CYBER LAW CHALLENGES IN THE POST-PANDEMIC ERA: DATA PROTECTION AND PRIVACY

Lecture at the School of Strategic and Global Studies (SKSG), Universitas Indonesia, 22 October 2021

ASSOC. PROF. DR. SONNY ZULHUDA
International Islamic University Malaysia

sonny@iium.edu.my
sonnyzulhuda.com
twitter.com/zulhuda

Agenda

01 The Pandemic Check

02 New Cyberspace Intensity

03 The Global New Norms

04 Key Issues and Challenges

05 Lessons Learned

THE PANDEMIC

REALITY CHECK

sonnyzulhuda.com

Covid-19 Statistics as of 20 Oct 2021

PANDEMIC

Twenty-two months and counting...

241 million

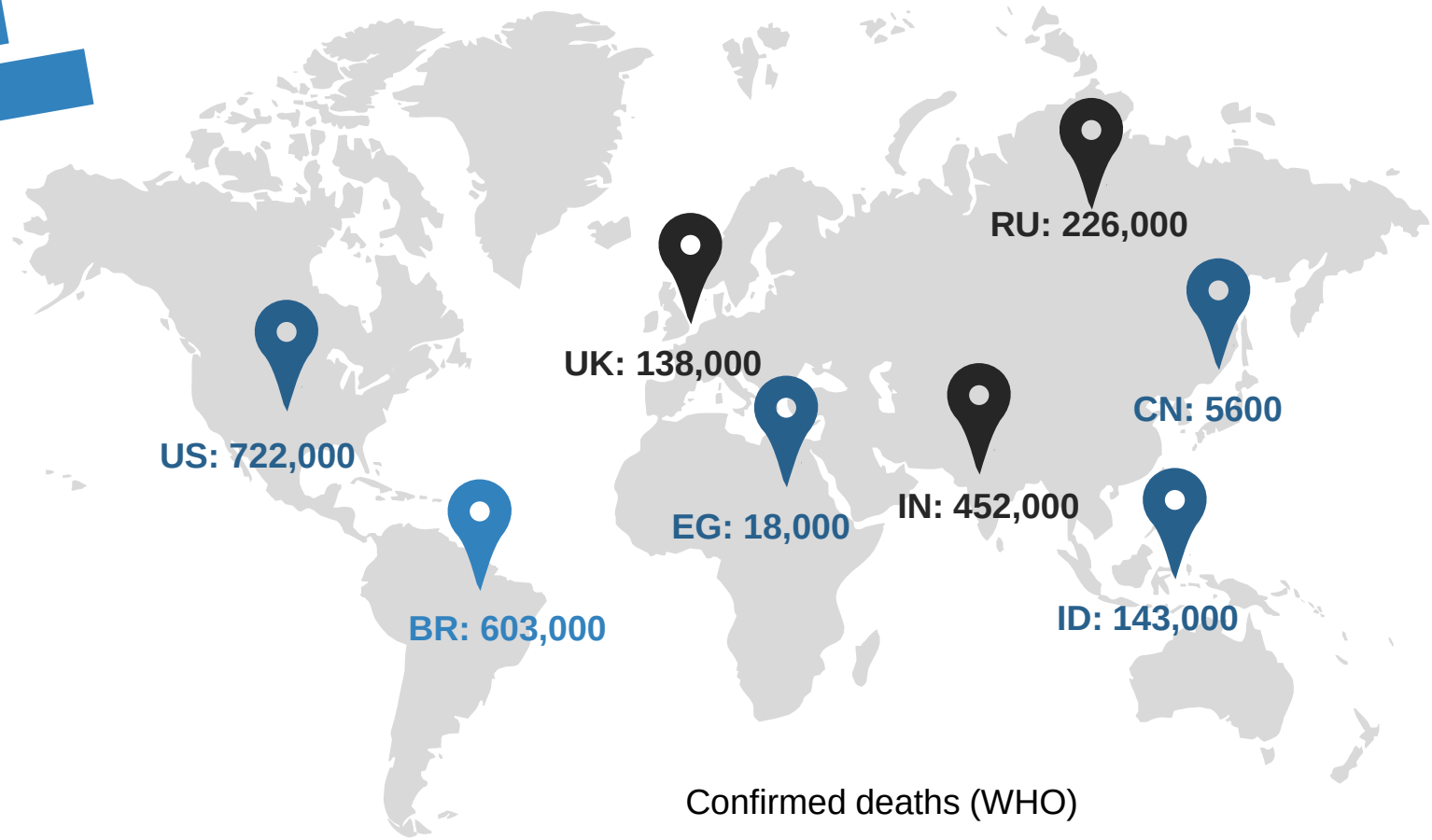
Confirmed cases

4.91 million

Confirmed deaths

220

Countries, areas or territories with cases



Confirmed deaths (WHO)

