PERLINDUNGAN DATA PRIBADI

Anwar Siregar

18 Agustus 2020

CBQA GLOBAL
We Inspire in Trust

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

ABOUT ME

- More than 10 year at certification and auditing businesses
- Lead Auditor base on ISO/IEC 27001
- Lead Auditor base on ISO/IEC 20000
- Lead Auditor base on ISO 50001
- Lead Auditor base on ISO 55001
- Lead Assessor Indeks KAMI at BSSN (*use to be at Kominfo)
- Lead Tutor IRCA UK
- Lead Tutor Data Privacy and ISO Standards

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

PERATURAN DATA PRIBADI

- Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.
- UU No. 36 Tahun 2009 tentang Kesehatan - Pasal 57 ayat (1) UU Kesehatan “Setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan.” Namun UU Kesehatan memberikan pengecualian terhadap: a. perintah undang-undang; b. perintah pengadilan; c. izin yang bersangkutan; d. kepentingan masyarakat; atau e. kepentingan orang tersebut
- Peraturan Menteri Kesehatan RI No. 4 Tahun 2018 tentang Kewajiban Rumah Sakit dan Kewajiban Pasien (Permenkes 4/2018). Pasal 17 ayat (1) Permenkes 4/2018 bahwa RS berkewajiban untuk menghormati dan melindungi hak Pasien. Salah satu hak pasien yakni: mendapatkan privasi dan kerahasiaan penyakit yang diderita termasuk data medisnya
- Peraturan Menteri Kesehatan RI No. 269 / MENKES / PER / III / 2008 tentang Rekam Medis (Permenkes 269/2008)
- Peraturan Menteri Kesehatan RI No. 269 / MENKES / PER / III / 2008 tentang Rekam Medis

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

PERLINDUNGAN DATA PRIBADI

Berita

- Data warga terkait Covid-19 di Indonesia diduga telah dicuri oleh **peretas (hacker).** Mereka diduga menjual data pasien terinfeksi virus corona tersebut di forum dark web RapidForums
- Data-data warga yang dijual itu terbilang lengkap, antara lain **nama, status kewarganegaraan, tanggal lahir, umur, nomor telepon, alamat rumah, Nomor Identitas Kependudukan (NIK**), dan alamat **hasil tes corona**.
- Hasil tes Covid-19 juga muncul secara detail dalam basis data tersebut. Data yang dijual berupa **gejala, tanggal mulai sakit, dan tanggal pemeriksaan**

https://www.cnnindonesia.com/teknologi/20200620083944-192-515418/230-ribu-data-pasien-covid-19-di-indonesia-bocor-dan-dijual

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

PERLINDUNGAN DATA PRIBADI

Berita

- Perhimpunan Rumah Sakit Seluruh Indonesia (Persi) menjelaskan bahwa 230 ribu data pasien virus corona atau Covid-19 yang dikabarkan bocor menjadi tanggung jawab Kementerian Kesehatan (Kemenkes). Sebab, pihak rumah sakit telah melaporkan semua data pasien secara berjenjang dan berakhir di Kementerian Kesehatan
- Data pasien tersebut disimpan dalam bentuk digital dan manual. "Di beberapa rumah sakit, klinik, Pusat Kesehatan Masyarakat (Puskesmas) belum cukup baik, ada yang semuanya dapat disimpan digital, ada juga manual, dan masih ada kemungkinan bocor,"

