langkah keamanan dimasukkan ke dalam peralatan dimana data pribadi disimpan. Langkah-langkah tersebut berfungsi untuk menjamin keandalan, integritas dan kompetensi personel memiliki akses ke data pribadi.

Pengamanan data pribadi digunakan untuk memastikan transfer data secara aman. Apabila pengolahan data pribadi dilakukan oleh prosesor data atas nama pengguna data, data pengguna dengan tujuan untuk melindungi data pribadi dari kerugian, penyalahgunaan, modifikasi, akses yang tidak sah atau tidak disengaja atau pengungkapan, perubahan atau perusakan, harus memastikan bahwa data processor- memberikan jaminan yang memadai sehubungan dengan langkah-langkah keamanan teknis dan organisasi yang mengatur pengolahan data yang akan dilakukan; dan (b) mengambil langkah-langkah yang wajar untuk memastikan kepatuhan langkah-langkah pengamanan data pribadi.

Retention Principle

10. (1) *The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.*
- (2) *It shall be the duty of a data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.*²⁵⁴

Data pribadi dengan tujuan apapun tidak seharusnya disimpan lebih lama dari keperluan tujuan tersebut. Hal ini menjadi tugas dari

²⁵⁴ Law of Malaysia, Act 79, *Personal Data Act*, 2010

pengguna data untuk mengambil langkah yang wajar untuk memastikan bahwa semua data pribadi secara permanen dihapus jika sudah tidak diperlukan untuk tujuan tertentu.

Data Integrity Principle

11. *A data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.*

Access Principle

12. *A data subject shall be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under this Act.*²⁵⁵

Prinsip integritas data merupakan langkah-langkah pengguna data untuk memastikan bahwa informasi data pribadi yang diberikan adalah lengkap, tidak menyesatkan dan terus up to date dengan memperhatikan tujuan terkait dimana data pribadi dikumpulkan dan diproses lebih lanjut.

Prinsip akses bahwa subjek data yang memberikan data pribadi yang dimiliki pengguna data harus dapat memperbaiki data pribadi dimana data pribadi tidak akurat, tidak lengkap, menyesatkan atau tidak up to date, kecuali permintaan untuk mengakses atau mengoreksi tersebut di tolak berdasarkan Undang-Undang.

*Division 2
Registration*

Application of this Division

13. (1) *This Division shall apply to a data user who belongs to a class of data users as specified in the order made under subsection 14(1).*

(2) *A data user who belongs to a class of data users not specified in the order made under subsection 14(1) shall comply with all the provisions of this Act other than the*

commit to user

²⁵⁵ Law of Malaysia, Act 79, Personal Data Act, 2010

provisions of this Division relating to the registration of data users and matters connected thereto.

Divisi dua menerangkan tentang pendaftaran. Pendaftaran ini diperuntukkan bagi yang dijelaskan dalam nomor 14. Bahwa tidak semua pengguna data ditentukan memenuhi apa yang disebutkan dalam nomor 14

Registration of data users

14. (1) *The Minister may, upon the recommendation of the Commissioner, by order published in the Gazette, specify a class of data users who shall be required to be registered as data users under this Act.*

(2) *The Commissioner shall, before making his recommendation under subsection (1), consult with—*

(a) such bodies representative of data users belonging to that class; or

*(b) such other interested persons.*²⁵⁶

Pendaftaran pengguna data menerangkan bahwa Menteri atas rekomendasi Komisaris, dapat memberikan perintah yang diumumkan dalam Berita, untuk menentukan pengguna data mana yang wajib terdaftar sebagai pengguna data di bawah Undang-Undang ini. Komisaris wajib, berkonsultasi dengan perwakilan badan-badan tersebut dari pengguna data seperti yang diatur dalam Undang-Undang.

Application for registration

15. (1) *A person who belongs to the class of data users as specified in the order made under subsection 14(1) shall submit an application for registration to the Commissioner in the manner and form as determined by the Commissioner.*

(2) *Every application for registration shall be accompanied with the prescribed registration fee and such documents as may be required by the Commissioner.*

(3) *The Commissioner may in writing at any time after receiving the application and before it is determined, require the applicant to provide such additional*

commit to user

²⁵⁶ *Ibid.*

documents or information within the time as specified by the Commissioner.

- (4) *If the requirement under subsection (3) is not complied with, the application for registration shall be deemed to have been withdrawn by the applicant and shall not be further proceeded with by the Commissioner, but without prejudice to a fresh application being made by the applicant.*²⁵⁷

Permohonan pendaftaran wajib mereka yang telah ditentukan dalam keputusan menteri. Setiap permohonan pendaftaran harus disertai dengan biaya pendaftaran yang ditentukan serta kelengkapan dokumen yang diperlukan. Komisaris setiap saat dapat menerima aplikasi permohonan dan secara tertulis dapat meminta dokumen atau informasi kelengkapan data dalam waktu yang ditentukan. Jika syarat tersebut tidak dipenuhi permohonan pendaftaran dianggap telah ditarik oleh pemohon dan tidak akan diproses lebih lanjut oleh komisaris.

Certificate of registration

16. (1) *After having given due consideration to an application under subsection 15(1), the Commissioner may—*
- (a) *register the applicant and issue a certificate of registration to the applicant in such form as determined by the Commissioner; or*
 - (b) *refuse the application.*
- (2) *The certificate of registration may be issued subject to such conditions or restrictions as the Commissioner may think fit to impose.*
- (3) *Where the Commissioner refuses the application for registration in pursuance of subsection (1), he shall inform the applicant by a written notice that the application has been refused and the reasons for the refusal.*
- (4) *A person who belongs to the class of data users as specified in the order made under subsection 14(1) and who processes personal data without a certificate of registration issued in pursuance of paragraph 16(1)(a) commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to*

commit to user

²⁵⁷ Law of Malaysia, Act 79, Personal Data Act, 2010

*imprisonment for a term not exceeding three years or to both.*²⁵⁸

Sertifikat pendaftaran dijelaskan dalam nomor 16 bahwa akan diberikan apabila pemohon telah memenuhi persyaratan seperti yang dikatakan dalam nomor 15 ayat (1). Komisaris dapat menerima atau menolak permohonan pendaftaran. Sertifikat akan diterbitkan dengan batas waktu yang telah ditentukan. Bila permohonan ditolak, komisaris akan memberitahukan secara tertulis bahwa aplikasi telah ditolak disertai dengan alasan penolakan aplikasi tersebut. Bagi seseorang atau yang telah ditentukan oleh menteri melakukan memrosesan data pribadi tanpa sertifikat pendaftaran maka telah melakukan pelanggaran dan akan didenda tidak lebih dari lima ratus ribu ringgit atau penjara tidak lebih dari tiga tahun atau keduanya.

Renewal of certificate of registration

17. (1) *A data user may make an application for the renewal of the certificate of registration not later than ninety days before the date of expiry of the certificate of registration in the manner and form as determined by the Commissioner and the application shall be accompanied with the prescribed renewal fee and such documents as may be required by the Commissioner, but no application for renewal shall be allowed where the application is made after the date of expiry of the certificate of registration.*
- (2) *When renewing a certificate of registration, the Commissioner may vary the conditions or restrictions imposed upon the issuance of the certificate of registration or impose additional conditions or restrictions.*
- (3) *The Commissioner may refuse to renew a certificate of registration—*
- (a) if the data user has failed to comply with any of the provisions of this Act;*
 - (b) if the data user has failed to comply with any conditions or restrictions imposed upon the issuance of the certificate of registration; or*²⁵⁹

²⁵⁸ *Ibid.*

commit to user

²⁵⁹ Law of Malaysia, Act 79, Personal Data Act, 2010

(c) if he is satisfied that the data user is unable to continue the processing of personal data in accordance with this Act.

Pengguna data dimungkinkan untuk membuat aplikasi untuk memperpanjang sertifikat pendaftaran paling lambat sembilan puluh hari sebelum tanggal berakhirnya sertifikat pendaftaran dengan cara dan bentuk yang ditetapkan oleh Komisaris. Perpanjangan aplikasi tersebut akan dikenai biaya perpanjangan yang ditentukan oleh dokumen-dokumen seperti yang ditetapkan komisaris. Permohonan perpanjangan akan diijinkan sepanjang aplikasi tersebut dibuat setelah tanggal berakhirnya sertifikat pendaftaran. Ketika memperbarui sertifikat pendaftaran, diberlakukan ketentuan yang berbeda berupa ketentuan tambahan atau pembatasan. Komisaris dapat menolak untuk memperbaharui sertifikat jika pengguna data telah gagal untuk mematuhi setiap ketentuan Undang-Undang, gagal untuk mematuhi persyaratan atau pembatasan yang diberlakukan pada penerbitan sertifikat pendaftaran; atau jika data pengguna tidak dapat melanjutkan pengolahan data pribadi sesuai dengan Undang-Undang ini.

Revocation of registration

18. (1) The Commissioner may revoke the registration of a data user if the Commissioner is satisfied that—

- (a) the data user has failed to comply with any of the provisions of this Act;*
- (b) the data user has failed to comply with any conditions or restrictions imposed upon the issuance of the certificate of registration;*
- (c) the issuance of the certificate of registration was induced by a false representation of fact by the data user; or*
- (d) the data user has ceased to carry on the processing of personal data.*

(2) Notwithstanding subsection (1), the Commissioner shall not revoke the registration of a data user unless the Commissioner is satisfied that, after giving the data user an opportunity of making any representation in writing he may wish to make, the registration should be revoked.

- (3) *Where the registration of the data user is revoked, the Commissioner shall issue a notice of revocation of registration to the data user, and the certificate of registration issued in respect of such registration shall have no effect upon service of the notice of revocation of registration.*
- (4) *A data user whose registration has been revoked under this section and who continues to process personal data thereafter commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.*²⁶⁰

Komisaris dapat mencabut pendaftaran pengguna data pengguna telah gagal untuk mematuhi setiap ketentuan Undang-Undang, gagal untuk mematuhi persyaratan atau pembatasan yang diberlakukan pada penerbitan sertifikat pendaftaran, penerbitan sertifikat pendaftaran diinduksi oleh representasi palsu fakta oleh pengguna data; atau pengguna telah berhenti untuk melakukan pengolahan data pribadi.. Dalam penyimpangan dalam mematuhi Undang-Undang, Komisaris wajib tidak mencabut pendaftaran pengguna data kecuali Komisaris memberikan pengguna data kesempatan untuk membuat presentasi tertulis sehingga pendaftaran tidak harus dicabut. Dalam hal pendaftaran pengguna data dicabut, Komisaris menerbitkan pemberitahuan pencabutan pendaftaran kepada pengguna data, dan sertifikat pendaftaran yang dikeluarkan sehubungan pendaftaran tersebut harus tidak berpengaruh terhadap pelayanan pemberitahuan pencabutan pendaftaran. Bila pengguna data yang telah registrasi dicabut dan tetap memproses data pribadi setelah melakukan pelanggaran maka dikenakan denda tidak melebihi lima ratus ribu ringgit atau penjara untuk jangka waktu tidak melebihi tiga tahun atau keduanya.

²⁶⁰ Law of Malaysia, Act 79, *Personal Data Act*, 2010

Surrender of certificate of registration

19. (1) *Where the certificate of registration is revoked in pursuance of section 18, the holder of the certificate shall, within seven days from the date of service of the notice of revocation of registration, surrender the certificate to the Commissioner.*
- (2) *A person who fails to comply with subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.*²⁶¹

Bila sertifikat pendaftaran dicabut menurut bagian 18, pemegang sertifikat wajib, dalam waktu tujuh hari dari tanggal pelayanan melakukan pemberitahuan pencabutan pendaftaran dan menyerahkan sertifikat kepada Komisaris. Bila dalam waktu tujuh hari setelah pemberitahuan pencabutan tidak menyerahkan sertifikat dikenakan denda tidak melebihi dua ratus ribu ringgit atau penjara untuk jangka waktu tidak lebih dari dua tahun atau kedua

Register of Data Users

20. (1) *The Commissioner shall maintain a Register of Data Users in accordance with section 128.*
- (2) *The Register of Data Users shall contain the names of data users who have been registered in pursuance of this Division and any other particulars regarding such data users as may be determined by the Commissioner.*²⁶²

Komisaris wajib memelihara Daftar Data Pengguna. Dalam pendafaran Pengguna data harus memuat nama-nama pengguna data yang telah terdaftar menurut Divisi dan setiap keterangan lainnya mengenai pengguna data seperti dapat ditentukan oleh Komisaris.

²⁶¹ *Ibid.*

²⁶² Law of Malaysia, Act 79, *Personal Data Act*, 2010

*Division 3**Data user forum and code of practice****Data user forum***

21. (1) *The Commissioner may designate a body as a data user forum in respect of a specific class of data users for the purposes of this Act by notifying that body in writing, if the Commissioner is satisfied that—*
- (a) the membership of the body is open to all data users of that class;*
 - (b) the body is capable of performing as required under the relevant provisions of this Act; and*
 - (c) the body has a written constitution.*
- (2) The body shall agree in writing to be a data user forum before the designation is registered by the Commissioner in the Register of Data User Forums.*
- (3) The Commissioner may decide that an existing body that was previously designated as a data user forum under subsection (1) is no longer a data user forum for the purposes of this Act, if he is satisfied that the body no longer meets the requirements as set out in that subsection.*
- (4) Where the Commissioner decides that an existing body which has been designated as a data user forum is no longer a data user forum for the purposes of this Act, he shall withdraw the designation and subsequently cancel the registration of the designation in the Register of Data User Forums.*
- (5) A designation or withdrawal of designation under this section shall take effect from the date of registration of the designation or the date of cancellation of the registration of the designation, as the case may be, or such later date as specified by the Commissioner.²⁶³*

Komisaris dapat menunjuk suatu badan sebagai forum data pengguna untuk tujuan Undang-Undang dengan memberitahukan secara tertulis, keanggotaan forum terbuka untuk semua badan sesuai yang dipersyaratkan dalam ketentuan yang relevan dari Undang-Undang ini. Anggota forum memiliki konstitusi tertulis. Anggota harus menyetujui secara tertulis untuk menjadi forum data pengguna

²⁶³ Law of Malaysia, Act 79, *Personal Data Act*, 2010

sebelum penunjukan terdaftar oleh Komisaris dalam Daftar Forum Data Pengguna Forum. Komisaris dapat memutuskan bahwa sebuah badan yang ada yang sebelumnya ditunjuk sebagai forum data pengguna dalam ayat (1) tidak lagi menjadi forum data pengguna untuk tujuan Undang-Undang jika tidak lagi memenuhi persyaratan sebagaimana diatur dalam Undang-Undang. Apabila Komisaris memutuskan bahwa sebuah badan yang ada yang telah ditunjuk sebagai forum data pengguna tidak lagi menjadi forum data pengguna untuk tujuan Undang-undang ini, komisaris akan menarik penunjukan dan kemudian membatalkan pendaftaran penunjukan dalam Daftar Data Pengguna Forum. Penunjukkan atau penarikan berlaku dari tanggal pendaftaran penunjukan atau tanggal pembatalan penunjukan seperti yang ditentukan oleh Komisaris .

Register of Data User Forums

22. (1) *The Commissioner shall maintain a Register of Data User Forums in accordance with section 128.*

(2) *The Register of Data User Forums shall contain the names of data user forums which have been designated and registered in pursuance of this Division and any other particulars regarding such data user forums as may be determined by the Commissioner.*²⁶⁴

Komisaris wajib memelihara Daftar Data Pengguna Forum. Bagian pendaftaran memuat Data Pengguna Forum yang telah ditunjuk dan terdaftar menurut Divisi ini dan keterangan lain mengenai forum pengguna data ditentukan oleh Komisaris.

Code of practice

23. (1) *A data user forum may prepare a code of practice—*

(a) on its own initiative; or

(b) upon request by the Commissioner.