Let´s stay at home

- **HEALTH CONCERNS:** intensified reporting, patients tagging, scheduled control, body temp scanning, contact tracing, high-risk people identification
- **POLICY MEASURES:** Governments impose movement restriction, isolation, lockdown, surveillance, curfew, quarantine and border control
- **NEW NORM:** Physical distancing and its ramifications. New way of Work, Learn, Shop, Meet, Business from Home
- **BRING ABOUT**: Social, Psychological, Technical, Public Trusts, Business and Governance **VULNERABILITIES**

Pandemic-created Vulnerabilities

INFORMATION

TECHNICAL

FINANCIAL

TRUST

People tend to **rush collecting** information about the Pandemic, click on links and web pages, spreading the information with **poor exercise of fact-checking**

People work on **official documents** using home-based computers, with **inadequate security protection** and support as they have in office.

Reduced mobility, **losing jobs**, scarcity of earning opportunities, etc. creates financially challenged society, who would **turn into shortcuts (crimes, etc)**.

Wide and fast **adoption of mobile Apps** for social networking, e-shopping, e-meeting, e-learning and cloud services, but with poor **security and privacy measures** or policies

Pandemic-created Vulnerabilities

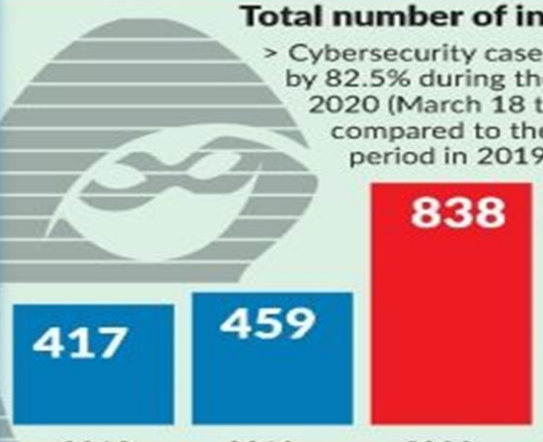
PANDEMIC

COVID-19

Beware of cyberattacks!

Total number of incidents

> Cybersecurity cases increased by 82.5% during the MCO 2020 (March 18 to April 7) compared to the same period in 2019.



Tips to stay safe online

Working from home

> Update all systems including Virtual Private Networks (VPN) and devices with the latest security patches
> Alert employees about phishing attempts.
> Avoid logging in to your work environment using public Internet Wi-Fi. Connect through your home or mobile network data.
> Enable Multi Factor tication

Covid-19 scams

> Always verify information from emails, text messages and social media posts about Covid-19.
> Do not share personal or financial information in emails
> Do not click on suspicious links provided to you on Covid-19, verify with the sender or agencies that can help.
> Use legitimate, government websites for up-to-date, fact-based information

Video teleconferencing apps

> Use the latest version of apps and security software
> Only download software from its official website or app store.
> Never share confidential information during a meeting
> Enable non-recordable videos and audio, and limit file sharing.
> If something is suspicious, log out.
> If you lose your computer or mobile phone, log out from all clients immediately and change your login password.
> Do not share or publish the confer
> Log out from the app after a meeting.

