



Secure Data Center, BCP, DRC and Data Retention

An information security regulation strategic perspective

IC-SIRTII

UU 11/2008 ITE: Reliability

- + Inside the Information and Electronic Transaction Law Number 11/2008: BAB IV (Chapter IV), Bagian Kedua (Section Two), Pasal 15 (Article 15)
- + Sub Section (1): *"Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya"*
- + Electronic Systems Provider must responsible to conduct an , appropriate, reliable, secure operation of Electronic Systems

UU 11/2008 ITE: Min. Requirement

- + Pasal 16 (1): Sepanjang tidak ditentukan lain oleh UU tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:
 - a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
 - b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
 - c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;
 - d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
 - e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

UU 11/2008 ITE: Min. Requirement

- + Article 16 (1): To the extent not otherwise provided by separate legislation, each Provider shall operate the Electronic Systems that meet the following minimum requirements:
 - a. to display the back of Electronic Information and / or Electronic Records as a whole in accordance with the retention period specified by legislation;
 - b. to protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information in the Provision of Electronic Systems;
 - c. to operate in accordance with the procedures or instructions in the Provision of Electronic Systems;
 - d. equipped with procedures or instructions announced by the language, information, or symbol that can be understood by the parties concerned with the Provision of Electronic Systems; and
 - e. have a sustainable mechanism to maintain the novelty, clarity, and accountability procedures or instructions.

UU 11/2008 ITE: Mandated Govt. Act

- + Pasal 16 (article 16) Sub Section (2): *"Ketentuan lebih lanjut tentang Penyelenggaraan Sistem Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah"*
- + Further provisions on the Implementation of Electronic System referred to in paragraph sub section (1) regulated by Government Regulation
- + mandated to the government to prepare Information and Electronic Transaction Provider Government Act (RPP PITE)

RPP PITE (Draft): BCP

- + Inside the Information and Electronic Transaction Provider Government Act (Draft): BAB V (Chapter V), Bagian Kedua (Section Two), Pasal 24 (Article 24)
- + Sub Section (2): *"Setiap Penyelenggara Sistem Elektronik untuk pelayanan publik wajib menjalankan perencanaan keberlangsungan kegiatan untuk menanggulangi gangguan atau bencana sesuai dengan risiko dari dampak yang ditimbulkannya"*
- + Electronic System Provider for public service (i.e. banks) shall have continuity plan to overcome disruption or disaster in accordance with the risk of impacts

RPP PITE (Draft): Data Center

- + Inside the Information and Electronic Transaction Provider Government Act (Draft): BAB V (Chapter V), Bagian Kedua (Section Two), Pasal 24 (Article 24)
- + Sub Section (3): *"Setiap Penyelenggara Sistem Elektronik untuk pelayanan publik yang mengoperasikan pusat data wajib menempatkan pusat data dan pusat pemulihan bencana yang dioperasikannya di wilayah Indonesia"*
- + Electronic System Providers for public service (i.e. banks) should operate and place the data centers and disaster recovery centers within Indonesia territory

Why It Should Be Regulated?

- + Transaction occurred within Indonesia law jurisdiction
- + Using Indonesia electronic system and infrastructure
- + Involving Indonesia citizens and/or people lives in Indonesia
- + Exchange of money, goods and services in Indonesia
- + Data and information related to Indonesian interest

Main Issues: Applied To Whom?

- + It's not for banks and/or financial sectors only
- + Aimed to all sectors providing electronic transaction
- + It might be affecting to many others sector: Central & local govt; Public services private & government sector; Defense, security, civil public order sector; Natural resources, oil and gas, energy sector; Public transportation, land, sea/water & air; Banking, investment, capital, finance sector; Education & public health sector; Trade, industry, state owned enterprise sector; Telecommunication, media & broadcasting; Art, culture & tourism;
- + There will be many implications and consequences

Main Issues: Retention of The Data

- + Retention period, with data portion to be stored, how to manage availability, integrity, authenticity, confidentiality accessibility (different regulation in each sector)
- + Foreign institution: retention of data portion copy/duplicate vs full local retention which is need double storage/investment
- + Data relay (co-location, virtual, cloud) vs full physical local data center infrastructure including data retention and DRC
- + Appropriate guidelines and procedures and authorized staff needed to obtain data properly and to ensure compliance

Main Issues: BCP and DRC

- + Compliance to international standards
- + Quality and operation procedures assurance
- + Assessment (pre), monitoring (during) and audit (post)
- + Should be applied to all sector (equal treatment)

Main Issues: Law Enforcement

- + Different kind of data requirement, rules and procedures: court order, wiretapping/lawful interception, transaction and correlation analysis, in depth search/data mining, etc.
- + LEA: Anti Corruption Commission, National Police, Financial Transaction Reports & Analysis Centre, Attorney at General, Anti Drugs, Anti Terrorism, etc. Sector Regulatory: Central Bank, Telco's, Public Transportation, Energy etc.
- + Cross border jurisdiction and international collaboration
- + Procedures declaration to obtain data retention from each government/sector regulator and/or LEA are needed

Main Issues: Local Data Centers

- + National interest: to improve economy, domestic IT industry and IT infrastructure, job opportunities, knowledge and skills, IT market, regional IT investment competitiveness etc.
- + Infrastructure development strategic: local data centers will encourage the placement of content that will increase data traffic that is needed to establish domestic exchange point (it will help us to save national foreign exchange reserve)
- + Growth of local data traffic means investment attraction
- + Data privacy, infosec and law enforcement jurisdiction

What's Missing?

- + National standards and regulations establishment and/or adoption on Secure Data Center and DRC facility, i.e.:
 - + **TIA-568 Wiring Standards, TIA-942 Data Center Standards**
 - + **SAS 70, SSAE 16, SOC and Data Center Auditing Standards**
 - + **Data Center Star Audit (DCSA), ISO, ECO, SOX, HIPAA, etc.**
- + Professional independent agency to evaluate technical design, operation procedures and to administer periodic assesment, inspection and accreditation (compliance audit)
- + Mutual recognition amongs counterpart regulations

New Article Proposed in RPP PITE

- + More details on data retention related issues
- + DC, BCP and DC standards and regulations
- + Law enforcement procedures and technical guidelines
- + Clear reward and punishment statement clause

Thank You

- + Ravindo Tower 17th Floor
- + Kebon Sirih Raya, Kav. 75
- + Central Jakarta, 10340
- + Phone +62 21 3192 5551 ; Fax +62 21 3193 5556
- + info@idsirtii.or.id ; www.idsirtii.or.id