(2) *The data user forum shall, in preparing a code of practice under subsection (1), consider matters including—*

²⁶⁴ Law of Malaysia, Act 79, *Personal Data Act*, 2010

- (a) the purpose for the processing of personal data by the data user or class of data users;*
- (b) the views of the data subjects or groups representing data subjects;*
- (c) the views of the relevant regulatory authority, if any, to which the data user is subject to; and*
- (d) that the code of practice, upon having regard to all of the matters in paragraphs (a), (b) and (c) and any other matters, offers an adequate level of protection for the personal data of the data subjects concerned.*
- (3) The Commissioner may register the code of practice prepared pursuant to subsection (1), if the Commissioner is satisfied that—*
 - (a) the code of practice is consistent with the provisions of this Act; and*
 - (b) the matters as set out in subsection (2) have been given due consideration.*
- (4) The code of practice under subsection (1) shall take effect on the date of registration of the code of practice by the Commissioner in the Register of Codes of Practice.*
- (5) If the Commissioner refuses to register the code of practice, the Commissioner shall notify the relevant data user forum of his decision in writing and provide the reasons for it.*
- (6) If the Commissioner neither registers nor refuses to register a code of practice within thirty days from the date of receipt of the code of practice by him for registration, he shall be deemed to have refused the registration of the code of practice.*
- (7) The Commissioner may register different codes of practice for different classes of data users.*
- (8) The Commissioner and data user shall make available to the public any code of practice registered under subsection (3).²⁶⁵*

Forum data pengguna wajib mempersiapkan kode etik praktek atas inisiatif sendiri maupun permintaan Komisariss. Forum data pengguna akan, dalam mempersiapkan kode praktek dalam ayat (1), dengan pertimbangan hal-hal termasuk tujuan pengolahan data pribadi oleh pengguna data atau kelas pengguna data; pandangan dari subyek data atau kelompok yang mewakili data tertentu, kode etik

dengan memperhatikan semua hal dalam ayat (a), (b) dan (c) dan hal-hal lain, menawarkan tingkat perlindungan yang memadai untuk data pribadi dari subyek data yang bersangkutan. Kode etika harus konsisten dengan ketentuan Undang-undang. Kode etik berlaku pada tanggal pendaftaran kode praktek oleh Komisaris dalam Daftar Kode Etik. Jika Komisaris menolak untuk mendaftarkan kode praktek, Komisaris wajib memberitahukan forum data pengguna terkait keputusannya secara tertulis dan memberikan alasan untuk itu. Jika Komisaris menolak pendaftaran kode etik dalam waktu tiga puluh hari sejak tanggal diterimanya kode etik olehnya untuk pendaftaran, maka akan dianggap telah menolak pendaftaran kode etik. Komisaris dapat mendaftar kode yang berbeda dari praktek untuk kelas yang berbeda dari pengguna data.

Commissioner may issue code of practice

24. (1) *The Commissioner may issue a code of practice, if—*

- (a) a code of practice is not prepared under paragraph 23(1)(a);*
- (b) the Commissioner is satisfied that a code of practice for a specific class of data users is unlikely to be prepared by the relevant data user forum within the period as specified by the Commissioner; or*
- (c) there is no data user forum to develop the relevant code of practice for the class of data users.*

(2) *The Commissioner shall, before issuing a code of practice under subsection (1), consider matters including—*

- (a) the purpose for the processing of personal data by the data user or class of data users;*
- (b) the views of the data users or groups representing data users, to which the code of practice is applicable;*
- (c) the views of the data subjects or groups representing data subjects;*
- (d) the views of the relevant regulatory authority, if any, to which the data user is subject to; and*
- (e) that the code of practice, upon having regard to all of the matters in paragraphs (a), (b) and (c) and any other matters, offers an adequate level of protection for the personal data of the data subjects concerned.*

- (3) *The Commissioner may issue different codes of practice for different classes of data users.*
- (4) *The code of practice issued by the Commissioner under subsection (1) shall be registered in the Register of Codes of Practice.*
- (5) *The code of practice under subsection (1) shall take effect on the date of registration of the code of practice by the Commissioner.*
- (6) *The Commissioner shall make available to the public any code of practice issued by him under subsection (1).²⁶⁶*

Komisaris dapat mengeluarkan kode etik jika tidak disiapkan oleh forum data pengguna yang relevan dalam periode yang ditentukan oleh Komisaris; atau tidak ada forum data pengguna yang mengembangkan kode praktek yang relevan untuk kelas pengguna data. Sebelum mengeluarkan kode etik, Komisaris wajib, pertimbangkan hal-hal termasuk tujuan untuk pengolahan data pribadi oleh pengguna data atau kelas pengguna data; pandangan dari pengguna data atau kelompok yang mewakili pengguna data, dimana kode etik yang berlaku; pandangan dari pihak otoritas yang relevan, jika ada, dimana data pengguna tunduk; dan kode etik harus menawarkan tingkat perlindungan yang memadai untuk data pribadi dari subyek data yang bersangkutan. Komisaris dapat mengeluarkan kode etik yang berbeda dari praktek untuk subjek yang berbeda dari pengguna data. Kode etik yang dikeluarkan oleh Komisaris wajib didaftarkan dalam Daftar Kode Etik. Kode etik) mulai berlaku pada tanggal pendaftaran kode etik oleh Komisaris.

Applicable code of practice

- 25. (1) *The Commissioner shall ensure that there is only one code of practice registered for a class of data users at a given time.*
- (2) *All data users belonging to a class of data users shall comply with the relevant registered code of practice that is applicable to that class of data users at a given time.*

commit to user

²⁶⁶ Law of Malaysia, Act 79, Personal Data Act, 2010

- (3) *Where a code of practice is registered by the Commissioner under section 23 or 24, the Commissioner shall notify, in such manner as he may determine, the relevant class of data users to whom the code of practice is applicable—*
- (a) of the identity of the code of practice concerned and the date on which the code of practice is to take effect; and*
 - (b) of the specific requirements under this Act for which the code of practice is issued and registered.*
- (4) *If there is any uncertainty or ambiguity as to which code of practice is applicable to a particular data user or class of data users, the data user or person concerned may apply to the Commissioner for his opinion on which code of practice is the applicable code of practice in relation to the circumstances of such data user or person.*
- (5) *The Commissioner shall provide his opinion within thirty days from the date of receipt of an application made under subsection (4).*
- (6) *The Commissioner shall, when making his opinion under subsection (5), take into account any relevant previous opinions, if any.*
- (7) *The Commissioner may withdraw an opinion made under this section if the Commissioner is satisfied that the nature of the activity engaged by the data user has changed materially.²⁶⁷*

Komisaris wajib memastikan bahwa hanya ada satu kode etik terdaftar untuk kelas pengguna data pada waktu tertentu. Semua pengguna data harus sesuai dengan kode kode etik terdaftar yang relevan dan berlaku untuk kelas pengguna data dalam waktu tertentu. Apabila kode etik terdaftar oleh Komisaris di bawah bagian 23 atau 24, Komisaris wajib memberitahukan, dengan cara menentukan kelas yang relevan dari pengguna data dan kepada siapa kode etik diterapkan. Identitas kode etik yang bersangkutan dan tanggal dimana kode etik tersebut berlaku. Ketidakpastian atau ambiguitas pada kode etik maka pengguna data atau orang yang bersangkutan dapat mengajukan permohonan kepada Komisaris pendapatnya yang

²⁶⁷ *Ibid.*

kode praktek adalah Kode berlaku praktek dalam kaitannya dengan keadaan seperti data pengguna atau orang. Komisaris wajib menyediakan pendapatnya dalam waktu tiga puluh hari sejak tanggal diterimanya permohonan yang dibuat. Komisaris wajib, ketika membuat pendapatnya dalam ayat (5), memperhitungkan pendapat yang relevan sebelumnya, jika ada. Komisaris dapat menarik pendapat yang dibuatnya jika Komisaris dipekerjakan oleh pengguna data telah berubah secara material.

Revocation, etc., of code of practice

26. (1) *The Commissioner may revoke, amend or revise, whether in whole or in part, any code of practice registered under this Act—*

(a) on his own accord; or

(b) upon an application by the data user forum or such bodies representing the data users.

(2) *The Commissioner shall, before revoking, amending or revising a code of practice under subsection (1), consult with—*

(a) such data users or bodies representative of data users to which the code of practice shall apply, whether in whole or in part; and

(b) such other interested persons, as the Commissioner thinks fit.

(3) *Where any code of practice has been revoked, amended or revised under subsection (1), the Commissioner—*

(a) shall enter the particulars of such revocation, amendment or revision in the Register of Codes of Practice; and

(b) shall notify the relevant data user forum, class of data users, data users and the public of such revocation, amendment or revision in such manner as may be determined by him.

(4) *The Commissioner shall make available to the public any code of practice as amended or revised by him under this section.*²⁶⁸

Komisaris dapat mencabut kode etik mengubah atau merevisi, baik secara keseluruhan atau sebagian, kode etik terdaftar di bawah

ACT baik karena kebijakan komisariss atau setelah adanya aplikasi dengan forum pengguna data atau badan yang mewakili pengguna data. Sebelum mencabut, mengubah atau merevisi Komisariss wajib, berkonsultasi dengan pengguna atau badan data seperti perwakilan dari pengguna data yang memberlakukan kode etik, baik secara keseluruhan atau sebagian. Bila mana kode etik telah dicabut, diubah atau direvisi dalam ayat (1), Komisariss wajib memberitahukan forum data pengguna yang relevan, kelas pengguna data, pengguna data dan masyarakat pencabutan tersebut, perubahan atau revisi dengan cara yang telah ditentukan.

Submission of new code of practice by data user forum

27. (1) *A data user forum may submit a new code of practice to replace an existing code of practice.*

(2) *The new code of practice submitted in pursuance of subsection (1) shall be subject to the provisions of this Division.*

Penyampaian kode etik baru oleh forum pengguna data menjelaskan bahwa forum pengguna data dapat mengajukan kode etik baru untuk menggantikan kode etik yang sudah ada. Kode etik baru dapat diajukan sesuai dengan ayat (1) harus tunduk pada ketentuan Divisi ini.

Register of Codes of Practice

28. (1) *The Commissioner shall maintain a Register of Codes of Practice in accordance with section 128.*

(2) *The Register of Codes of Practice shall contain—*

(a) *particulars of codes of practice registered under section 23 or 24 and any revocation, amendment or revision to such codes of practice under section 26; and Personal Data Protection 31*

(b) *any opinion made by the Commissioner under section 25, including particulars of withdrawal of previous opinions.*

Pada nomor 28 berisi tentang kewajiban komisariss untuk memelihara daftar kode etik sesuai dengan bagian 128. Pendaftaran tersebut berisi mengenai keterangan dari kode etik terdaftar mengenai *commit to user*

pencabutan, perubahan dan revisi serta perlindungan data pribadi serta setiap pendapat yang dibuat oleh Komisaris di bagian 25 termasuk keterangan penarikan sebelumnya.

Non-compliance with code of practice

29. A data user who fails to comply with any provision of the code of practice that is applicable to the data user commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both.

Ketidakpatuhan dengan kode etik diatur dalam nomor 29 yang menjelaskan bahwa pengguna data yang gagal untuk mematuhi ketentuan kode etik yang diterapkan untuk pengguna data dan melakukan pelanggaran dikenakan denda tidak melebihi seratus ribu ringgit atau penjara untuk jangka waktu tidak melebihi satu tahun atau keduanya.

*Division 4
Rights of data subject*

Right of access to personal data

- 30. (1) An individual is entitled to be informed by a data user whether personal data of which that individual is the data subject is being processed by or on behalf of the data user.*
- (2) A requestor may, upon payment of a prescribed fee, make a data access request in writing to the data user—*
- (a) for information of the data subject's personal data that is being processed by or on behalf of the data user; and*
 - (b) to have communicated to him a copy of the personal data in an intelligible form.*
- (3) A data access request for any information under subsection (2) shall be treated as a single request, and a data access request for information under paragraph (2)(a) shall, in the absence of any indication to the contrary, be treated as extending also to such request under paragraph (2)(b).*
- (4) In the case of a data user having separate entries in respect of personal data held for different purposes, a separate data access request shall be made for each separate entry.*

(5) *Where a data user does not hold the personal data, but controls the processing of the personal data in such a way as to prohibit the data user who holds the personal data from complying, whether in whole or part, with the data access request under subsection (2) which relates to the personal data, the firstmentioned data user shall be deemed to hold the personal data and the provisions of this Act shall be construed accordingly.*²⁶⁹

Hak subjek data diatur dalam Divisi 4. Pada Divisi ini diatur ketentuan mengenai hak akses ke data pribadi dimana seorang individu berhak untuk diberitahu oleh data pengguna apakah data pribadi dari mana individu yang menjadi subjek data yang sedang diproses oleh atau atas nama pengguna data. Pemohon mungkin, atas pembayaran biaya yang ditentukan, membuat permintaan akses data tertulis kepada pengguna data atas informasi data pribadi subyek data yang sedang diproses oleh atau atas nama pengguna data; dan telah disampaikan kepadanya salinan data pribadi dalam bentuk yang dimengerti. Dalam hal pengguna data yang memiliki tujuan berbeda harus memiliki entri terpisah sehubungan data pribadi. Pengguna data pribadi dimungkinkan tidak memegang data pribadi namun hanya mengontrol pengolahan data pribadi, larangan berlaku sama dengan pengguna data yang memegang data pribadi serta diwajibkan mematuhi, baik secara keseluruhan atau sebagian, permintaan akses data yang berkaitan dengan data pribadi.

Compliance with data access request

31. (1) *Subject to subsection (2) and section 32, a data user shall comply with a data access request under section 30 not later than twenty-one days from the date of receipt of the data access request.*
- (2) *A data user who is unable to comply with a data access request within the period specified in subsection (1) shall before the expiration of that period—*

²⁶⁹ *Ibid.*

- (a) *by notice in writing inform the requestor that he is unable to comply with the data access request within such period and the reasons why he is unable to do so; and*
- (b) *comply with the data access request to the extent that he is able to do so.*
- (3) *Notwithstanding subsection (2), the data user shall comply in whole with the data access request not later than fourteen days after the expiration of the period stipulated in subsection (1).*

Pengguna data harus memenuhi permintaan akses data di bawah bagian 30 tidak lebih dari dua puluh satu hari sejak tanggal diterimanya permintaan akses data. Seorang pengguna Data yang tidak dapat memenuhi permintaan akses data dalam jangka waktu yang ditentukan dalam ayat (1) wajib sebelum berakhirnya periode yang dengan pemberitahuan secara tertulis menginformasikan pemohon bahwa ia tidak dapat memenuhi permintaan akses data dalam jangka waktu tersebut dan alasan mengapa ia tidak mampu melakukannya; dan berusaha memenuhi permintaan akses data sampai ia mampu melakukannya. Pengguna harus memenuhi secara keseluruhan dengan permintaan akses data paling lambat empat belas hari setelah berakhirnya jangka waktu yang ditetapkan dalam ayat (1).

Circumstances where data user may refuse to comply with data access request

32. (1) *A data user may refuse to comply with a data access request under section 30 if—*
- (a) *the data user is not supplied with such information as he may reasonably require—*
 - (i) *in order to satisfy himself as to the identity of the requestor; or*
 - (ii) *where the requestor claims to be a relevant person, in order to satisfy himself—*
 - (A) *as to the identity of the data subject in relation to whom the requestor claims to be the relevant person; and Personal Data Protection 33*
 - (B) *that the requestor is the relevant person in relation to the data subject;*

- (b) *the data user is not supplied with such information as he may reasonably require to locate the personal data to which the data access request relates;*
- (c) *the burden or expense of providing access is disproportionate to the risks to the data subject's privacy in relation to the personal data in the case in question;*
- (d) *the data user cannot comply with the data access request without disclosing personal data relating to another individual who can be identified from that information, unless—*
 - (i) *that other individual has consented to the disclosure of the information to the requestor; or*
 - (ii) *it is reasonable in all the circumstances to comply with the data access request without the consent of the other individual;*
- (e) *subject to subsection (3), any other data user controls the processing of the personal data to which the data access request relates in such a way as to prohibit the first-mentioned data user from complying, whether in whole or in part, with the data access request;*
- (f) *providing access would constitute a violation of an order of a court;*
- (g) *providing access would disclose confidential commercial information; or*
- (h) *such access to personal data is regulated by another law.*²⁷⁰

Pengguna data dapat menolak untuk memenuhi permintaan akses data jika tidak memberikan cukup informasi mengenai pengguna data yang dimaksud serta tidak memenuhi syarat identitas pemohon; atau pemohon mengklaim menjadi orang yang relevan, dalam rangka untuk memenuhi identitas subjek data, beban atau biaya penyediaan akses tidak sebanding dengan risiko privasi subyek data dalam kaitannya dengan data pribadi dalam kasus tersebut; Pengguna data tidak dapat memenuhi permintaan akses data tanpa mengungkapkan data pribadi yang berhubungan dengan individu lain yang dapat diidentifikasi dari informasi itu, kecuali- bahwa individu

²⁷⁰ Law of Malaysia, Act 79, *Personal Data Act*, 2010

lain telah menyetujui untuk pengungkapan informasi kepada pemohon. Penolakan dianggap dalam semua keadaan untuk memenuhi permintaan akses data tanpa persetujuan dari individu lain; menyediakan akses merupakan pelanggaran perintah pengadilan; menyediakan akses akan mengungkapkan informasi rahasia komersial; atau akses tersebut ke data pribadi diatur oleh hukum lain.