Source: CyberSecurity Malaysia

Pandemic-created Vulnerabilities

PERFORMANCE IMPROVEMENT PARTNERS
an ERIE STREET company

The United States declares its first case of COVID-19, cyber attacks go up **48%**

30TH JANUARY

Multiple states in the US declare a public emergency; cyber attacks go up **64%**

» 29TH FEBRUARY

The country of Italy goes into lockdown, attacks go up **28%**

» 8TH MARCH

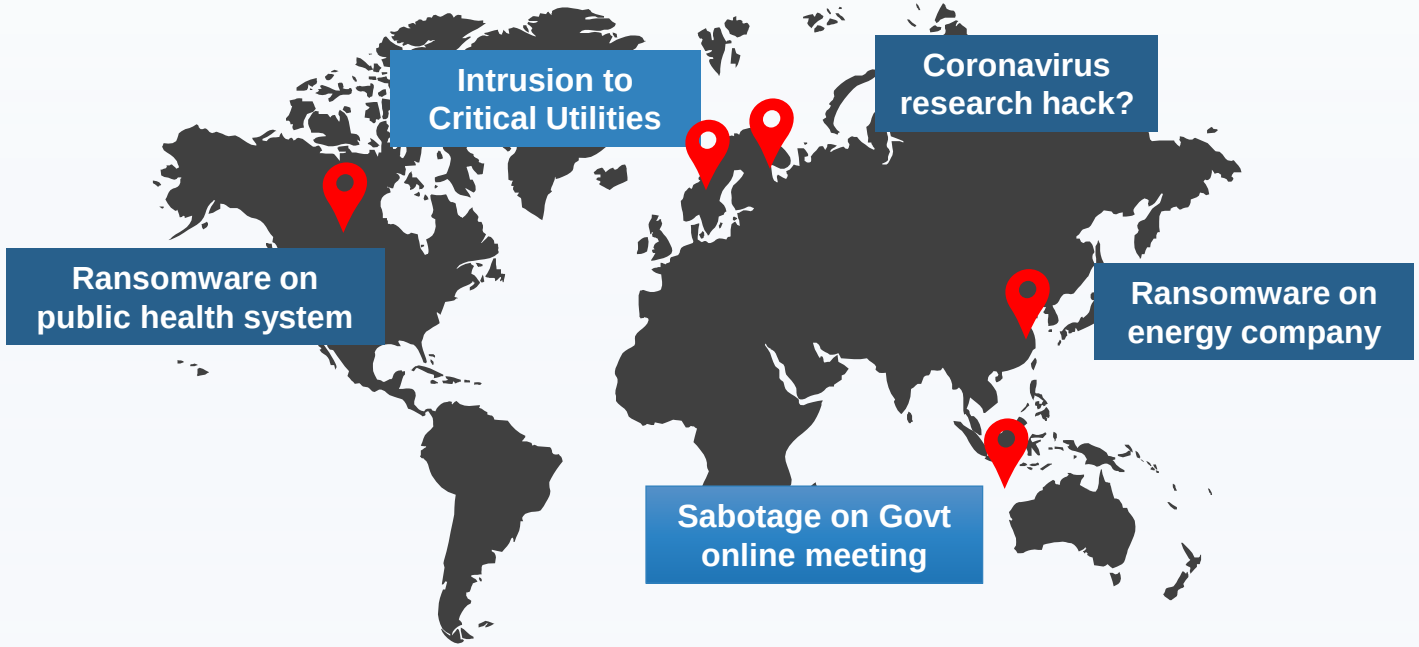
The World Health Organization declares COVID-19 a pandemic, cyber attacks go up **22%**

» 11TH MARCH

Data source: Computer Weekly via Carbon Black

Exploitation of Cyber Information Infrastructure (CIIP)

What had happened in the Cyberspace during Covid-19 Crisis?