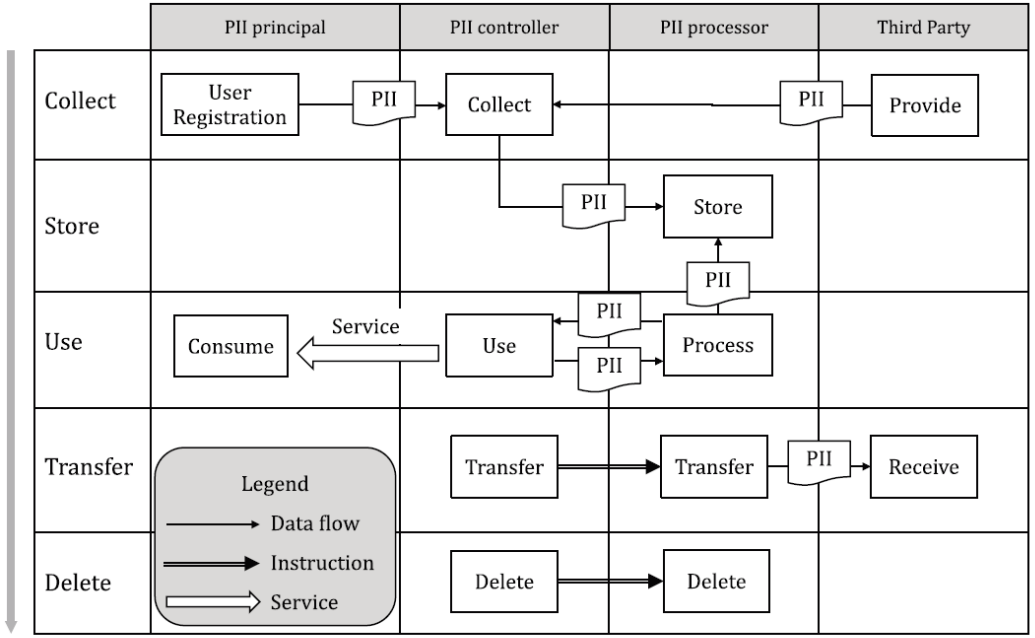
https://katadata.co.id/yuliawati/digital/5f02f85af052d/data-pasien-covid-19-bocor-dianggap-tanggung-jawab-kemenkes

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

DATA PRIVACY LIFE CYCLE

D.1 Workflow diagram of the PII processing

Figure D.1 shows an example workflow of the PII processing (according to 6.4.1).



NOTE The instruction and service in Figure D.1 are used in a way to express a certain quality of data flow.

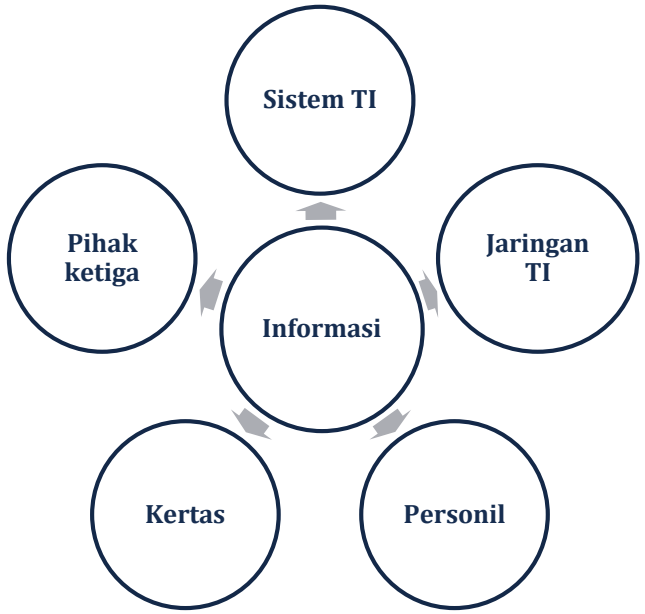
- PII — Personal Identifiable Information
- PII Principal — Natural person / Individual to whom the PPI relates
- PII Controller — Privacy stakeholders that determine the purpose and means for processing the PII
- PII Processor — Privacy stakeholders that process PII on behalf and accordance to the PII Controller

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

INFORMASI / DATA PRIBADI

Jenis :

- Kertas
- Hard disk
- Flash Disk
- Video
- Percakapan
- Gambar (*Design)



PENGAMANAN INFORMASI adalah penjagaaan terhadap kerahasian , integritas dan ketersedian informasi