- (2) *In determining for the purposes of subparagraph (1)(d)(ii) whether it is reasonable in all the circumstances to comply with the data access request without the consent of the other individual, regard shall be had, in particular, to—*
- (a) any duty of confidentiality owed to the other individual;*
 - (b) any steps taken by the data user with a view to seeking the consent of the other individual;*
 - (c) whether the other individual is capable of giving consent;*
 - and*
 - (d) any express refusal of consent by the other individual.*
- (3) *Paragraph (1)(e) shall not operate so as to excuse the data user from complying with the data access request under subsection 30(2) to any extent that the data user can comply with the data access request without contravening the prohibition concerned.²⁷¹*

Kewajaran yang dimaksud untuk memenuhi permintaan akses data tanpa persetujuan dari individu lain, adalah bahwa setiap kewajiban kerahasiaan tergantung kepada individu lain; langkah-langkah yang diambil oleh pengguna data dengan maksud untuk mencari persetujuan dari individu lain; apakah individu lain yang mampu memberikan persetujuan; dan menolak untuk membuat persetujuan dengan individu lain.

Notification of refusal to comply with data access request

33. *Where a data user who pursuant to section 32 refuses to comply with a data access request under section 30, he shall, not later than twenty-one days from the date of receipt of the data access request, by notice in writing, inform the requestor—*

²⁷¹ *Ibid.*

- (a) of the refusal and the reasons for the refusal; and*
- (b) where paragraph 32(1)(e) is applicable, of the name and address of the other data user concerned.*

Apabila pengguna data seperti yang tertuang dalam nomor 32 menolak untuk mematuhi permintaan akses data seperti yang disebutkan nomor 30, paling lambat dua puluh satu hari sejak tanggal diterimanya permintaan akses data, dengan pemberitahuan secara tertulis, menginformasikan alasan penolakan; dan berlaku, nama dan alamat pengguna data lainnya yang bersangkutan.

Right to correct personal data

34. (1) Where—

- (a) a copy of the personal data has been supplied by the data user in compliance with the data access request under section 30 and the requestor considers that the personal data is inaccurate, incomplete, misleading or not up-to-date; or*
 - (b) the data subject knows that his personal data being held by the data user is inaccurate, incomplete, misleading or not up-to-date, the requestor or data subject, as the case may be, may make a data correction request in writing to the data user that the data user makes the necessary correction to the personal data.*
- (2) Where a data user does not hold the personal data, but controls the processing of the personal data in such a way as to prohibit the data user who holds the personal data from complying, whether in whole or in part, with the data correction request under subsection (1) which relates to the personal data, the first-mentioned data user shall be deemed to be the data user to whom such a request may be made and the provisions of this Act shall be construed accordingly.²⁷²*

Hak untuk mengoreksi isi data pribadi dituangkan dalam nomor 34 yang menyebutkan bahwa salinan data pribadi yang telah disediakan oleh data pengguna sesuai dengan permintaan akses data di bawah bagian 30 dan pemohon menganggap bahwa data pribadi tidak

²⁷² *Ibid.*

akurat, tidak lengkap, menyesatkan atau tidak *up-to-date*. Subjek data yang tahu bahwa data pribadi yang digunakan oleh pengguna data tidak akurat, tidak lengkap, menyesatkan atau tidak *up-to-date*, pemohon atau subjek data, dimungkinkan membuat permintaan koreksi data dalam bentuk tertulis kepada pengguna data yang data pengguna membuat koreksi yang diperlukan untuk data pribadi. Apabila pengguna data tidak memegang data pribadi, tetapi mengontrol pengolahan data pribadi sedemikian rupa untuk melarang pengguna data yang memegang data pribadi untuk mematuhi, baik secara keseluruhan atau sebagian, dengan permintaan koreksi berkaitan dengan data pribadi, data pengguna yang disebut pertama akan dianggap sebagai data pengguna kepada siapa permintaan seperti itu dapat dibuat dan ketentuan Undang-undang ini akan ditafsirkan sesuai.

Compliance with data correction request

35. (1) *Subject to subsections (2), (3) and (5) and section 36, where a data user is satisfied that the personal data to which a data correction request relates is inaccurate, incomplete, misleading or not up-to-date, he shall, not later than twenty-one days from the date of receipt of the data correction request—*

- (a) make the necessary correction to the personal data;*
- (b) supply the requestor with a copy of the personal data as corrected; and*

(c) subject to subsection (4), where—

- (i) the personal data has been disclosed to a third party during the twelve months immediately preceding the day on which the correction is made; and*

- (ii) the data user has no reason to believe that the third party has ceased using the personal data for the purpose, including any directly related purpose, for which the personal data was disclosed to the third party, take all practicable steps to supply the third party with a copy of the personal data as so corrected accompanied by a*

commit to user

*notice in writing stating the reasons for the correction.*²⁷³

Permintaan koreksi data yang berhubungan tidak akurat, tidak lengkap, menyesatkan atau tidak *up- to-date*, ia harus, paling lambat dua puluh satu hari sejak tanggal diterimanya permintaan-koreksi data yang diperlukan untuk data pribadi; menyediakan pemohon dengan salinan data pribadi dikoreksi; dan data pribadi yang telah diungkapkan kepada pihak ketiga selama dua belas bulan segera sebelum hari di mana koreksi dibuat; dan pengguna data tidak memiliki alasan untuk percaya bahwa pihak ketiga telah berhenti menggunakan data pribadi untuk tujuan tersebut, termasuk tujuan langsung terkait, dimana data pribadi itu diungkapkan kepada pihak ketiga, mengambil semua langkah praktis untuk mengganti data pribadi pada pihak ketiga dengan salinan data pribadi disertai koreksi dengan pemberitahuan tertulis yang menyatakan alasan untuk koreksi.

- (2) *A data user who is unable to comply with a data correction request within the period specified in subsection (1) shall before the expiration of that period—*
 - (a) *by notice in writing inform the requestor that he is unable to comply with the data correction request within such period and the reasons why he is unable to do so; and*
 - (b) *comply with the data correction request to the extent that he is able to do so.*
- (3) *Notwithstanding subsection (2), the data user shall comply in whole with the data correction request not later than fourteen days after the expiration of the period stipulated in subsection (1).*
- (4) *A data user is not required to comply with paragraph (1)(c) in any case where the disclosure of the personal data to a third party consists of the third party's own inspection of a register—*

²⁷³ Law of Malaysia, Act 79, *Personal Data Act*, 2010

- (a) in which the personal data is entered or otherwise recorded; and*
- (b) which is available for inspection by the public.*

Seorang pengguna data yang tidak dapat memenuhi permintaan koreksi data dalam periode yang ditentukan dalam ayat (1) wajib sebelum berakhirnya periode penggunaan data pribadi membuat pemberitahuan secara tertulis menginformasikan pemohon bahwa ia tidak dapat memenuhi permintaan koreksi data dalam periode tersebut dan alasan mengapa ia tidak mampu melakukannya; dan memenuhi permintaan koreksi data yang sejauh bahwa ia mampu melakukannya. Penyimpangan terhadap ayat (2), pengguna data harus memenuhi secara keseluruhan dengan permintaan koreksi data yang paling lambat empat belas hari setelah berakhirnya jangka waktu yang ditetapkan dalam ayat (1). Seorang pengguna data tidak diwajibkan untuk memenuhi ayat (1) (c) dalam hal apapun di mana pengungkapan data pribadi kepada pihak ketiga terdiri dari pemeriksaan pihak ketiga sendiri dari dalam mendaftarkan sebuah data pribadi yang dimasukkan atau dicatat; dan yang tersedia untuk diperiksa oleh publik.

Withdrawal of consent to process personal data

38. (1) *A data subject may by notice in writing withdraw his consent to the processing of personal data in respect of which he is the data subject.*
- (2) *The data user shall, upon receiving the notice under subsection (1), cease the processing of the personal data.*
- (3) *The failure of the data subject to exercise the right conferred by subsection (1) does not affect any other rights conferred on him by this Part.*
- (4) *A data user who contravenes subsection (2) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both.*²⁷⁴

commit to user

²⁷⁴ Law of Malaysia, Act 79, Personal Data Act, 2010

Subjek data dengan pemberitahuan tertulis dapat menarik persetujuan untuk pengolahan data pribadi dalam hal yang ia adalah subjek data. Pengguna data yang telah menerima pemberitahuan dalam ayat (1), harus menghentikan pengolahan data pribadi. Kegagalan subjek data yang menggunakan hak yang diberikan oleh ayat (1) tidak mempengaruhi hak-hak lain yang diberikan kepadanya oleh Bagian ini. Seorang pengguna Data yang bertentangan ayat (2) melakukan pelanggaran dikenakan denda tidak melebihi seratus ribu ringgit atau penjara untuk jangka waktu tidak melebihi satu tahun atau keduanya.

Extent of disclosure of personal data

39. *Notwithstanding section 8, personal data of a data subject may be disclosed by a data user for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection or any other purpose directly related to that purpose, only under the following circumstances:*

- (a) the data subject has given his consent to the disclosure;*
- (b) the disclosure —*
 - (i) is necessary for purpose of preventing or detecting a crime, or for the purpose of investigations; or*
 - (ii) was required or authorized by or under any law or by the order of a court;*
- (c) the data user acted in the reasonable belief that he had in law the right to disclose the personal data to the other person;*
- (d) the data user acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or*
- (e) the disclosure was justified as being in the public interest in circumstances as determined by the Minister.*

Berdasarkan kutipan tersebut diatas, pada nomor 39 dijelaskan mengenai Tingkat pengungkapan data pribadi. Pengungkapan data pribadi dapat dilakukan apabila subjek data telah memberikan persetujuannya untuk pengungkapan; pengungkapan diperlukan untuk tujuan mencegah atau mendeteksi kejahatan, atau untuk tujuan *commit to user* investigasi; atau diizinkan oleh undang-undang atau atas perintah

pengadilan; pengguna data dapat bertindak wajar bahwa ia memiliki hak secara hukum untuk mengungkapkan data pribadi kepada orang lain; pengguna data memiliki persetujuan dari subjek data jika subjek data yang telah diketahui dari penyajian data pribadi dan keadaan pengungkapan tersebut; atau pengungkapan itu dibenarkan sebagai kepentingan umum dalam keadaan yang ditetapkan oleh Menteri.

Processing of sensitive personal data

40. (1) *Subject to subsection (2) and section 5, a data user shall not process any sensitive personal data of a data subject except in accordance with the following conditions:*

(a) the data subject has given his explicit consent to the processing of the personal data;

(b) the processing is necessary—

(i) for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data user in connection with employment;

(ii) in order to protect the vital interests of the data subject or another person, in a case where—

(A) consent cannot be given by or on behalf of the data subject; or

(B) the data user cannot reasonably be expected to obtain the consent of the data subject;

(iii) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;

(iv) for medical purposes and is undertaken by—

(A) a healthcare professional; or

(B) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;

(v) for the purpose of, or in connection with, any legal proceedings;

(vi) for the purpose of obtaining legal advice;

(vii) for the purposes of establishing, exercising or defending legal rights;

(viii) for the administration of justice;

(ix) for the exercise of any functions conferred on any person by or under any written law; or²⁷⁵

commit to user

²⁷⁵ Law of Malaysia, Act 79, Personal Data Act, 2010

- (x) for any other purposes as the Minister thinks fit;
or
(c) the information contained in the personal data has
been made public as a result of steps deliberately
taken by the data subject.*

Pengolahan data pribadi yang sensitif tidak akan diolah oleh pengguna data kecuali sesuai dengan ketentuan sebagai berikut: subyek data telah memberikan persetujuan eksplisit untuk pengolahan data pribadi, proses yang diperlukan untuk melakukan hak atau kewajiban yang diberikan atau dikenakan oleh hukum pada data pengguna sehubungan dengan pekerjaan; untuk melindungi kepentingan vital subyek data atau orang lain, persetujuan tidak dapat diberikan oleh atau atas nama subjek data; atau pengguna data dapat tidak diperkirakan mungkin mendapatkan persetujuan dari subyek data; untuk melindungi kepentingan vital orang lain, untuk tujuan medis dan dilakukan oleh- profesional kesehatan; untuk tujuan, atau sehubungan dengan, setiap proses hukum; untuk tujuan memperoleh nasihat hukum; untuk tujuan membangun, berolahraga atau membela hak-hak hukum; untuk administrasi peradilan; untuk pelaksanaan fungsi-fungsi yang diberikan pada setiap orang dengan atau berdasarkan hukum tertulis.

Right to prevent processing likely to cause damage or distress

42. (1) *Subject to subsection (2), a data subject may, at any time by notice in writing to a data user, referred to as the “data subject notice”, require the data user at the end of such period as is reasonable in the circumstances, to—*
- (a) cease the processing of or processing for a specified purpose or in a specified manner; or*
 - (b) not begin the processing of or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject if, based on reasons to be stated by him—*

- (A) *the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another person; and*
- (B) *the damage or distress is or would be unwarranted.*²⁷⁶

Hak untuk mencegah pengolahan mungkin menyebabkan kerusakan atau tekanan dapat dilakukan dengan pemberitahuan tertulis kepada pengguna data, disebut sebagai "Data pemberitahuan", memerlukan pengguna data pada akhir periode seperti adalah wajar dalam situasi, menghentikan pengolahan atau pemrosesan untuk tujuan tertentu atau dengan cara tertentu; atau tidak memulai pengolahan atau pemrosesan untuk tujuan tertentu atau dengan cara tertentu, data pribadi sehubungan mana ia merupakan subjek data jika, berdasarkan alasan yang akan dikemukakan oleh subjek data bahwa pengolahan data pribadi atau pengolahan data pribadi untuk tujuan itu atau dengan cara yang menyebabkan atau mungkin menyebabkan kerusakan besar atau tekanan yang cukup besar untuk subjek data atau untuk orang lain.

- (2) *Subsection (1) shall not apply where—*
 - (a) *the data subject has given his consent;*
 - (b) *the processing of personal data is necessary—*
 - (i) *for the performance of a contract to which the data subject is a party;*
 - (ii) *for the taking of steps at the request of the data subject with a view to entering a contract;*
 - (iii) *for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by contract; or*
 - (iv) *in order to protect the vital interests of the data subject; or*
 - (c) *in such other cases as may be prescribed by the Minister by order published in the Gazette.*

²⁷⁶ *ibid*

Pencegahan pengolahan data tidak berlaku manakala subyek data telah memberikan persetujuannya untuk pengolahan data pribadi yang diperlukan untuk kinerja kontrak dengan berbagai pihak. Untuk mengambil langkah-langkah atas permintaan dari subyek data dengan maksud untuk memasuki kontrak; untuk memenuhi kewajiban hukum yang pengguna data subjek, selain kewajiban yang dikenakan oleh kontrak; atau untuk melindungi kepentingan vital subjek data; atau dalam kasus lain seperti dapat ditentukan oleh Menteri atas perintah yang diumumkan dalam Berita.

(3) The data user shall, within twenty-one days from the date of receipt of the data subject notice under subsection (1), give the data subject a written notice—

(a) stating that he has complied or intends to comply with the data subject notice; or

(b) stating his reasons for regarding the data subject notice as unjustified, or to any extent unjustified, and the extent, if any, to which he has complied or intends to comply with it.

(4) Where the data subject is dissatisfied with the failure of the data user to comply with the data subject notice, whether in whole or in part, under paragraph (3)(b), the data subject may submit an application to the Commissioner to require the data user to comply with the data subject notice.²⁷⁷

Pengguna data dalam waktu dua puluh satu hari sejak tanggal diterimanya pemberitahuan maka pengguna data wajib memberikan subjek data pemberitahuan tertulis yang menyatakan bahwa ia telah memenuhi atau bermaksud untuk mematuhi pemberitahuan data; atau yang menyatakan alasannya mengenai pemberitahuan data dibenarkan, sampai batas tertentu dan sejauh, jika ada yang telah ia penuhi. Dimana subjek data yang tidak puas dengan kegagalan pengguna data untuk mematuhi pemberitahuan data, baik secara

²⁷⁷ Law of Malaysia, Act 79, *Personal Data Act*, 2010

keseluruhan atau sebagian, subjek data dapat mengajukan permohonan kepada Komisaris untuk meminta data pengguna untuk mematuhi pemberitahuan data.