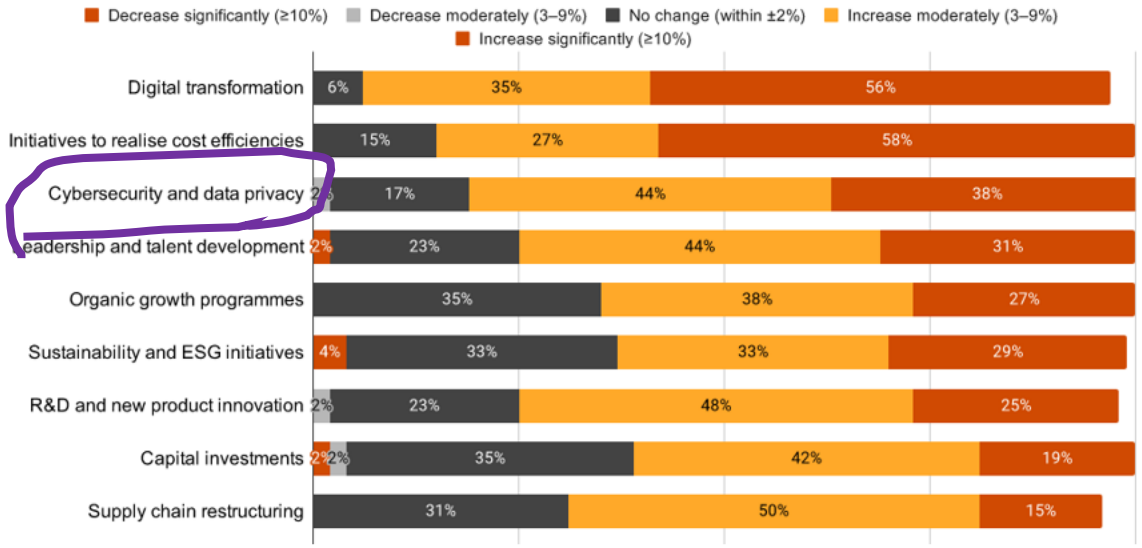
Terrorists and cybercriminals are always interested to exploit cyberspace vulnerabilities. The activity of cyber terrorism does not relax during Covid-19. Several cyber attacks do target a critical information infrastructure (CII), a traditional target for cyber terrorism.

PRIVACY RISKS

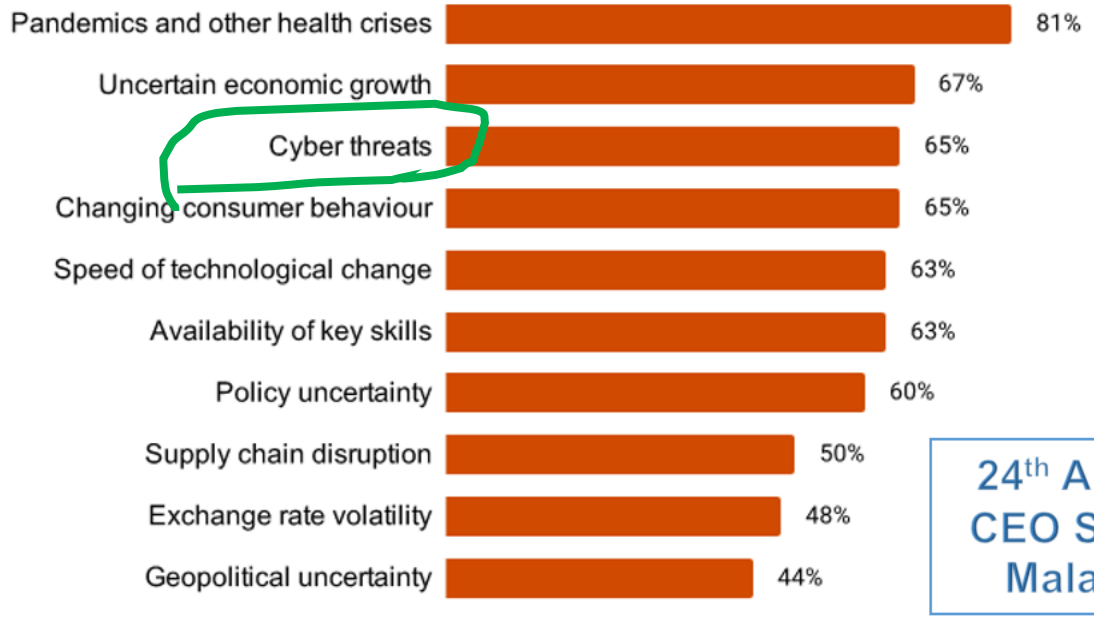
THE NEW INTENSITY

sonnyzulhuda.com

Investment due to COVID-19 crisis (Malaysia)