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

LIFE CYCLE DATA DI SEKTOR KESEHATAN – GO DIGITAL

Pengumpulan Data (Collect)	Penyimpanan Data (Store)	Penggunaan Data (Use)	Perpindahan Data (Transfer)	Penghapusan Data (Delete)
Kertas	Ruang Arsip	**Kertas**	Kertas	Shredder ~~Buang Tempat Sampah~~ Bakar
Aplikasi **Website** **E-mail**	**Laptop** **USB** **Server** **Cloud**	**Laptop** **USB** **Aplikasi** **Website**	**Aplikasi** **Website** **E-mail** **USB**	**Format** **Delete** **Destroy** **HD/Server**

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

DATA PRIVACY RISK / PRIVACY IMPACT ASSESSMENT – ISO 29134

Assets	Action	Privacy risk	Examples of threats
Paper documents	Spionase	Illegitimate accesses to the PII	Reading; photocopying; photographing, etc.
Paper documents	Hilang	Disappearances of PII	Theft of documents; loss of files during a move; disposal, etc.
Hardware	Abnormal use	Disappearances of PII	Storage of personal files; personal use, etc.
Hardware	Spionase	Illegitimate accesses to the PII	Watching a person's screen without them knowing while on the train; taking a photo of a screen; geolocation of hardware; remote detection of electromagnetic signals, etc.
Software	Abnormal use	Unwanted changes in the PII	Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data, etc
Software	Abnormal use	Disappearances of PII	Erasure of data; use of counterfeit or copied software; operator errors that delete data, etc.
Individuals	Abnormal use	Illegitimate accesses to the PII	Influence (phishing, social engineering, bribery, etc.); pressure (blackmail, psychological harassment, etc.), etc.
Computer	Overload	Disappearances of PII	Misuse of bandwidth; unauthorized downloading; loss of Internet connection, etc.

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

DATA PRIVACY RIGHTS

1. TO BE INFORMED
2. TO ACCESS
3. TO OBJECT
4. TO ERASURE OR BLOCKING
5. TO DAMAGES
6. TO FILE A COMPLAINT
7. TO RECTIFY
8. TO DATA PORTABILITY

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

ISO/IEC 27001:2013 (ISO/IEC 27002) CONTROLS

No	Security Clause Headings	Security Category	Control
A.5	Kebijakan Keamanan Informasi	1	2
A.6	Organisasi Keamanan Informasi	2	7
A.7	Keamanan Sumber Daya Manusia	3	6
A.8	Manajemen Aset	3	10
A.9	Pengendalian Akses	4	14
A.10	Kriptografi	1	2
A.11	Keamanan Fisik dan Lingkungan	2	15
A.12	Keamanan Operasional	7	14
A.13	Keamanan Komunikasi	2	7
A.14	Akuisisi, pengembangan & pemeliharaan sistem	3	13
A.15	Hubungan dengan *supplier*	2	5
A.16	Manajemen Insiden Keamanan Informasi	1	7
A.17	Aspek Keamanan Informasi dalam BCM	2	4
A.18	Kepatuhan	2	8