Right to prevent processing for purposes of direct marketing

43. (1) *A data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing.*
- (2) *Where the data subject is dissatisfied with the failure of the data user to comply with the notice, whether in whole or in part, under subsection (1), the data subject may submit an application to the Commissioner to require the data user to comply with the notice.*
- (3) *Where the Commissioner is satisfied that the application of the data subject under subsection (2) is justified or justified to any extent, the Commissioner may require the data user to take such steps for complying with the notice.*
- (4) *A data user who fails to comply with the requirement of the Commissioner under subsection (3) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.*
- (5) *For the purposes of this section, "direct marketing" means the communication by whatever means of any advertising or marketing material which is directed to particular individuals.*²⁷⁸

Berdasarkan kutipan diatas, pada nomor 43 menjelaskan tentang Hak untuk mencegah pemrosesan untuk tujuan pemasaran langsung. Subjek data mungkin, setiap saat dapat membuat pemberitahuan tertulis kepada pengguna data, untuk berhenti atau tidak untuk mengolah data pribadinya untuk tujuan pemasaran langsung. Apabila subjek data yang tidak puas dengan pengguna data untuk mematuhi pemberitahuan, baik secara keseluruhan atau sebagian, subjek data yang dapat mengajukan permohonan kepada Komisaris untuk

²⁷⁸ Law of Malaysia, Act 79, *Personal Data Act*, 2010

meminta pengguna data mematuhi pemberitahuan. Dalam hal Komisaris mengetahui bahwa aplikasi dari subyek data dalam ayat (2) adalah dibenarkan atau dibenarkan sampai batas tertentu, Komisaris dapat mengambil langkah-langkah terhadap pengguna data untuk mematuhi pemberitahuan. Pengguna data yang tidak memenuhi persyaratan Komisaris dalam ayat (3) melakukan pelanggaran dan harus, dikenakan denda tidak melebihi dua ratus ribu ringgit atau penjara untuk jangka waktu tidak melebihi dua tahun atau keduanya. Untuk keperluan bagian ini, "pemasaran langsung" berarti komunikasi dengan cara apapun dari setiap iklan atau pemasaran bahan yang diarahkan kepada individu tertentu.

Record to be kept by data user

44. (1) *A data user shall keep and maintain a record of any application, notice, request or any other information relating to personal data that has been or is being processed by him.*

(2) *The Commissioner may determine the manner and form in which the record is to be maintained.*

Rekaman yang disimpan oleh pengguna data harus dijaga dan dipelihara menggunakan catatan aplikasi melalui pemberitahuan, permintaan atau informasi lain yang berkaitan dengan data pribadi yang telah atau sedang diproses oleh pengguna data. Komisaris dapat menentukan cara dan bentuk yang catatan harus disimpan.

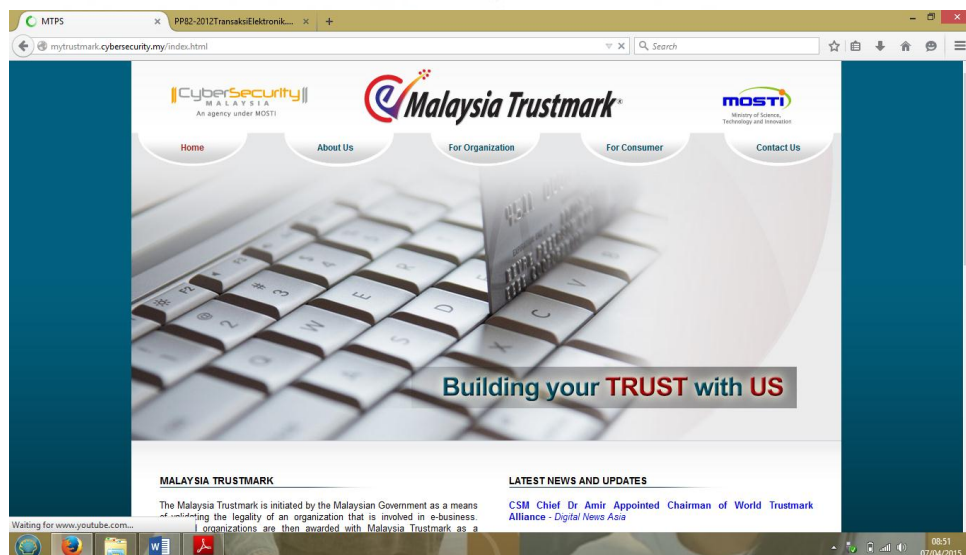
2). Display Malaysia Trustmark

Tahun 2013 *CyberSecurity Malaysia* memperkenalkan Malaysia Trustmark yaitu program khusus menentukan keabsahan bisnis online untuk memerangi penipuan internet, sekaligus meningkatkan kepercayaan pelanggan. Program itu adalah mekanisme bagi pelanggan untuk menilai dan memverifikasi badan e-bisnis tertentu sebelum melakukan transaksi online. Peluncuran Malaysia Trustmark, juga salah satu inisiatif pemerintah untuk meningkatkan kepercayaan rakyat

terhadap e-bisnis.²⁷⁹ Logo Malaysia *Trustmark* yang didisplay dalam *website* adalah sebagai berikut:



Gambar 29 *Trustmark* Malaysia



Gambar 30 Organisasi Malaysia *Trustmark*

3). Jaminan yang diberikan Malaysia *Trustmark* terhadap pelaku usaha dan Konsumen

Jaminan yang diberikan Malaysia *Trustmark* terhadap pelaku usaha dan konsumen di Malaysia meliputi:

- a). Akurasi dan Aksesibilitas Informasi yang terdiri dari Informasi Pemasaran, Informasi organisasi, informasi Barang / Jasa Informasi, Informasi Transaksi, Informasi Garansi atau jaminan.
- b). Pelaksanaan E-Bisnis berlaku untuk Organisasi yang meliputi pembatalan / pengembalian, komunikasi baik melalui Email maupun email Komersial (SPAM) dan *Consumer Care*.

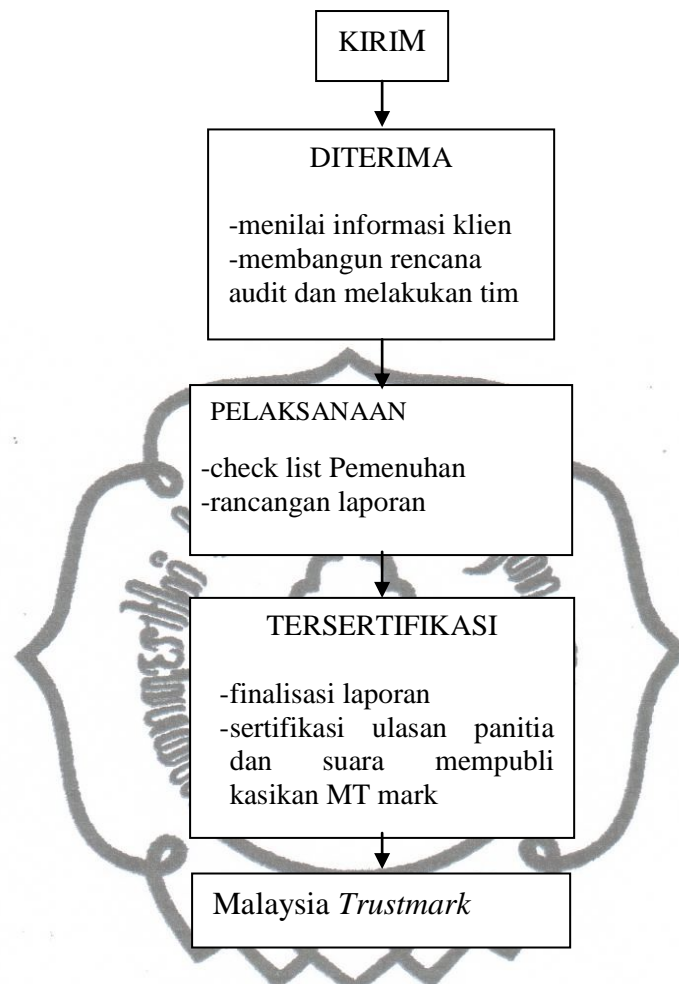
²⁷⁹Dodo, CyberSecurity Luncurkan Malaysia Trustmark, <http://www.batamtoday.com/berita30283-CyberSecurity-Luncurkan-Malaysia-Trustmark.html>. Diakses 7 April 2015 Jam 08.13 WIB *commit to user*

- c). Keamanan yang berupa keamanan informasi data konsumen dan transaksi elektronik.
- d). Prinsip Perlindungan Data Privacy yang terdiri dari Prinsip umum, Prinsip Keterbukaan, prinsip retensi, prinsip keamanan, Integritas Data, dan akses.
- e). Alternatif Penyelesaian Sengketa yang terdiri dari Pengaduan konsumen dan Penyelesaian Sengketa Manajemen. Resolusi keluhan internal Pemberitahuan mengenai pengajuan sengketa ke sistem ADR, Biaya sistem ADR

Jaminan yang diberikan Malaysia *Trustmark* tersebut merupakan ringkasan dari regulasi yang dibuat *Asia-Pacific Trustmark Alliance* (ATA), Pedoman *Trustmark* Operator (G | T | O) versi 1.0, Personal Data *Protection Act* 2010 dari Jabatan Perlindungan data Pribadi Malaysia

4). Bagan Alir permohonan Malaysia *Trustmark*

Prosedur pengajuan sertifikasi Malaysia *Trustmark* dilakukan dengan cara sebagai berikut:



Proses sertifikasi Malaysia *Trustmark* secara *Online*

Bagan 4. Proses Permohonan Malaysia *Trustmark*

Berdasarkan paparan diatas, kepercayaan pada dasarnya berbanding lurus dengan pengetahuan akan resiko serta sejauhmana pengaturan manajemen resiko tersebut sehingga transaksi elektronik atau *e commerce* layak dipercaya pelaku usaha, masyarakat dan pemerintah. Tingkat layanan kepercayaan sangat tergantung kepada sebuah prosedur dan *quality assurance level* di jalankan.

C. Perbandingan Negara Singapura, Malaysia dan Indonesia dalam meningkatkan keterpercayaan dalam Bisnis *E Commerce*

Kemajuan Pesat di bidang ICT (*Information and Communication Technology*) melahirkan masyarakat informasi dalam dunia maya yang disebut komunitas virtual. Salah satu yang meresap sebagian besar jenis komunitas virtual mencakup layanan jaringan sosial, yang terdiri dari berbagai komunitas *online*. *Internet* sejak pertengahan 1990-an juga telah menumbuhkan perkembangan masyarakat virtual mengambil bentuk layanan jaringan sosial dan komunitas *online*. Di dalam suatu komunitas virtual hubungan sosial disebut Interaksi *online* merupakan efektif sebuah penggabungan dari email, *chatting* dan bentuk komunikasi publik (diskusi forum dan *newsgroup*). Komunitas *online* dapat dikatakan bila cukup banyak orang melakukan diskusi publik yang cukup lama, dengan perasaan manusia yang memadai untuk membentuk *web* dari hubungan pribadi²⁸⁰

Tidak mudah untuk meningkatkan penggunaan *e commerce* di Indonesia. Banyak faktor yang mempengaruhi kepercayaan konsumen untuk menggunakan *e commerce* salah satunya adalah nilai-nilai keluarga atas kehidupan ekonomi yang dapat memberikan gambaran yang kompleks dan kontradiktif. Dalam pelaksanaan *e commerce*, sistem pembayaran secara elektronik menjadi hal yang penting. Keberhasilan *e commerce* tidak lepas dari penerimaan masyarakat atas penggunaan sistem pembayaran secara elektronik baik dengan transfer, kartu debit maupun kartu kredit atau fasilitas perbankan yang lain. Pemahaman masyarakat serta kemudahan atas beban biaya dan penggunaan pembayaran menggunakan sistem elektronik setelah melaksanakan transaksi *online* dalam *e commerce* juga menjadi salah satu pertimbangan

²⁸⁰Devon Ariell Yulianto, Hubungan Sosial dalam Transaksi Ekonomi Pada Komunitas Virtual Pecinta Ikan Hias (Study Deskriptif tentang Proses Pengembangan Kepercayaan antar Anggota dalam Proses Transaksi Jual Beli Ikan Hias pada Komunitas Virtual Pecinta Ikan O-Fish Forum), Departemen Ilmu Informasi dan Perpustakaan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Airlangga, <http://journal.unair.ac.id/filesPDF/Inec2f77f56bfull.pdf>. Diakses pada 8 April 2015 Jam 01.52 WIB.

pengguna atau user dalam *e commerce*.²⁸¹ Kesejahteraan sebuah negara, seperti kemampuannya untuk bersaing dengan negara lain, ditentukan oleh karakteristik budaya yang melekat dalam masyarakat. Karakteristik budaya yang melekat inheren dalam masyarakat ini adalah *trust*.²⁸²

Berdasarkan hasil penelitian yang telah penulis lakukan di Indonesia muncul organisasi maupun lembaga swasta yang melakukan sertifikasi kepada *website*. Sebagai contoh *website* yang kegiatannya memberikan informasi kepada konsumen pengguna *e commerce* mengenai tindak kejahatan di dunia maya *website* tersebut www.polisionline.com. Berdasarkan hasil penelitian yang telah penulis lakukan pada *website polisionline* tersebut dijelaskan bahwa visi *polisionline.com* adalah mencegah tindak kejahatan yang berupa kasus penipuan online dan masyarakat mengerti mana toko yang benar-benar menjual produk dan mana toko online yang bersifat fiktif atau penipu. Misi *polisionline.com* adalah memberikan informasi dan meminimalisir tindak kejahatan di dunia maya berupa penipuan online yang dilakukan toko online fiktif. *Polisionline.com* akan memonitor dan memberikan informasi situs-situs yang dicurigai pelaku penipuan online toko online baik melalui *website*, facebook maupun laman yang lainnya.²⁸³

Berdasarkan informasi yang telah penulis peroleh dari *website* tersebut dijelaskan bahwa,

“untuk memasang *widget* *polisionline.com* kami memberikan 2 opsi yaitu standart atau gratis dan premium atau berbayar dengan syarat yang sudah kami tentukan”

Website tersebut juga sudah membentengi jawaban atas pertanyaan mengenai alamat kantor *polisionline.com*,

“Maaf kami tidak bisa menjawab ini untuk keamanan kami. Situs kami boleh dilihat untuk umum namun kami berhak mengubah layanan dan sega isi sesuai denganketentuan yang kami punya. Semua komentar yang

²⁸¹Dennish Abrazhevich, Importance of User-Related Factors in Electronic Payment Systems. Trust in Electronic Commerce, The Role of Trust from a Legal an Organizational and Technical Point of View. Kluwer Law International. The Hague/London/ New York. hlm. 83

²⁸²Fukuyama. F. *Trust: The Social Virtues and the Creation of Prosperity*. Free Press. New York, 1995. hlm. 197

²⁸³Tentang Kami, www.polisionline.com diakses 24 Februari 2016 jam 10.50 WIB

tampil disetiap review dapat dilihat oleh pengunjung lain tanpa harus login terlebih dahulu dan kami berhak merubah atau menghapus komentar tersebut tanpa sepengetahuan penulis komentar. Kami terus berupaya memberi informasi dengan meng update secara rutin dan kami berhak merubah atau mengembalikannya ke draft. Semua link dari situs kami bersifat aktif atau *do follow* yang bersifat informasi seputar toko *online* terpercaya maupun menipu. Kami tidak bertanggungjawab atas kerugian yang anda peroleh dari polisionline.com terkecuali dengan website yang menggunakan widget “terjamin” dari Polisionline.com”²⁸⁴

Logo *Trustmark* yang dibuat oleh polisionline.com adalah sebagai berikut,



Gambar 30. *Trustmark* Polisionline

Lebih lanjut polisionline.com memberikan jaminan kepada *website* untuk diverifikasi dengan memberikan keterangan bahwa toko *online* terpercaya 100%, namun *website* ini membuka peluang untuk melakukan klaim dengan menunjukkan bukti transaksi tanpa perantara dalam jangka waktu >1 bulan dari waktu pembelian. Lebih dari waktu yang ditentukan polisionline.com tidak bisa memberikan jaminan uang kembali dengan cara di transfer ke rekening selambat-lambatnya 30 hari kerja.

Selain polisionline.com, Asosiasi *E Commerce* Indonesia (IdEA) yang merupakan wadah komunikasi antar pelaku industri *e commerce* Indonesia juga memiliki Visi yaitu memberikan kontribusi terhadap perkembangan ekonomi dan pemerataan kekayaan Indonesia melalui *e commerce*, menjadikan fasilitas

²⁸⁴Syarat dan ketentuan toko online bisa terverifikasi di polisionline.com, terdapat dalam www.polisionline.com diakses pada 24 Februari 2016 Jam 12.18 WIB

e commerce tersedia bagi pengguna internet di Indonesia dan menjadikan Indonesia sebagai basis ekonomi digital terbesar di Asia Tenggara. Misi IdEA adalah melakukan kegiatan edukasi yang meluas tentang *e commerce*, melakukan kegiatan promosi yang menyeluruh tentang *e commerce*, mengembangkan sumber daya manusia dibidang *e commerce* dan mengembangkan teknologi yang superior yang dapat mendorong kesuksesan industri *e commerce*.