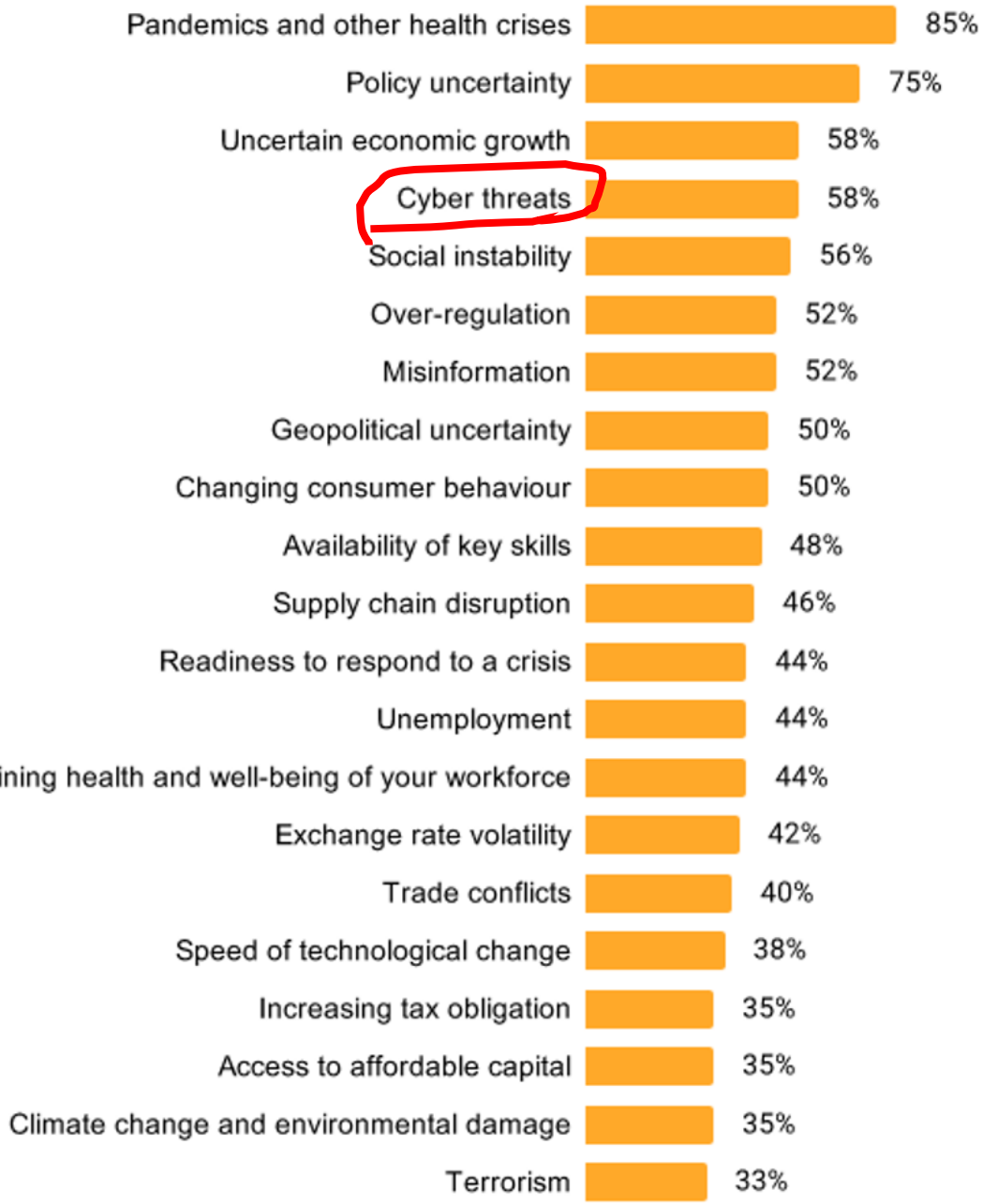


Top threats considered in strategic risk management



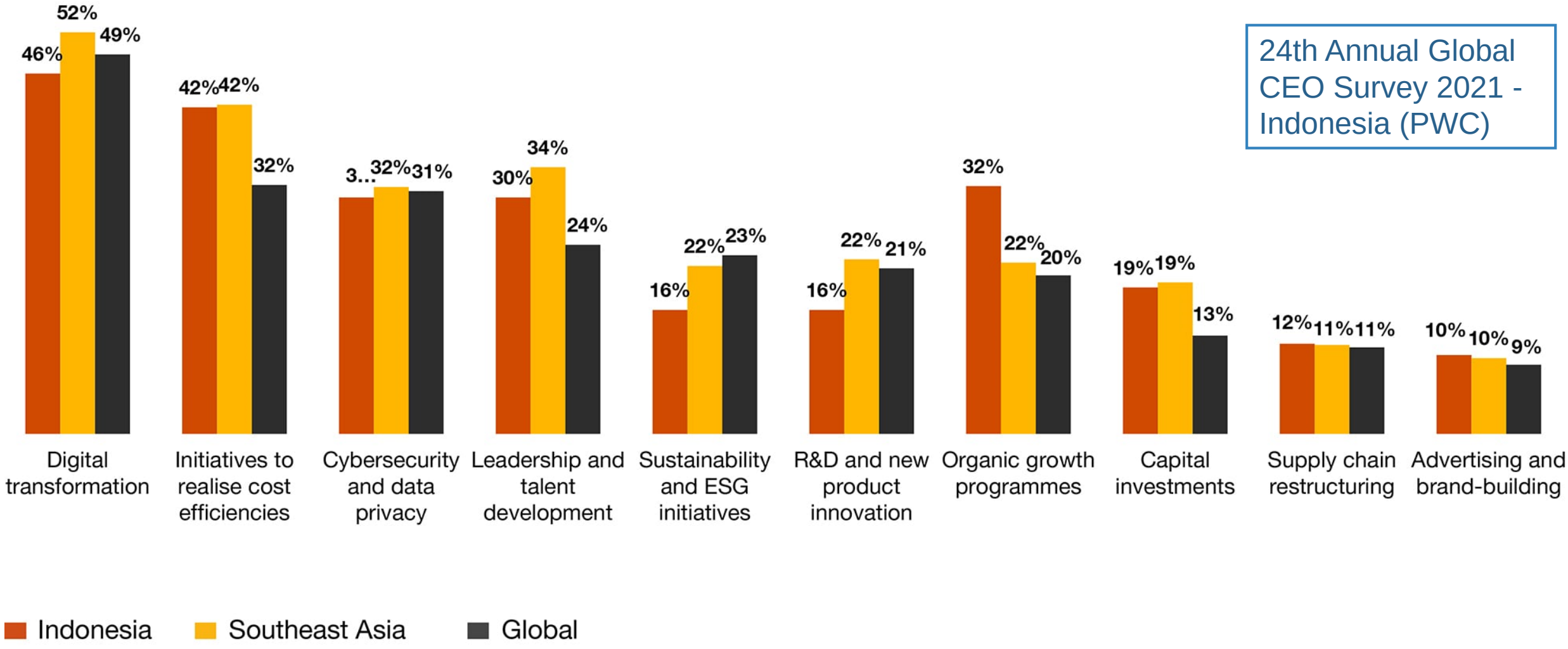
24th Annual Global CEO Survey 2021 – Malaysia (PWC)

Top potential threats to organizations in Malaysia

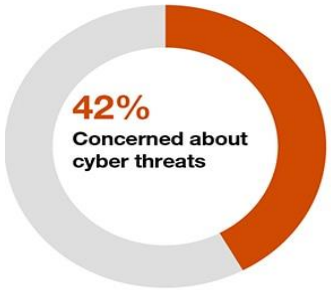


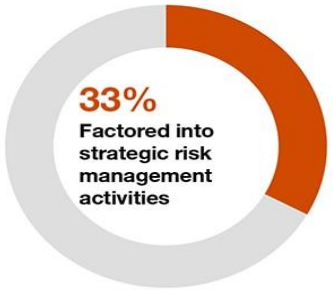
How much specific issues raised companies' long-term investment after Covid-19 crisis?

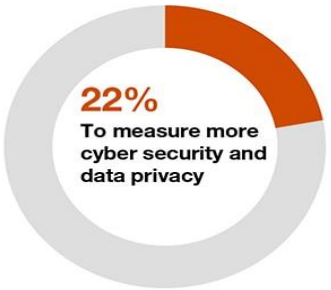
24th Annual Global CEO Survey 2021 - Indonesia (PWC)