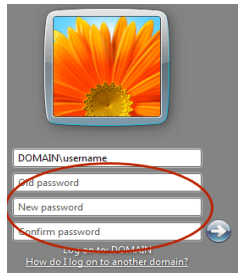
114 Controls

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

HOW TO MANAGE DATA PRIVACY

Registered Asset

Anti Virus



Licensed Software

Encrypted Confidential Data

Auto Lock if not used

Password

USB Port Closed/Scan

Configure Privacy and Security

Do Not Remember Password

Whitelist website

Site Setting

Log Activity

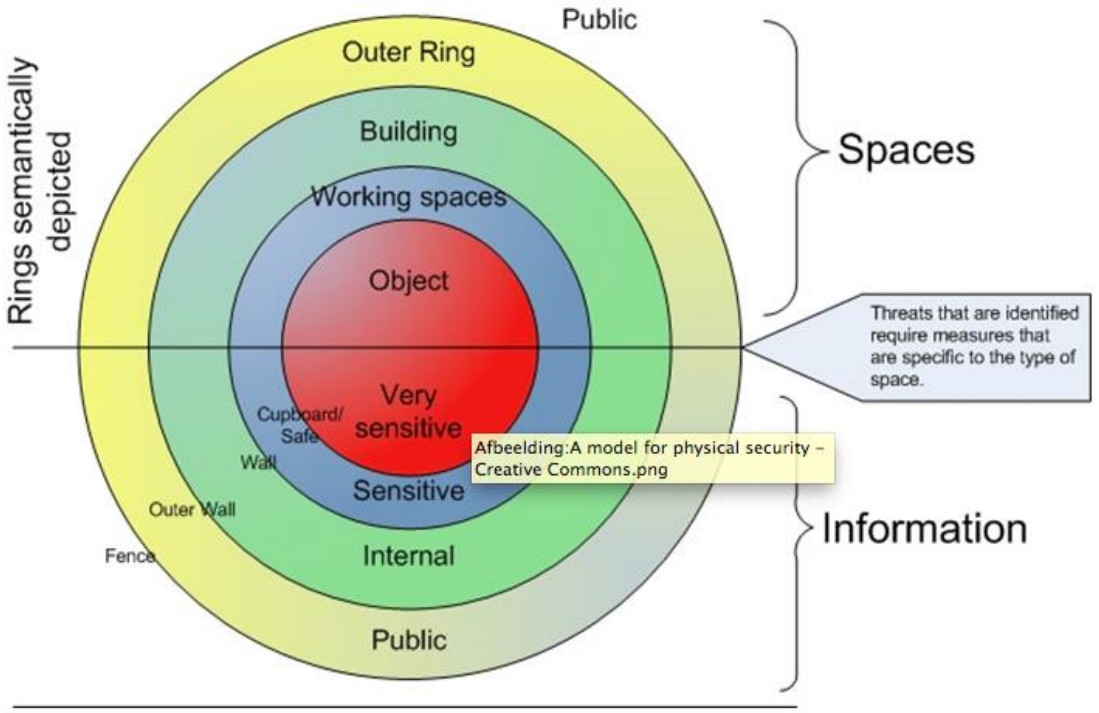
Permission Access

Whitelist website

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

PASSWORD, CLEAN DESK , SECURE AREA

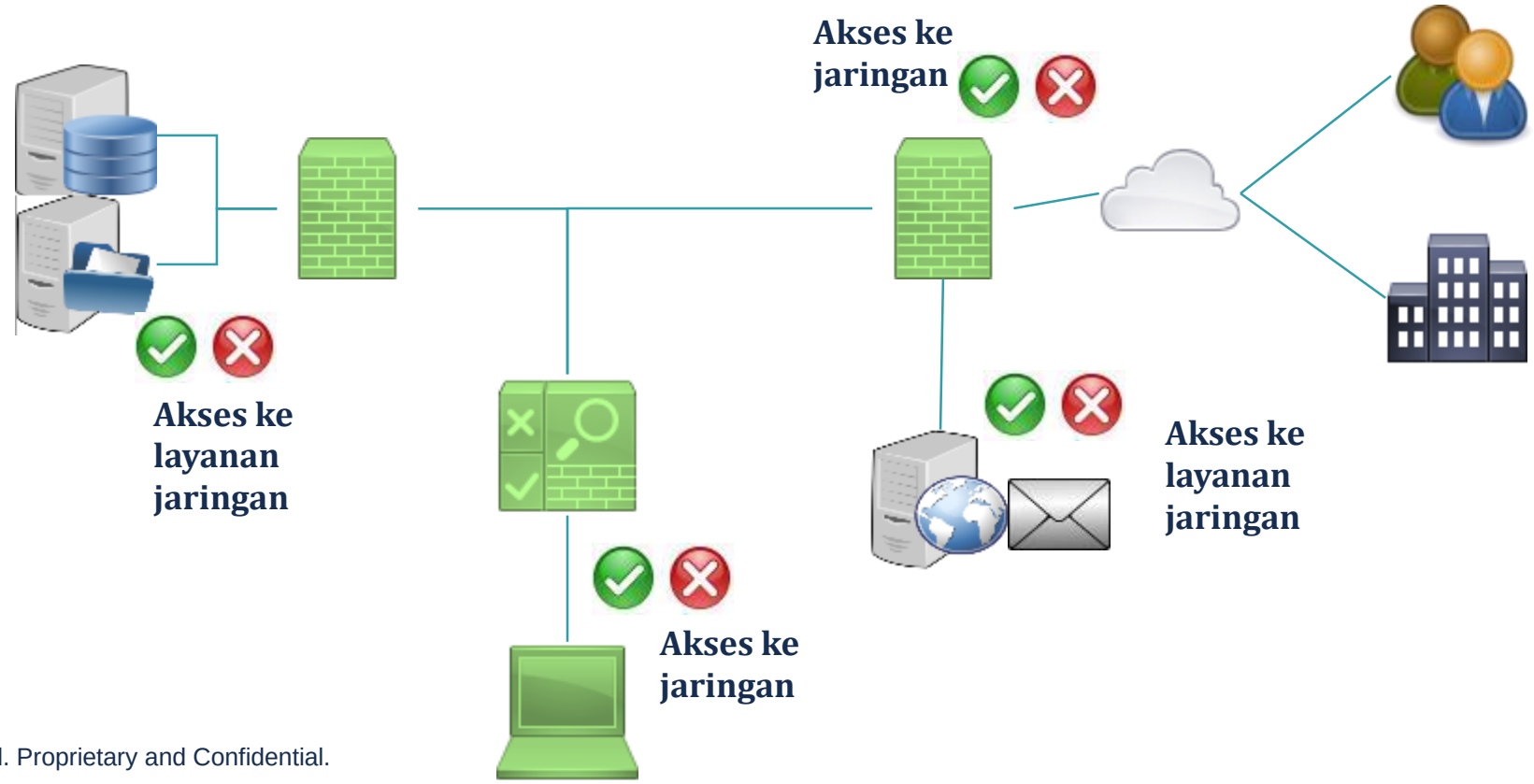
- Select a good one
- At least 7 characters
- Mixture of upper and lowercase characters
- Mixture of alpha and numeric characters
- Don’t use dictionary words
- Keep passwords safe
- Change them often
- Don’t share or reuse passwords
- Two-factor authentication



Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

ACCESS RIGHT

- Only allow access that is absolutely required
- Don’t grant accounts based on the fact that access “may” be required
- Use least privilege access policies that state access will only be granted if required, not by default
- Are accounts removed and passwords changed when someone changes jobs or is terminated?
- Perform audits



Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

DATA PRIVACY STANDARD

Mandatory di Indonesia

Mandatory di Negara Lain

- ISO/IEC 27018
- ISO/IEC 27701
- ISO/IEC 29151

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

BAGAIMANA PERLINDUNGAN DATA PRIBADI YANG BAIK

1. Menerapkan dan tersertifikasi standard ISO/IEC 27001:2013 sebagai minimum standard sesuai regulasi
2. Melakukan Privacy Impact Assessment ISO/IEC 29134:2017
3. Menerapkan control ISO/IEC 27002:2013
4. Menjadikan pengelolaan data Pribadi yang aman merupakan ***budaya*** organisasi

INGAT !!!!

KEAMANAN DATA PRIBADI BUKAN BUAT MEREKA

MELAINKAN

UNTUK KITA !!!

Copyright CBQA Global © 2020 All rights reserved. Proprietary and Confidential.

CBQA GLOBAL

We inspire in trust

info@cbqaglobal.com

www.cbqaglobal.com