Dari hasil penelitian yang telah penulis lakukan, saat ini IdEA telah menyediakan *Trustmark* bagi *e commerce*. Proses memperoleh *Trustmark* relatif mudah yaitu hanya perlu mengikuti tahap-tahap registrasi dan verifikasi. Proses pertama pemiliknya mendaftarkan websitenya ke IdEA, kemudian akan ada sejumlah verifikasi yang dilakukan admin IdEA seperti KTP, NPWP. Setelah diverifikasi, pemilik situs akan mendapat konfirmasi melalui sms yang berisi 15 digit kode untuk melakukan pembayaran. Setelah pembayaran terverifikasi proses registrasi pun selesai. IdEA akan melakukan verifikasi secara berkala. Tiap minggu, sistem akan mengirim email berisi kode rahasia yang harus dikirim pemilik situs melalui sms 24 jam. Satu bulan sekali admin akan melakukan verifikasi situs dengan *screen capture* untuk memastikan situs tersebut masih aktif atau tidak. Selain itu admin IdEA akan memastikan apakah barang yang dibeli sesuai dengan spesifikasi produk dan waktu pengiriman.²⁸⁵

²⁸⁵David Alexander, Ini cara menangkal lapak online Abal-Abal, www.detik.com Diakses pada 24 Februari 2016 Jam 134.01 WIB



Gambar 31. IdEA Trustmark yang telah memverifikasi situs

Indonesia perlu segera memberlakukan *Trustmark* untuk transaksi *e commerce*. Pemerintah melalui Kementrian Kominfo masih melakukan pembenahan untuk meningkatkan iklim transaksi elektronik atau *e commerce* melalui pembuatan rancangan menteri tentang Lembaga Sertifikasi Keandalan. Saat ini beberapa kali melakukan revisi atas regulasi yang bertujuan untuk memberikan perlindungan bagi pengguna transaksi elektronik melalui *Regulation (EU) No. 910 / 2014 of The European Parliament and The Council of 23 July 2014 on electronic and trust services for electronic transactions in internal market repealing Directive 1999/93/EC* mengatur tentang *Trust Service* yang di dalamnya tidak hanya mengatur mengenai *Trustmark*.

Pada regulasi tersebut mengatur banyak hal yang bertujuan untuk membangun kepercayaan pengguna internet yang salah satunya mengenai *Trust Service*. *Trust Service* dalam regulasi ini berarti layanan elektronik yang disediakan untuk penciptaan, verifikasi dan validasi tanda tangan elektronik, segel elektronik, stempel waktu elektronik, pengiriman register elektronik dan sertifikat yang berhubungan dengan layanan, penciptaan, verifikasi dan sertifikat validasi untuk *autentikasi website*, pelestarian tanda tangan elektronik, sertifikasi segel yang sesuai dengan layanan elektronik. *Trust service* di bedakan menjadi *qualified trust service* dan *non qualified trust service*. *Qualified trust service* yang berarti *trust service* yang memenuhi persyaratan yang berlaku dan telah ditetapkan dalam regulasi No. 910/2014.

Sebagai upaya untuk mengejar ketertinggalan dengan negara-negara lain dalam mengatur masalah *e commerce* serta untuk melaksanakan ketentuan Pasal 68 ayat (2) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Kementrian Kominfo berupaya menetapkan Peraturan Menteri Komunikasi dan Informatika tentang Lembaga Sertifikasi Keandalan dengan Rancangan Peraturan Menteri sebagai berikut,

Pasal 1 dalam Peraturan Menteri ini angka 1 yang dimaksud dengan Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, foto, rancangan, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Angka 2 menjelaskan mengenai pengertian Transaksi Elektronik yaitu perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya. Pasal 1 angka (3) menyebutkan, Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh tenaga profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan Sertifikat Keandalan dalam Transaksi Elektronik. Lebih lanjut pada nomor (4) di sebutkan Sertifikat Keandalan adalah dokumen yang menyatakan Orang, lembaga dan/atau Pelaku Usaha yang menyelenggarakan transaksi secara elektronik telah lulus penilaian dan audit dari Lembaga Sertifikasi Keandalan. Nomor (5) menyebutkan, Label Sertifikat Keandalan adalah label (*trustmark*) berupa penanda secara elektronik yang ditunjukkan pada laman (*home page*) dan/atau Sistem Elektronik Pelaku Usaha sebagai bukti telah dilakukan sertifikasi keandalan. (6) Penyelenggaraan Sertifikasi Keandalan adalah penyediaan layanan sertifikasi keandalan berupa penerbitan, perpanjangan, pencabutan, dan publikasi Sertifikat Keandalan yang menjadi pelekat antara Pengguna dengan Sistem Elektronik tertentu. (7) Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang

berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirim-kan, dan/atau menyebarkan Informasi Elektronik. (8) *Certification Policy* adalah aturan tata cara dan/atau prosedur yang ditulis dan digunakan oleh Lembaga Sertifikasi Keandalan untuk penerbitan, perpanjangan, pencabutan dan publikasi Sertifikat Keandalan. (9) *Certification Practice Statement* adalah ketentuan prosedur operasional Penyelenggaraan Sertifikasi Keandalan termasuk tata cara penerbitan Sertifikat Keandalan.

Nomor (10) menyebutkan, *Certificate of Conformity* adalah sertifikat kemampuan kesesuaian terhadap *Certification Policy* dan *Certification Practice Statement* yang harus dimiliki oleh Lembaga Sertifikasi Keandalan Asing yang ingin melakukan Penyelenggaraan Sertifikasi Keandalan di wilayah Indonesia. (11) dikatakan bahwa, Pengguna Sertifikat Keandalan yang selanjutnya disebut sebagai Pengguna adalah Orang, lembaga, dan/atau Pelaku Usaha yang menggunakan Sertifikat Keandalan dalam Sistem Elektronik tertentu. Pada nomor (12) Daftar Lembaga Sertifikasi Keandalan adalah daftar resmi Lembaga Sertifikasi Keandalan. (13) Menteri adalah Menteri yang lingkup tugas dan tanggung jawabnya di bidang Komunikasi dan Informasi dan (14) Direktur Jenderal adalah Direktur Jenderal yang lingkup tugas dan tanggung jawabnya di bidang Aplikasi Informatika.

Pasal 2 Peraturan Menteri ini mencakup Lembaga Sertifikasi Keandalan, tata cara permohonan pengakuan dan pencabutan pengakuan Lembaga Sertifikasi Keandalan; Penyelenggaraan Sertifikasi Keandalan; profesi pendukung Lembaga Sertifikasi Keandalan; dan pengawasan Penyelenggaraan Sertifikasi Keandalan.

Lebih lanjut pada Pasal 3 ayat (1) menyebutkan, Penyelenggaraan Sertifikasi Keandalan diselenggarakan oleh Lembaga Sertifikasi Keandalan. (2) Lembaga Sertifikasi Keandalan sebagaimana dimaksud pada ayat (1) harus mendapatkan pengakuan dari Menteri dan ayat (3) Pengakuan sebagaimana dimaksud pada ayat (2) dilaksanakan oleh Direktur Jenderal.

Pasal 4 ayat (1) menjelaskan bahwa Lembaga Sertifikasi Keandalan terdiri atas a. Lembaga Sertifikasi Keandalan Indonesia; dan b. Lembaga Sertifikasi Keandalan asing. (2) Lembaga Sertifikasi Keandalan sebagaimana dimaksud pada ayat (1) berbentuk badan hukum Indonesia yang berdomisili di Indonesia. (3) Lembaga Sertifikasi Keandalan asing dapat bekerja sama dengan Lembaga Sertifikasi Keandalan Indonesia. (4) Kerja sama sebagaimana dimaksud pada ayat (3) harus dilaporkan secara tertulis kepada Direktur Jenderal.

Pada Pasal 5 ayat (1) Lembaga Sertifikasi Keandalan berfungsi memberikan layanan penerbitan Sertifikat Keandalan yang memberi jaminan kebenaran (*trust*) terhadap informasi Pelaku Usaha beserta Sistem Elektroniknya. (2) Sertifikat Keandalan sebagaimana dimaksud pada ayat (1) merupakan jaminan bahwa Pelaku Usaha telah memenuhi kriteria yang ditentukan oleh Lembaga Sertifikasi Keandalan. Lebih lanjut Pasal 6 ayat (1) Lembaga Sertifikasi Keandalan berhak menerbitkan Sertifikat Keandalan kepada Pelaku Usaha Penyelenggara Sistem Elektronik. (2) Pelaku Usaha sebagaimana dimaksud pada ayat (1) berhak menggunakan Sertifikat Keandalan pada laman (*home page*) dan/atau Sistem Elektronik lainnya. (3) Terhadap penerbitan Sertifikat Keandalan sebagaimana dimaksud pada ayat (1), Lembaga Sertifikasi Keandalan berhak memungut biaya atas layanannya.

Kategori sertifikat keandalan yang diterbitkan oleh Lembaga Sertifikasi Keandalan oleh Rancangan Peraturan Menteri terdapat dalam Pasal 7 antara lain, a. pengamanan terhadap identitas; b. pengamanan terhadap pertukaran data; c. pengamanan terhadap kerawanan; d. pemeringkatan konsumen; dan e. pengamanan terhadap kerahasiaan Data Pribadi.

Kewajiban Lembaga Sertifikasi Keandalan diatur dalam Pasal 8 yang berbunyi, a. melakukan pengujian keautentikan identitas dan keandalan Sistem Elektronik Pelaku Usaha; b. menyusun dan melaksanakan tata cara dan prosedur untuk melindungi dan/atau merahasiakan integritas data, catatan, dan informasi terkait Sertifikat Keandalan; c. memiliki rencana keberlangsungan bisnis (*business continuity plan*) termasuk rencana kontingensi yang efektif

untuk memastikan tersedianya sistem dan jasa Sertifikasi Keandalan secara berkesinambungan; d. menempatkan data, catatan, dan informasi Sertifikat Keandalan ke dalam sistem penyimpanan (*repository*) yang aman dan handal sesuai dengan ketentuan perundang-undangan yang berlaku; e. menjamin stabilitas finansial untuk keberlangsungan Penyelenggaraan Sertifikasi Keandalan; dan f. menyampaikan laporan operasional secara berkala kepada Direktur Jenderal.

Persyaratan sebagai Lembaga sertifikasi Keandalan diatur pada Bagian tiga Pasal 9 yang berisi a. merupakan badan hukum yang memiliki ruang lingkup usaha di bidang Teknologi Informasi dan/atau yang terkait Teknologi Informasi; b. memiliki modal kerja untuk melaksanakan tanggung jawab Lembaga Sertifikasi Keandalan; c. memiliki kemampuan teknis dalam penerbitan Sertifikat Keandalan; d. memiliki tenaga profesional paling sedikit 3 (tiga) profesi yaitu konsultan Teknologi Informasi, auditor Teknologi Informasi, dan konsultan hukum bidang Teknologi Informasi; e. tenaga profesional sebagaimana dimaksud dalam huruf d memiliki sertifikat profesi dan/atau izin profesi dan/atau sertifikat kompetensi sesuai peraturan perundang-undangan; f. tenaga profesional sebagaimana dimaksud dalam huruf d sekurang-kurangnya 1 (satu) tenaga profesional tetap untuk setiap profesi dimaksud; g. memiliki dukungan profesional lainnya yang memiliki sertifikat profesi dan/atau izin profesi dan/atau sertifikat kompetensi yang dibutuhkan untuk daya dukung layanan sertifikasi keandalan; dan h. tenaga profesional sebagaimana dimaksud pada huruf d dan huruf g harus menggunakan profesional berkewarga negaraan Indonesia.

Bab III mengatur mengenai Tata Cara Permohonan Pengakuan Lembaga Sertifikasi Keandalan. Pada bab ini di bagi menjadi tiga bagian yaitu tata cara permohonan pengakuan, proses evaluasi dan verifikasi serta daftar lembaga sertifikasi keandalan. Bagian satu pada Pasal 10 ayat (1) Lembaga Sertifikasi Keandalan mengajukan permohonan pengakuan kepada Direktur Jenderal sebagai Lembaga Sertifikasi Keandalan sesuai dengan format tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Menteri

ini. (2) Permohonan sebagaimana dimaksud pada ayat (1) sesuai dengan kategori layanan Lembaga Sertifikasi Keandalan sebagaimana dimaksud dalam Pasal 7. (3) Direktur Jenderal melakukan evaluasi terhadap permohonan pengakuan sebagai Lembaga Sertifikasi Keandalan dan ayat (4) Evaluasi sebagaimana dimaksud dalam ayat (3) dilaksanakan oleh tim evaluasi permohonan pengakuan yang dibentuk oleh Direktur Jenderal.

Lebih lanjut Pasal 11 Permohonan pengakuan sebagai Lembaga Sertifikasi Keandalan melampirkan a. profil badan hukum sesuai dengan format tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini; b. dokumen badan hukum antara lain salinan akta pendirian perusahaan dan pengesahannya; salinan akta perubahan perusahaan terakhir dan pengesahannya dalam hal telah terjadi perubahan; salinan Nomor Pokok Wajib Pajak (NPWP); dan salinan keterangan domisili. c. proposal Penyelenggaraan Sertifikasi Keandalan terdiri dari 1) komponen Sistem Elektronik Lembaga Sertifikasi Keandalan, disesuaikan dengan jenis layanan yang akan diajukan sebagaimana dimaksud dalam Pasal 7, meliputi a) perangkat lunak; b) perangkat keras; c) dukungan tenaga profesional dan sumber daya manusia; d) kebijakan tata kelola Sistem Elektronik; d) sistem keamanan Sistem Elektronik untuk Penyelenggaraan Sertifikasi Keandalan; e) prosedur perlindungan keamanan informasi; dan f) kemampuan menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik.

Certification Policy dan *Certificate Practice Statement* Penyelenggaraan Sertifikasi Keandalan untuk kategori layanan pengamanan terhadap identitas, pengamanan pertukaran data, dan pengamanan terhadap kerawanan; 1. salinan sertifikat kelaikan dari LS LSK; 2. pengalaman badan hukum baik pengalaman umum maupun pengalaman yang terkait dengan Teknologi Informasi; dan 3. penjelasan sumber daya manusia badan hukum dan melampirkan salinan sertifikat profesi dan/atau izin profesi dan/atau sertifikat kompetensi. Kemampuan keuangan yang dibuktikan dengan, 1. untuk badan hukum yang telah lama beroperasi, modal likuid perusahaan senilai paling sedikit Rp5.000.000.000,00 (lima milyar rupiah), yang dibuktikan dengan salinan

neraca keuangan *audited* 2 (dua) tahun terakhir; 2. untuk badan hukum yang baru beroperasi, modal disetor perusahaan senilai paling sedikit Rp5.000.000.000,00 (lima milyar rupiah), yang dibuktikan dengan akte pendirian perusahaan dan salinan rekening keuangan perusahaan.

Bagian Kedua tentang Proses Evaluasi dan Verifikasi termuat dalam Pasal 12 ayat (1) Dalam hal permohonan pengakuan sebagai Lembaga Sertifikasi Keandalan, pemohon harus memenuhi kelengkapan dokumen sebagaimana dimaksud dalam Pasal 10 dan Pasal 11. Ayat (2) Atas kelengkapan sebagaimana dimaksud pada ayat (1) dilakukan evaluasi dan verifikasi terhadap pemenuhan dan keabsahan dokumen, kemampuan finansial, kemampuan operasional, dan kemampuan teknis.

Pasal 13 ayat (1) Dalam hal proses evaluasi dan verifikasi menyatakan pemohon memenuhi persyaratan sebagai Lembaga Sertifikasi Keandalan, Direktur Jenderal menerbitkan surat pengakuan sebagai Lembaga Sertifikasi Keandalan paling lambat 20 (dua puluh) hari kerja sejak tanggal diterimanya surat permohonan, Ayat (2) Dalam hal proses evaluasi dan verifikasi menyatakan pemohon tidak memenuhi persyaratan sebagai Lembaga Sertifikasi Keandalan, Direktur Jenderal memberikan penolakan secara tertulis disertai alasan penolakan paling lambat 20 (dua puluh) hari kerja sejak tanggal diterimanya surat permohonan, ayat (3) dalam hal permohonan pendaftaran pengakuan sebagai Lembaga Sertifikasi Keandalan tidak memenuhi kelengkapan dokumen, Direktur Jenderal memberikan penolakan alasan ketidaklengkapan dokumen secara tertulis paling lambat 14 (empat belas) hari kerja sejak tanggal diterimanya surat permohonan.

Pada Pasal 14 berbunyi, Surat pengakuan sebagaimana dimaksud dalam Pasal 13 ayat (1) berlaku selama 10 (sepuluh) tahun sejak tanggal surat pengakuan, lebih lanjut Pasal 15 ayat (1) Pemberian pengakuan Lembaga Sertifikasi Elektronik dikenakan biaya sebagai Penerimaan Negara Bukan Pajak. (2) Biaya sebagaimana dimaksud pada ayat (1) diatur berdasarkan peraturan pemerintah.

Daftar Lembaga Sertifikasi Keandalan terdapat dalam Bagian Tiga, antara lain pada Pasal 16 ayat (1) Direktur Jenderal membuat Daftar Lembaga Sertifikasi Keandalan yang memuat Lembaga Sertifikasi Keandalan yang memiliki layanan sertifikasi keandalan bersifat aktif. (2) Direktur Jenderal menempatkan Lembaga Sertifikasi Keandalan yang telah memperoleh surat pengakuan ke dalam Daftar Lembaga Sertifikasi Keandalan dan (3) Direktur Jenderal mempublikasikan Daftar Lembaga Sertifikasi Keandalan melalui laman (*home page*) milik Kementerian Komunikasi dan Informatika.

Layanan sertifikasi keandalan diatur dalam Pasal 17 ayat (1) Layanan sertifikasi keandalan, meliputi sebagai berikut a. penerbitan Sertifikat Keandalan; b. perpanjangan Sertifikat Keandalan; c. pencabutan Sertifikat Keandalan; dan/atau d. publikasi Sertifikat Keandalan. Ayat (2) Layanan sertifikasi keandalan dijalankan sesuai dengan prinsip-prinsip yang benar dan sesuai dalam *Certification Policy* dan *Certification Practice Statement*. Lebih lanjut pada Pasal 18 berisi tentang Sertifikat Keandalan wajib memenuhi unsur-unsur sebagai berikut a. Sertifikat Keandalan harus menunjukkan dan/atau menggambarkan informasi, data, dan dokumen yang sesuai dan benar yang melekat pada Sertifikat Keandalan tersebut terkait dengan Pengguna; b. Sertifikat Keandalan harus menunjukkan informasi, data, dan dokumen dari Lembaga Sertifikasi Keandalan yang mengeluarkan Sertifikat Keandalan; dan c. Perubahan terhadap informasi, data, dan dokumen yang melekat pada Sertifikat Keandalan harus sepengetahuan Lembaga Sertifikasi Keandalan dan Pengguna.

Pasal 19 ayat (1) Lembaga Sertifikasi Keandalan melakukan penerimaan pendaftaran Sertifikat Keandalan kepada Orang, lembaga, dan/atau Pelaku Usaha yang membutuhkan layanan sertifikasi keandalan. (2) Lembaga Sertifikasi Keandalan melakukan verifikasi secara benar dan teliti terhadap pendaftar sesuai dengan jenis Sertifikat Keandalan yang dibutuhkan. (3) Terhadap pendaftaran sebagaimana dimaksud pada ayat (1), Lembaga Sertifikasi Keandalan harus melakukan cek fisik terhadap calon Pengguna tersebut. (4) Dalam hal proses pendaftaran selesai dilaksanakan maka Lembaga

Sertifikasi Keandalan memberikan Label Sertifikat Keandalan kepada Pengguna untuk dimasukkan ke dalam laman (*home page*) dan/atau Sistem Elektronik lainnya milik Pengguna.

Lebih lanjut pasal Pasal 20 ayat (1) Sertifikat Keandalan memiliki masa berlaku 1 (satu) tahun dan dapat diperpanjang sesuai dengan kebutuhan Pengguna. Ayat (2) 1 (satu) bulan sebelum masa berlaku berakhir, Lembaga Sertifikasi Keandalan wajib memberikan notifikasi kepada Pengguna untuk memperpanjang Sertifikat Keandalan. Pasal 21 ayat (1) Sertifikat Keandalan dapat berstatus tidak aktif dikarenakan hal-hal sebagai berikut: a. berakhirnya masa berlaku Sertifikat Keandalan dan tidak diperpanjang oleh Pengguna; dan/atau, b. pembatalan Sertifikat Keandalan. Ayat (2) Pembatalan Sertifikat Keandalan sebagaimana dimaksud pada ayat (1) huruf b dapat disebabkan hal-hal sebagai berikut: a. permintaan Pengguna yang bersangkutan; dan/atau b. adanya pengaduan pelanggaran hukum Pengguna. Pasal 22 ayat (1) Lembaga Sertifikasi Keandalan menerbitkan daftar Pengguna dan mempublikasikan daftar Pengguna dalam laman (*home page*) dan/atau media publikasi lainnya. (2) Daftar Pengguna berisi sebagai berikut: a. Pengguna yang aktif; dan b. Pengguna yang tidak aktif.

Bagian Kedua mengatur tentang Penggunaan Sertifikat Keandalan. Terdapat dalam Pasal 23 ayat (1) Sertifikat Keandalan selain untuk memberikan jaminan identitas, dapat juga memberikan jaminan bentuk kebenaran lainnya. Ayat (2) Sertifikat Keandalan sebagaimana dimaksud pada ayat (1) memiliki beberapa kategorisasi antara lain: a. pengamanan terhadap identitas; b. pengamanan terhadap pertukaran data; c. pengamanan terhadap kerawanan; d. pemeringkatan konsumen; dan/atau e. pengamanan terhadap kerahasiaan Data Pribadi. (2) Kategori Sertifikat Keandalan dapat berkembang diluar kategori sebagaimana dimaksud pada ayat (2) sesuai dengan kebutuhan Pengguna. (3) Sertifikat Keandalan diakui dan dinyatakan sah apabila diterbitkan oleh Lembaga Sertifikasi Keandalan.

Pada Pasal 24 ayat (1) Kategori pengamanan terhadap identitas merupakan produk Sertifikat Keandalan yang berisi jaminan kebenaran

identitas Pengguna. Ayat (2) Kategori pengamanan terhadap pertukaran data merupakan produk Sertifikat Keandalan yang berisi jaminan bahwa Sistem Elektronik dari Pengguna telah diperkuat dengan layanan keamanan pengisian dan pengiriman data misalnya produk protokol SSL/*Secure Security Layer*. (3) Kategori pengamanan terhadap kerawanan merupakan produk Sertifikat Keandalan yang berisi jaminan bahwa Sistem Elektronik dari Pengguna telah dilengkapi dengan sistem keamanan tertentu misalnya manajemen keamanan informasi yang dilengkapi dengan proses sertifikasinya dan/atau dilengkapi dengan perangkat sekuriti lainnya baik perangkat keras maupun perangkat lunak. (4) Kategori pemeringkatan konsumen merupakan produk Sertifikat Keandalan yang menjelaskan bahwa layanan Sistem Elektronik dari Pengguna memiliki sertifikat-sertifikat terkait dengan jaminan konsumen/ pasar/produk yang diterbitkan oleh Lembaga Sertifikasi Keandalan atau lembaga lain yang terkait dengan konsumen dan pemasaran. (5) Kategori pengamanan terhadap kerahasiaan Data Pribadi merupakan produk Sertifikat Keandalan yang berisi jaminan bahwa Data Pribadi konsumen yang bertransaksi dengan Pengguna dilindungi kerahasiaannya sesuai dengan ketentuan peraturan perundang-undangan.

Disebutkan pula dalam Pasal 25 ayat (1) Lembaga Sertifikasi Keandalan harus melakukan verifikasi untuk tiap kategori Sertifikat Keandalan. (2) Verifikasi minimal yang harus dilakukan oleh Lembaga Sertifikasi Keandalan adalah sebagai berikut: a. terhadap Sertifikat Keandalan kategori pengamanan terhadap identitas, Lembaga Sertifikasi Keandalan wajib melakukan verifikasi kebenaran identitas Pengguna; b. terhadap Sertifikat Keandalan kategori pengamanan terhadap pertukaran data, Lembaga Sertifikasi Keandalan wajib melakukan unsur-unsur sebagai berikut: 1. verifikasi Sertifikat Elektronik yang dimiliki Pengguna; dan 2. melakukan pengujian terhadap Sertifikat Elektronik Pengguna. c. terhadap Sertifikat Keandalan kategori pengamanan terhadap kerawanan, Lembaga Sertifikasi Keandalan wajib melakukan unsur-unsur sebagai berikut. 1. menerapkan Standar Nasional Indonesia (SNI) ISO 17799:2005 tentang Teknologi Informasi – Kode Pengaturan Manajemen

Pengamanan Informasi; 2. menerapkan Standar Nasional Indonesia (SNI) ISO 27001:2009 tentang Teknologi informasi – Teknik Keamanan – Sistem manajemen keamanan informasi – Persyaratan; 3. menerapkan Standar Nasional Indonesia (SNI) ISO 19-7125:2005 tentang Teknologi Informasi – Teknik Keamanan – Panduan Teknik untuk Penggunaan dan Manajemen Jasa Pihak Ketiga Terpercaya; dan 4. menerapkan Standar Nasional Indonesia (SNI) ISO 9001 tentang Manajemen Mutu. a. terhadap Sertifikat Keandalan kategori pemeringkatan konsumen, Lembaga Sertifikasi Keandalan wajib melakukan mekanisme tertentu dalam mempublikasikan metode, pelaksanaan, dan hasil pemeringkatan konsumen; b. terhadap Sertifikat Keandalan kategori pengamanan terhadap kerahasiaan Data Pribadi, Lembaga Sertifikasi Keandalan wajib melakukan penerapan prosedur dan pengamanan terhadap prosedur tersebut atas penyimpanan, penggandaan cadangan, batas waktu, penghapusan, dan pemanfaatan data oleh pihak ketiga.

Pelaporan Penyelenggaraan Sertifikasi Keandalan termuat dalam Pasal 26 ayat (1) Lembaga Sertifikasi Keandalan wajib menyampaikan laporan kepada Direktur Jenderal sebagai berikut: a. laporan kegiatan Penyelenggaraan Sertifikasi Keandalan tahunan, periode Januari sampai dengan Desember setiap tahun; dan b. laporan kegiatan Penyelenggaraan Sertifikasi Keandalan 5 (lima) tahunan. Ayat (2) Laporan sebagaimana dimaksud pada ayat (1) sesuai dengan format tercantum dalam Lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini. (3) Lembaga Sertifikasi Keandalan wajib menyampaikan laporan kepada Direktur Jenderal apabila diminta oleh Direktur Jenderal selain kewajiban laporan sebagaimana dimaksud pada ayat (1) sesuai dengan tenggang waktu yang diminta. Lebih lanjut Pasal 27 ayat (1) Laporan kegiatan Penyelenggaraan Sertifikasi Keandalan tahunan diterima oleh Direktur Jenderal paling lambat akhir bulan April tahun berikutnya. Ayat (2) Laporan kegiatan Penyelenggaraan Sertifikasi Keandalan 5 (lima) tahunan diterima oleh Direktur Jenderal paling lambat akhir bulan Mei tahun berikutnya dari setiap periode 5 (lima) tahunan. Ayat (3) Laporan sewaktu-waktu diterima

commit to user

oleh Direktur Jenderal paling lambat 20 (dua puluh) hari kerja sejak permintaan disampaikan oleh Direktur Jenderal.

Profesi pendukung lembaga sertifikasi keandalan diatur dalam BAB V. Pada Pasal 28 ayat (1) Keahlian atau profesi pendukung Penyelenggaraan Sertifikasi Keandalan, meliputi dan tidak terbatas kepada a. konsultan Teknologi Informasi; b. auditor Teknologi Informasi; c. konsultan hukum bidang Teknologi Informasi; d. konsultan manajemen bidang Teknologi Informasi; e. akuntan; f. penilai (*appraiser* atau *assessor*); g. notaris. Ayat (2) Keahlian atau profesi pendukung Penyelenggaraan Sertifikasi Keandalan selain sebagaimana dimaksud pada ayat (1) diperbolehkan sepanjang terkait dengan kebutuhan dan daya dukung untuk Penyelenggaraan Sertifikasi Keandalan. Ayat (3) Tenaga profesi yang diajukan tidak sedang dalam status hukum tersangka atau dalam hukuman.

Pasal 29 ayat (1) Kesesuaian profesi pendukung Lembaga Sertifikasi Keandalan dinilai oleh LS LSK. Ayat (2) Ketentuan lebih lanjut mengenai persyaratan profesi pendukung Lembaga Sertifikasi Keandalan sebagaimana dimaksud pada ayat (1) diatur secara terpisah dalam Peraturan Menteri tersendiri.

Pengawasan penyelenggaraan sertifikasi keandalan diatur dalam Pasal 30 ayat (1) Direktur Jenderal melakukan evaluasi operasional Penyelenggaraan Sertifikasi Keandalan kepada Lembaga Sertifikasi Keandalan. (2) Evaluasi operasional sebagaimana dimaksud pada ayat (1) mencakup: a. evaluasi secara periodik setiap tahun; b. evaluasi menyeluruh setiap 5 (lima) tahun; dan c. evaluasi sewaktu-waktu apabila dibutuhkan. (3) Evaluasi sebagaimana dimaksud pada ayat (2) melakukan penilaian, sebagai berikut, a. kesesuaian Lembaga Sertifikasi Keandalan sebagai penyelenggara Sertifikasi Keandalan; b. rekam jejak dan keberlangsungan layanan sertifikasi keandalan; c. manajemen operasional Lembaga Sertifikasi Keandalan; dan d. pencapaian dan kinerja operasional Penyelenggaraan Sertifikasi Keandalan. Lebih lanjut Pasal 31 ayat (1) Dalam melakukan evaluasi sebagaimana dimaksud dalam Pasal 30, Direktur Jenderal membentuk tim evaluasi dengan melibatkan instansi

pengawas dan pengatur sektor terkait. Ayat (2) Apabila diperlukan, tim evaluasi dapat mengikutsertakan pihak ketiga yang memiliki profesional yang sesuai untuk melakukan penelitian lebih seksama dalam rangka evaluasi menyeluruh.

Teguran Penyelenggaraan sertifikasi keandalan diatur dalam Pasal 32 ayat (1) Apabila Lembaga Sertifikasi Keandalan tidak menyampaikan laporan sebagaimana dimaksud pada Pasal 27 sesuai dengan batas waktu yang ditentukan, maka dalam waktu 8 (delapan) hari kerja dari batas waktu dimaksud Direktur Jenderal memberikan surat peringatan pertama yang berisi teguran terkait kepada Lembaga Sertifikasi Keandalan. (2) Apabila surat peringatan pertama sebagaimana dimaksud pada ayat (1) tidak dijawab dan/atau ditanggapi oleh Lembaga Sertifikasi Keandalan sampai dengan 10 (sepuluh) hari kerja sejak tanggal surat peringatan pertama, maka Direktur Jenderal memberikan surat peringatan kedua kepada Lembaga Sertifikasi Keandalan. (3) Apabila surat peringatan kedua sebagaimana dimaksud pada ayat (2) tidak dijawab dan/atau ditanggapi oleh Lembaga Sertifikasi Keandalan sampai dengan 10 (sepuluh) hari kerja sejak tanggal surat peringatan kedua, maka Direktur Jenderal memberikan surat peringatan ketiga kepada Lembaga Sertifikasi Keandalan dan (4) Apabila surat peringatan ketiga sebagaimana dimaksud pada ayat (3) tidak dijawab dan/atau ditanggapi oleh Lembaga Sertifikasi Keandalan sampai dengan 10 (sepuluh) hari kerja sejak tanggal surat peringatan ketiga, maka Direktur Jenderal akan melakukan evaluasi menyeluruh terhadap Lembaga Sertifikasi Keandalan baik dari sisi kelembagaan, manajemen, maupun operasional.

Pasal 33 ayat (1) Dalam hasil evaluasi menyeluruh 5 (lima) tahunan ditemukan adanya ketidaksesuaian dan/atau penyimpangan baik dari sisi badan hukum maupun operasi layanan sertifikasi keandalan, maka Direktur Jenderal memberikan teguran kepada Lembaga Sertifikasi Keandalan melalui surat peringatan pertama. (2) Apabila surat peringatan pertama sebagaimana dimaksud pada ayat (1) tidak dijawab dan/atau ditanggapi oleh Lembaga Sertifikasi Keandalan sampai dengan 10 (sepuluh) hari kerja sejak tanggal surat

peringatan pertama, maka Direktur Jenderal memberikan surat peringatan kedua kepada Lembaga Sertifikasi Keandalan. (3) Apabila surat peringatan kedua sebagaimana dimaksud pada ayat (2) tidak dijawab dan/atau ditanggapi oleh Lembaga Sertifikasi Keandalan sampai dengan 10 (sepuluh) hari kerja sejak tanggal surat peringatan kedua, maka Direktur Jenderal memberikan surat peringatan ketiga kepada Lembaga Sertifikasi Keandalan. (4) Apabila surat peringatan ketiga sebagaimana dimaksud pada ayat (3) tidak dijawab dan/atau ditanggapi oleh Lembaga Sertifikasi Keandalan sampai dengan 10 (sepuluh) hari kerja sejak tanggal surat peringatan ketiga, maka Direktur Jenderal akan melakukan evaluasi menyeluruh terhadap Lembaga Sertifikasi Keandalan baik dari sisi kelembagaan, manajemen, maupun operasional.

Pasal 34 ayat (1) Dalam hasil evaluasi sewaktu-waktu ditemukannya adanya ketidaksesuaian dan/atau penyimpangan baik dari sisi badan hukum maupun operasi layanan sertifikasi keandalan, maka Direktur Jenderal memberikan teguran kepada Lembaga Sertifikasi Keandalan melalui surat peringatan pertama. Ayat (2) Apabila surat peringatan pertama sebagaimana dimaksud pada ayat (1) tidak dijawab dan/atau ditanggapi oleh Lembaga Sertifikasi Keandalan sampai dengan 10 (sepuluh) hari kerja sejak tanggal surat peringatan pertama, maka Direktur Jenderal memberikan surat peringatan kedua kepada Lembaga Sertifikasi Keandalan. (3) Apabila surat peringatan kedua sebagaimana dimaksud pada ayat (2) tidak dijawab dan/atau ditanggapi oleh Lembaga Sertifikasi Keandalan sampai dengan 10 (sepuluh) hari kerja sejak tanggal surat peringatan kedua, maka Direktur Jenderal memberikan surat peringatan ketiga kepada Lembaga Sertifikasi Keandalan. (4) Apabila surat peringatan ketiga sebagaimana dimaksud pada ayat (3) tidak dijawab dan/atau ditanggapi oleh Lembaga Sertifikasi Keandalan sampai dengan 10 (sepuluh) hari kerja sejak tanggal surat peringatan ketiga, maka Direktur Jenderal akan melakukan evaluasi menyeluruh terhadap Lembaga Sertifikasi Keandalan baik dari sisi kelembagaan, manajemen, maupun operasional.

Pencabutan Surat Pengakuan diatur dalam Pasal 35 ayat (1) Direktur Jenderal berwenang mencabut surat pengakuan sebagai Lembaga Sertifikasi

Keandalan atas nama badan hukum tertentu apabila, a. atas permintaan Lembaga Sertifikasi Keandalan sendiri; dan/atau, b. adanya pelanggaran oleh Lembaga Sertifikasi Keandalan. Ayat (2) Atas pemenuhan pencabutan sebagaimana dimaksud pada ayat (1), Lembaga Sertifikasi Keandalan wajib melakukan hal-hal sebagai berikut, a. menyampaikan pemberitahuan terbuka kepada publik melalui iklan di media massa nasional sekurang-kurangnya 3 (tiga) bulan, sejak diterbitkannya surat pencabutan pengakuan Lembaga Sertifikasi Keandalan; dan d. mengalihkan Pengguna kepada Lembaga Sertifikasi Keandalan lain yang mendapat pengakuan dari Menteri paling lama 3 (tiga) bulan sejak diterbitkannya surat pencabutan pengakuan Lembaga Sertifikasi Keandalan.

Leboh lanjut pada Pasal 36 ayat (1) Pencabutan pengakuan Lembaga Sertifikasi Keandalan atas permintaan sendiri dapat dilakukan jika Lembaga Sertifikasi Keandalan tidak dapat memenuhi satu atau seluruh butir kewajiban sebagaimana diatur dalam Pasal 8. (2) Pencabutan pengakuan Lembaga Sertifikasi Keandalan atas permintaan sendiri harus mengajukan permohonan pemberhentian Penyelenggaraan Sertifikasi Keandalan kepada Direktur Jenderal dengan melampirkan alasan-alasan penghentian operasi Lembaga Sertifikasi Keandalan yang bersangkutan.

Pada Pasal 37 berisi tentang Pencabutan pengakuan Lembaga Sertifikasi Keandalan karena pelanggaran dapat dilakukan jika terjadi hal-hal berikut: a. hasil evaluasi menyeluruh sebagaimana dimaksud dalam Pasal 33; b. Lembaga Sertifikasi Keandalan tidak menjawab dan/atau menanggapi surat peringatan ketiga sampai dengan waktu yang ditentukan sebagaimana dimaksud dalam Pasal 32, Pasal 33, dan Pasal 34; dan/atau c. Adanya putusan pengadilan terkait pelanggaran peraturan perundang-undangan yang dilakukan Lembaga Sertifikasi Keandalan.

Perpanjangan Pengakuan Lembaga Sertifikasi Keandalan terdapat dalam Pasal 38 ayat (1) Lembaga Sertifikasi Keandalan dapat mengajukan perpanjangan pengakuan Lembaga Sertifikasi Keandalan dengan mengajukan surat permohonan perpanjangan pengakuan paling lambat 4 (empat) bulan

sebelum masa berlaku pengakuan habis. (2) Evaluasi permohonan perpanjangan pengakuan sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan pada hasil evaluasi menyeluruh dan pemenuhan kewajiban sebagai Lembaga Sertifikasi Keandalan sebagaimana dimaksud dalam Pasal 8.

Lebih lanjut disebutkan dalam Pasal 39 ayat (1) Dalam hal proses evaluasi permohonan perpanjangan pengakuan sebagaimana dimaksud dalam Pasal 38 ayat (1) menyatakan pemohon memenuhi persyaratan sebagai Lembaga Sertifikasi Keandalan, Direktur Jenderal menerbitkan surat pengakuan sebagai Lembaga Sertifikasi Keandalan paling lambat 20 (dua puluh) hari kerja sejak tanggal diterimanya surat permohonan perpanjangan pengakuan dan kelengkapan evaluasi menyeluruh. (2) Dalam hal proses evaluasi permohonan perpanjangan pengakuan sebagaimana dimaksud dalam Pasal 38 ayat (1) tidak memenuhi persyaratan sebagai Lembaga Sertifikasi Keandalan, Direktur Jenderal memberikan penolakan secara tertulis disertai alasan penolakan paling lambat 20 (dua puluh) hari kerja sejak tanggal diterimanya surat permohonan perpanjangan pengakuan dan kelengkapan evaluasi menyeluruh.

Pasal 40 menyebutkan, Surat pengakuan sebagai Lembaga Sertifikasi Keandalan yang telah diperbaharui sebagaimana dimaksud dalam Pasal 39 ayat (1) berlaku selama 10 (sepuluh) tahun sejak berakhirnya tanggal masa laku surat pengakuan sebelumnya. Ketentuan lain-lain diatur dalam Pasal 41 yang berbunyi Sertifikat Keandalan dapat menjadi alat bukti yang sah di pengadilan sepanjang diterbitkan oleh Lembaga Sertifikasi Keandalan yang telah mendapat pengakuan. Pasal 42 ayat (1) Dalam hal Lembaga Sertifikasi Keandalan sebagaimana dimaksud dalam Pasal 3 belum tersedia, apabila diperlukan layanan sertifikasi keandalan oleh masyarakat, Direktur Jenderal membentuk tim sertifikasi keandalan. (2) Tim Sertifikasi Keandalan sebagaimana dimaksud ayat (1) melaksanakan kewajiban-kewajiban Lembaga Sertifikasi Keandalan sebagaimana dimaksud dalam Pasal 8.

Pasal 43 ayat (1) Pengaturan tentang LS LSK diatur dalam peraturan menteri tersendiri. Dalam hal LS LSK belum tersedia, penilaian kelaikan calon

Lembaga Sertifikasi Keandalan dilakukan oleh Tim Penilai Kelaikan yang dibentuk oleh Direktur Jenderal. (3) Tim Penilai sebagaimana dimaksud pada ayat (2) menilai parameter calon Lembaga Sertifikasi Keandalan meliputi: a. kemampuan sumber daya manusia dalam penguasaan penerapan Sertifikasi Keandalan; dan b. kemampuan Sistem Elektronik penerbit Sertifikat Keandalan dalam kesesuaian penerbitan Sertifikat Keandalan. Ayat (4) Tim Penilai Kelaikan Lembaga Sertifikasi Keandalan menerbitkan berita acara pemeriksaan atas hasil pemeriksaan Sistem Elektronik Lembaga Sertifikasi Keandalan. (5) Berita acara pemeriksaan sebagaimana dimaksud pada ayat (4) dapat digunakan untuk menggantikan persyaratan calon Lembaga Sertifikasi Keandalan sebagaimana dimaksud dalam Pasal 11 Huruf c Poin 3. (6) Dalam hal di kemudian hari tersedia LS LSK, maka Lembaga Sertifikasi Keandalan harus memperoleh sertifikat kelaikan Lembaga Sertifikasi Keandalan yang diterbitkan oleh LS LSK.

Ketentuan peralihan terdapat dalam Pasal 44 ayat (1) Pada saat Peraturan Menteri ini mulai berlaku, Sertifikat Keandalan yang diterbitkan oleh Lembaga Sertifikasi Keandalan asing sebelum berlakunya Peraturan Menteri ini tetap diakui sepanjang tidak bertentangan dengan Peraturan Menteri ini. Ayat (2) Pada saat Peraturan Menteri ini mulai berlaku, Lembaga Sertifikasi Keandalan asing yang telah beroperasi sebelum berlakunya Peraturan Menteri ini, wajib menyesuaikan dengan Peraturan Menteri ini dalam jangka waktu paling lama 1 (satu) tahun sejak berlakunya Peraturan Menteri ini.

Berdasarkan Rancangan Peraturan Menteri Komunikasi dan Informatika tentang Lembaga Sertifikasi Keandalan, dapat dibandingkan dengan regulasi dari negara Singapura, Malaysia dapat ditunjukkan pada tabel berikut:

Tabel 13

Perbandingan Upaya Negara Singapura, Malaysia dan Indonesia dalam membangun keterpercayaan pada *e commerce* melalui penggunaan *Trustmark*

No	<i>Trustmark</i>	Singapura	Malaysia	Indonesia
1	Regulasi	<i>The Statutes of The Republic of Singapore Trust Companiest Act (Chapter 336).</i>	<i>Law Of Malaysia Act 709 Personal Data Protection Act 2010</i>	Pasal 65 ayat (1) Peraturan Pemerintah Nomor 82 Tahun 2012 Penyelenggaraan Sistem dan Transaksi Elektronik
2	Organisasi <i>Trustmark</i>	<i>Case Trust</i>	Malaysia <i>Trustmark</i>	-
3	Kode Etik Pelaku Usaha <i>e commerce</i>	V	V	-
4	Perlindungan terhadap konsumen <i>e commerce</i>	V	V	-

Sumber: Data mentah diolah, 2015

Berdasarkan tabel tersebut diatas, Singapura, Malaysia dan Indonesia masing-masing negara telah memiliki regulasi yang mengatur tentang *Trustmark*, namun di Indonesia belum ada Organisasi *Trustmark*, kode etik yang mengatur pelaku usaha *e commerce* khususnya yang menggunakan *website* dan belum ada perlindungan hukum secara spesifik bagi konsumen pengguna *website e commerce*. Lebih lanjut mengenai perbandingan isi regulasi yang mengatur tentang Lembaga Sertifikasi Keandalan yang terdapat dalam Rancangan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia dibandingkan dengan *The Statutes of The Republic of Singapore Trust Companiest Act (Chapter 336)* dan *Law Of Malaysia Act 709 Personal Data Protection Act 2010* secara spesifik dapat dilihat pada tabel berikut.

Tabel 14

Perbandingan Isi regulasi yang mengatur mengenai Lembaga Sertifikasi Keandalan di Indonesia, Singapore dan Malaysia

No	Singapura	Malaysia	Indonesia
Pengaturan	<i>The Statutes of The Republic of Singapore Trust Companies Act (Chapter 336).</i>	<i>Law Of Malaysia Act 709 Personal Data Protection Act 2010</i>	Rancangan Peraturan Menteri Komunikasi dan Informatika tentang Lembaga Sertifikasi Keandalan
Bagian I	<i>Preliminary</i>	<i>Preliminary</i>	Ketentuan Umum
Bagian II	<i>Licensing of Trust Company</i>	<i>Personal Data Protection</i>	Lembaga Sertifikasi Keandalan
Bagian III	<i>Control of and Shareholdings Voting Power</i> A. <i>Control over Licensed Trust Company</i> B. <i>Voluntary Transfer of Business</i>	<i>Exemption</i>	Tata Cara permohonan pengakuan Lembaga Sertifikasi Keandalan
Bagian IV	<i>Probate Administration</i>	<i>Appointment, Function and Power of Commisioner</i>	Penyelenggaraan Sertifikat Keandalan
Bagian V	<i>Conduct of Business</i>	<i>Personal data protection Fund</i>	Profesi Pendukung Lembaga Sertifikasi Keandalan
Bagian VI	<i>Books, Accounts and Audit</i>	<i>Personal data advisory Committee</i>	Pengawasan Penyelenggaraan Sertifikasi Keandalan
Bagian VII	<i>Supervision and Investigation</i>	<i>Appeal Tribunal</i>	Ketentuan lain-lain
Bagian VIII	<i>Disclosure of Information</i>	<i>Inspection, Complaint and Investigation</i>	Ketentuan Peralihan
Bagian IX	<i>Appeals</i>	<i>Enforcement</i>	Ketentuan Penutup
Bagian X	<i>Miscellaneous</i>	<i>Miscellaneous</i>	

Sumber: Data mentah diolah, 2015

Kebutuhan masyarakat akan *trust* terhadap *e commerce* menimbulkan dampak munculnya lembaga atau organisasi yang berupaya untuk memberikan jaminan kepada konsumen atas keberadaan sebuah situs. Tujuan dari organisasi dan lembaga swasta yang muncul di masyarakat tersebut memiliki tujuan yang baik, namun perlu pengaturan dan pembenahan lebih lanjut yang seharusnya diatur oleh pemerintah mengingat pemberian informasi atas sebuah situs terlebih pemberian jaminan kepada konsumen sangat rentan terhadap kepentingan masing-masing kelompok.

Trustmark atau tanda kepercayaan adalah jaminan proses pemeriksaan yang telah dilakukan suatu sistem secara obyektif dan telah diperiksa oleh profesional independen dengan standar pemeriksaan yang sesuai hukum, sehingga seperti apa yang disebutkan dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 69 ayat (2) Profesional yang membentuk Lembaga Sertifikasi Keandalan sebagaimana dimaksud pada ayat (1) paling sedikit meliputi profesi:

- a. konsultan Teknologi Informasi;
- b. auditor Teknologi Informasi; dan
- c. konsultan hukum bidang Teknologi Informasi.

Komposisi ini yang saat ini tidak dipenuhi oleh lembaga maupun organisasi swasta yang saat ini membuat *Trustmark*. Organisasi maupun lembaga swasta yang ingin menjadi Lembaga Sertifikasi Keandalan wajib memenuhi syarat tersebut karena untuk menghindari subyektifitas dan menghindari unsur muatan politis kepentingan. *Trustmark* yang diberikan oleh Lembaga Sertifikasi Keandalan yang diharapkan nantinya adalah *Trustmark* yang dapat mewakili memberikan informasi dalam hal pembuktian di pengadilan.

Hukum yang baik adalah hukum yang dapat diterima di masyarakat. Tidak mudah mengimplementasikan isi Pasal 69 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, namun adanya asosiasi atau organisasi swasta dapat membantu pemerintah memberikan informasi dan melakukan sertifikasi anggotanya sebagai upaya mewujudkan isi Pasal 66 ayat (3) Peraturan Pemerintah Nomor

82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang berbunyi, “Informasi yang lengkap dan benar sebagaimana dimaksud pada ayat (2) meliputi informasi yang: a. memuat identitas subjek hukum; b. memuat status dan kompetensi subjek hukum; c. menjelaskan hal tertentu yang menjadi syarat sahnya perjanjian; dan d. menjelaskan barang dan/atau jasa yang ditawarkan”

D. Teori *Trust* Fukuyama ditinjau dari Kontribusi *Trustmark* dalam meningkatkan Keterpercayaan dalam Dunia Bisnis dan Melindungi Konsumen Pengguna *E Commerce*

Dalam pembahasan ini penulis akan melakukan analisis berdasarkan teori *Trust* dari Fukuyama yang membagi kepercayaan masyarakat terhadap teknologi dalam dua hal yaitu:

1. Masyarakat berkepercayaan-tinggi (*high trust*)

Seperti halnya Singapura dan Malaysia dimana Pelaku usaha dalam upaya untuk membangun keterpercayaan konsumen dalam *e commerce* adalah menggunakan *Trustmark*. *Trustmark* juga disebut sebagai meterai persetujuan, kualitas segel, label atau *certificate* dalam bentuk logo, yang ditampilkan pada *homepage* dan / atau halaman *web* dari sebuah toko *online* dengan izin dari pihak ketiga yang terpercaya untuk memberikan bukti kepatuhan sukarela toko *online* dengan kode etik yang dikeluarkan oleh pihak ketiga dalam upaya memberikan yang terbaik yang mungkin secara *online* lingkungan bisnis bagi konsumen.

Jaminan yang diberikan oleh *Trustmark* Organisasi tidaklah sama. Namun *Trustmark* Organisasi tersebut akan tergabung di dalam satu wadah organisasi besar yaitu GTA (*Global Trustmark Alliance*) yang merupakan sebuah organisasi keanggotaan didorong oleh partisipasi aktif dari seluruh dunia organisasi yang bekerja dengan bisnis dan konsumen konstituen di masing-masing negara mereka untuk mempromosikan kepercayaan dalam *e-commerce*. Tujuan GTA sepenuhnya melaksanakan rekomendasi yang dibuat oleh *Global Business Dialog* untuk *Electronic*

Commerce (GBDe) untuk harmonisasi tinggi standar *e-commerce*, koperasi dan dapat diakses penyelesaian sengketa lintas batas, dan kerja sama antara program *trustmark*. Singapura menggunakan *Case Trust* sebagai organisasi *Trustmark* dan Malaysia memiliki *Malaysia Trustmark* yang mana kedua organisasi tersebut bertujuan untuk memberikan sertifikasi bagi pelaku usaha dan memberikan perlindungan bagi konsumen pengguna *e commerce*.

Unsur pokok konsumen *e commerce* sebagai modal sosial, yaitu:²⁸⁶ pertama, *Participation in a network* yang merupakan kemampuan sekelompok orang untuk melibatkan diri dalam suatu jaringan hubungan sosial, melalui berbagai variasi hubungan yang saling Ragam berdampingan dan dilakukan atas dasar prinsip kesukarelaan (*voluntary*), kesamaan (*equality*), kebebasan (*freedom*), dan keadaban (*civility*). Kemampuan anggota kelompok atau anggota masyarakat untuk selalu menyatukan diri dalam suatu pola hubungan yang sinergis akan sangat besar pengaruhnya dalam menentukan kuat tidaknya modal sosial suatu kelompok. Kedua *Reciprocity*, yang merupakan kecenderungan saling tukar kebaikan antar individu dalam suatu kelompok atau antar kelompok itu sendiri. Pola pertukaran terjadi dalam suatu kombinasi jangka panjang dan jangka pendek dengan nuansa altruism tanpa mengharapkan imbalan. Pada masyarakat dan kelompok-kelompok sosial yang terbentuk yang memiliki bobot resiprositas kuat akan melahirkan suatu masyarakat yang memiliki tingkat modal sosial yang tinggi.

Ketiga unsur *Trust* yang berarti suatu bentuk keinginan untuk mengambil resiko dalam hubungan hubungan sosialnya yang didasari oleh perasaan yakin bahwa yang lain akan melakukan sesuatu seperti yang diharapkan dan akan senantiasa bertindak dalam suatu pola tindakan yang saling mendukung. Paling tidak, yang lain tidak akan bertindak merugikan

²⁸⁶Hasbullah, Jousairi, Sosial Capital (Menuju Keunggulan Budaya Manusia Indonesia). MR United Press, Jakarta, 2006. hlm. 32

diri dan kelompoknya. Tindakan kolektif yang didasari saling percaya akan meningkatkan partisipasi masyarakat dalam berbagai bentuk dan dimensi terutama dalam konteks kemajuan bersama. Hal ini memungkinkan masyarakat untuk bersatu dan memberikan kontribusi pada peningkatan modal sosial. Keempat, *Social norma*, yang merupakan sekumpulan aturan yang diharapkan dipatuhi dan diikuti oleh masyarakat dalam suatu entitas sosial tertentu. Aturan aturan ini biasanya terinstitusionalisasi, tidak tertulis tapi dipahami sebagai penentu pola tingkah laku yang baik dalam konteks hubungan sosial sehingga ada sanksi sosial yang diberikan jika melanggar. Norma sosial akan menentukan kuatnya hubungan antar individu karena merangsang kohesifitas sosial yang berdampak positif bagi perkembangan masyarakat. Oleh karenanya norma sosial disebut sebagai salah satu modal sosial. Keenam *Values* atau sesuatu ide yang telah turun temurun dianggap benar dan penting oleh anggota kelompok masyarakat. Nilai merupakan hal yang penting dalam kebudayaan, biasanya ia tumbuh dan berkembang dalam mendominasi kehidupan kelompok masyarakat tertentu serta mempengaruhi aturan-aturan bertindak dan berperilaku masyarakat yang pada akhirnya membentuk pola *cultural*. Ketujuh adalah *Proactive action* yaitu keinginan yang kuat dari anggota kelompok untuk tidak saja berpartisipasi tetapi senantiasa mencari jalan bagi keterlibatan anggota kelompok dalam suatu kegiatan masyarakat. Anggota kelompok melibatkan diri dan mencari kesempatan yang dapat memperkaya hubungan hubungan sosial dan menguntungkan kelompok. Perilaku inisiatif dalam mencari informasi berbagai pengalaman, memperkaya ide, pengetahuan, dan beragam bentuk inisiatif lainnya baik oleh individu maupun kelompok, merupakan wujud modal sosial yang berguna dalam membangun masyarakat sosial dapat meningkatkan kesadaran individu tentang banyaknya peluang yang dapat dikembangkan untuk kepentingan masyarakat.

Masyarakat yang memiliki modal sosial tinggi terhadap teknologi khususnya dalam *e commerce* akan membuka kemungkinan menyelesaikan

kompleksitas persoalan dengan lebih mudah. Melalui sikap saling percaya, toleransi, dan kerjasama mereka dapat membangun jaringan baik di dalam kelompok masyarakatnya maupun dengan kelompok masyarakat lainnya yang diwujudkan dalam organisasi maupun asosiasi pelaku usaha maupun konsumen. Pada masyarakat tradisional, diketahui memiliki asosiasi-asosiasi informal yang umumnya kuat dan memiliki nilai-nilai, norma, dan etika kolektif sebagai sebuah komunitas yang saling berhubungan. Hal ini merupakan modal sosial yang dapat mendorong munculnya organisasi organisasi modern dengan prinsip keterbukaan, dan jaringan jaringan informal dalam masyarakat yang secara mandiri dapat mengembangkan pengetahuan dan wawasan dengan tujuan peningkatan kesejahteraan dan kualitas hidup bersama dalam kerangka pembangunan masyarakat.

2. Masyarakat berkepercayaan-rendah (*low-trust*)

Dalam konteks pembangunan ekonomi melalui peningkatan *e commerce* di Indonesia, Konsumen sebagai modal sosial mempunyai pengaruh yang besar sebab beberapa dimensi pembangunan manusia sangat dipengaruhi oleh modal sosial antara lain kemampuan untuk menyelesaikan kompleksitas berbagai permasalahan bersama, mendorong perubahan yang cepat di dalam masyarakat, menumbuhkan kesadaran kolektif untuk memperbaiki kualitas hidup dan mencari peluang yang dapat dimanfaatkan untuk kesejahteraan. Hal ini terbangun oleh adanya rasa saling mempercayai, tindakan proaktif, dan hubungan internal eksternal dalam membangun jaringan sosial didukung oleh semangat kebajikan untuk saling menguntungkan sebagai refleksi kekuatan masyarakat. Situasi ini akan memperbesar kemungkinan percepatan perkembangan individu dan kelompok dalam masyarakat tersebut. Bagaimanapun juga kualitas individu akan mendorong peningkatan kualitas hidup masyarakat itu berarti pembangunan manusia paralel dengan pembangunan sosial.

Dalam pembelian dan penjualan dari internet juga bisa memberikan peluang tertipu oleh pelaku usaha. Para *konsumen* dalam pelaksanaan *e commerce* akan memilih pelaku usaha yang jujur. Pelaku usaha harus

pintar pintar dalam mengolah modal sosial yang berupa jaringan sosial konsumen agar menjadi pilihan para konsumen. Dalam mengolah modal sosial ada hal penting yang dimiliki salah satunya adalah menumbuhkan *Trust* pada konsumen.

Pelaku usaha harus mampu berupaya untuk membuat dirinya peka pada tindakan yang diambil oleh konsumen berdasarkan pada rasa kepercayaan dan tanggung jawab. *Trust* yang dibangun pelaku usaha diharapkan dapat membuat penilaian positif atas hubungan seseorang dengan orang lain yang akan melakukan transaksi tertentu menurut harapan orang kepercayaannya dalam suatu lingkungan yang penuh ketidak-pastian. Pada kondisi tersebut *Trust* yang dimiliki konsumen adalah kepercayaan konsumen terhadap pelaku usaha dalam melakukan hubungan transaksi berdasarkan suatu keyakinan bahwa pelaku usaha yang dipercayainya tersebut akan memenuhi segala kewajibannya secara baik sesuai yang diharapkan.

Hingga saat ini Indonesia belum memiliki *Trustmark* yang menjamin konsumen pengguna *e commerce* di Indonesia. Meskipun di dalam Peraturan Pemerintah Nomer 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik telah di amanatkan tentang keberadaan Lembaga Sertifikasi Keandalan namun hingga saat ini pemerintah belum memiliki regulasi khusus atau Peraturan Pemerintah yang mengatur mengenai keberadaan *Trustmark* yang dapat membantu pemerintah untuk membangun keterpercayaan konsumen pengguna *e commerce* di Indonesia. Pelaku Usaha *e commerce* di Indonesia saat ini masih menggunakan *Trustmark* dari Luar Negeri yang tentu saja hanya dapat dilakukan oleh Pelaku Usaha yang besar dan tidak dapat menjangkau pelaku usaha kecil di Indonesia yang juga membutuhkan jaminan keterpercayaan untuk konsumen.

Faktor yang membentuk kepercayaan konsumen di Indonesia terhadap transaksi *e commerce* terdiri atas kemampuan (*ability*), kebaikan hati (*benevolence*), dan integritas (*integrity*) *commit to user*.

a. Kemampuan (*Ability*)

Kemampuan mengacu pada kompetensi dan karakteristik pelaku usaha dalam mempengaruhi konsumen. Dalam hal ini, bagaimana pelaku usaha mampu menyediakan, melayani, sampai mengamankan transaksi dari gangguan pihak lain. Artinya bahwa konsumen memperoleh jaminan kepuasan dan keamanan dari penjual dalam melakukan transaksi. *Ability* ini meliputi kompetensi, pengalaman, pengesahan institusional, dan kemampuan dalam ilmu pengetahuan. Hingga saat ini hanya konsumen yang sadar akan hak-hak nya dan memahami karakteristik *e commerce* yang mampu melakukan seleksi atas informasi yang diberikan oleh pelaku usaha. Belum semua pelaku usaha dalam *e commerce* memberikan jaminan kepuasan dan keamanan bagi konsumen khususnya bagi *Bisnis to Customer* dan *Customer to Customer*.

b. Kebaikan hati (*Benevolence*)

Kebaikan hati merupakan kemauan pelaku usaha dalam memberikan kepuasan konsumen yang saling menguntungkan antara dirinya dengan konsumen. Profit yang diperoleh pelaku usaha dapat dimaksimumkan, tetapi kepuasan konsumen juga tinggi. Pelaku usaha bukan semata-mata mengejar profit maksimum, melainkan juga memiliki perhatian yang besar dalam mewujudkan kepuasan konsumen. Hingga saat ini salah satu faktor ketidakpercayaan konsumen terhadap pelaku usaha adalah tidak adanya aturan hukum yang jelas mengenai *e commerce* secara otomatis hanya pelaku usaha yang memiliki etika bisnis yang baik yang akan memiliki kepedulian atau empati terhadap kepentingan kepuasan konsumen. Sedangkan pelaku usaha yang tidak memiliki etika bisnis yang baik tetap akan bergantung pada penegakan hukum *e commerce* yang hingga saat ini belum ada titik terangnya.

c. Integritas (*Integrity*)

Integritas merupakan perilaku pelaku usaha dalam menjalankan bisnisnya. Informasi yang diberikan kepada konsumen apakah benar

sesuai dengan fakta atau tidak. Kualitas produk yang dijual apakah dapat dipercaya atau tidak. *Integrity* ini dapat dilihat dari sudut kewajaran (*fairness*), pemenuhan (*fulfillment*), kesetiaan (*loyalty*), keterus-terangan (*honestly*), keterkaitan (*dependability*), dan kehandalan (*reliabilty*). Tidak banyak pelaku usaha yang secara detail memberikan informasi atas produk barang atau jasa yang ditawarkan hal ini terlihat dari beberapa *website* baik *Bisnis to customer* maupun *customer to customer*, pelaku usaha tersebut tidak melakukan *update atas website* yang digunakan sebagai media informasi untuk konsumen. Pelaku usaha juga tidak memberikan fasilitas testimoni konsumen serta tidak memberikan garansi atas keamanan data pribadi konsumen dan *wanprestasi* serta tidak adanya jaminan penyelesaian sengketa dan ganti rugi.

Tidak terpenuhinya unsur-unsur pembentuk keterpercayaan konsumen pada *e commerce* membuat pemerintah semakin sulit untuk menumbuhkan *e commerce* di Indonesia. Pemerintah memerlukan kerja extra untuk merubah budaya masyarakat tradisional dan mindset konsumen serta menumbuhkan keterpercayaan konsumen pada bisnis *e commerce*.

Konsumen merupakan modal sosial yang dapat dipandang sebagai investasi untuk mendapatkan sumberdaya baru dalam masyarakat. Modal sosial ini merupakan salah satu komponen utama dalam menggerakkan kebersamaan, mobilitas ide, saling kepercayaan dan saling menguntungkan untuk mencapai kemajuan bersama melalui peningkatan *e commerce*. Modal sosial memegang peranan yang sangat penting dalam memfungsikan dan memperkuat kehidupan masyarakat modern. Konsumen sebagai modal sosial merupakan syarat yang harus dipenuhi bagi pembangunan manusia, pembangunan ekonomi, sosial, politik dan stabilitas demokrasi. Permasalahan dan penyimpangan yang terjadi di berbagai negara utamanya adalah minimnya modal sosial yang tumbuh di tengah masyarakat. Modal sosial yang lemah akan meredupkan semangat

gotong royong, memperparah kemiskinan, meningkatkan pengangguran, kriminalitas, dan menghalangi setiap upaya untuk meningkatkan kesejahteraan penduduk²⁸⁷

Berdasarkan beberapa kasus yang dihadapi konsumen *pengguna e commerce* di Indonesia, dapat disimpulkan bahwa pengetahuan tinggi yang dimiliki konsumen akan menghasilkan kepercayaan yang tinggi, namun kepercayaan yang rendah belum tentu membuat kepercayaan konsumen pada *e commerce* juga rendah. Kepercayaan bisa terjadi dikarenakan konsumen tidak mengetahui akan resiko dan hanya terbius oleh reputasi atau tampilan visual yang interaktif dan menarik meskipun konsumen belum pernah memiliki pengalaman interaksi sebelumnya.

Masyarakat Indonesia sangat mudah meletakkan kepercayaan kepada pelaku usaha untuk melakukan transaksi *e commerce* dikarenakan ketidaktahuan dan ketidakpahaman terhadap mekanisme *e commerce* serta implikasi dari transaksi *e commerce*. Kondisi ini membuka peluang perilaku curang yang dilakukan oleh pelaku usaha, disisi lain Kemetrin koinfo dan Kementrian perdagangan hingga saat ini belum ada data kongkrit jumlah pelaku usaha *e commerce* yang menggunakan *website*. Belum adanya regulasi *e commerce* yang secara spesifik mengatur hak dan kewajiban pelaku usaha dalam *e commerce* mengakibatkan kendala dalam penegakan hukum.

Upaya pelaku usaha *e commerce* untuk meningkatkan keterpercayaan konsumen adalah adanya inisiatif dari organisasi pelaku usaha maupun lembaga swasta yang membuat verifikasi dan sertifikasi bagi anggotanya dengan cara memberikan *Trustmark* pada *website* situs anggota organisasi pelaku usaha tersebut.

Beberapa negara asean yang tergabung dalam *The Asia-Pacific Trustmark Alliance* (ATA) sekarang menjadi *World Trustmark Alliance* (WTA) memberikan wacana bahwa *Trustmark* bukan hal baru mengingat di negara-negara maju lain sudah mewajibkan semua pelaku usaha *e commerce* menggunakan *Trustmark* pada situs mereka. Salah satu alasan diambilnya

commit to user

²⁸⁷ *Ibid*, hlm 54

Malaysia dan Singapura dalam perbandingan regulasi perlindungan konsumen *e commerce* karena secara geografis Indonesia berdekatan dengan Malaysia dan Singapore, selain itu *Trustmark* yang berlaku di Malaysia dan Singapore di inisiasi oleh Pemerintah dan cenderung otoriter sehingga pemerintah juga menjadi salah satu *Trustmark Provider*. Hal ini juga yang akan diterapkan di Indonesia bahwa pemerintah melalui Kementrian Kominfo membuka peluang bagi profesional independen untuk membuat Lembaga Sertifikasi Keandalan.

Keberadaan regulasi yang mengatur mengenai Lembaga Sertifikasi Keandalan nantinya dapat menjadi payung hukum pengamanan sistem informasi nasional dan merupakan wujud kepedulian pemerintah dalam hal keamanan informasi. Upaya pemerintah ini tidak dapat dilakukan secara efektif tanpa satu kesatuan rencana administrasi, fisik dan teknis yang matang.