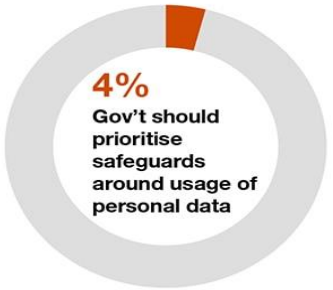


Indonesia

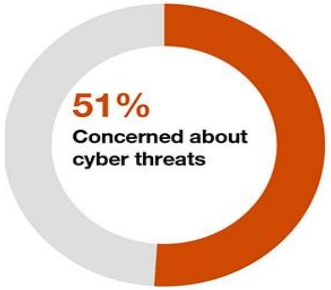


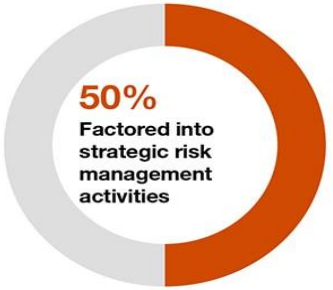


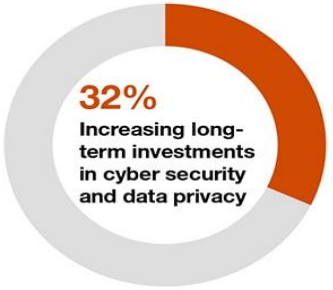


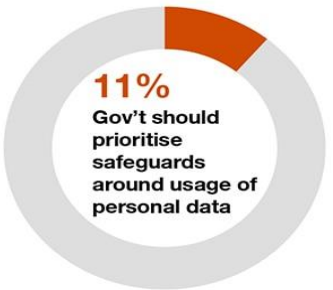


Southeast Asia

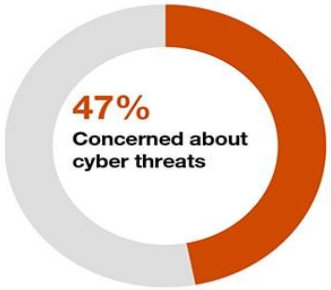


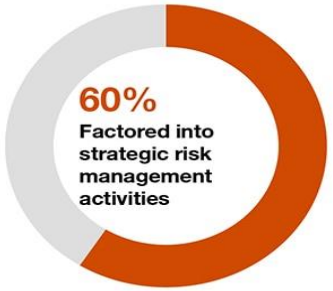


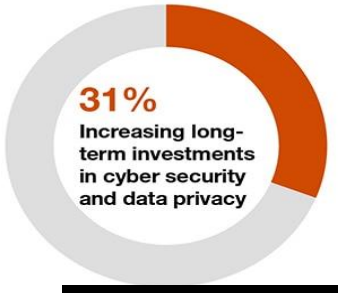




Global

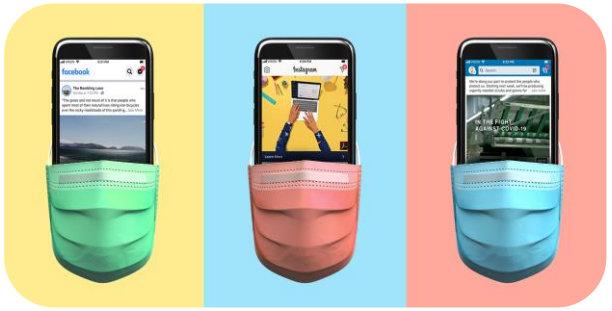






24th Annual Global CEO Survey 2021 (PWC)

Emerging Privacy Risks post-Pandemic



Personal data exploitation through **illicit collections** via online services (eg P2P lending), Apps, etc;

Scam via fake accounts begging for donation, fake charity drives, fake emergencies etc.

Misinformation: citizen journalism with unaccountable stories – a test-bed for phishing attacks.

Unsecured online platforms prone to personal data breaches (online shopping, online meeting, social media, etc).

The rise of **surveillance** and Private data collection?

Data Breach Incidents – in the past two years*

BPJS Kesehatan
Badan Penyelenggara Jaminan Sosial

komisi pemilihan umum

eHAC Indonesia
Health Quarantine MoH Indonesia

Lazada

facebook
Indonesia

BRIlife

tokopedia

bukalapak

BHINNEKA

RedDoorz

kreditplus
PT. KB FINANSIA MULTI FINANCE

https://nasional.kompas.com/read/2021/09/03/18445501/deretan-kasus-kebocoran-data-pribadi-dalam-dua-tahun-terakhir

PRIVACY RULES

THE GLOBAL NEW NORMS

sonnyzulhuda.com

Data Privacy as Epicenter of Global Disputes

NSA SURVEILLANCE OVER THE US AND GLOBAL INTERNET USERS (SNOWDEN SAGA) — **2013**

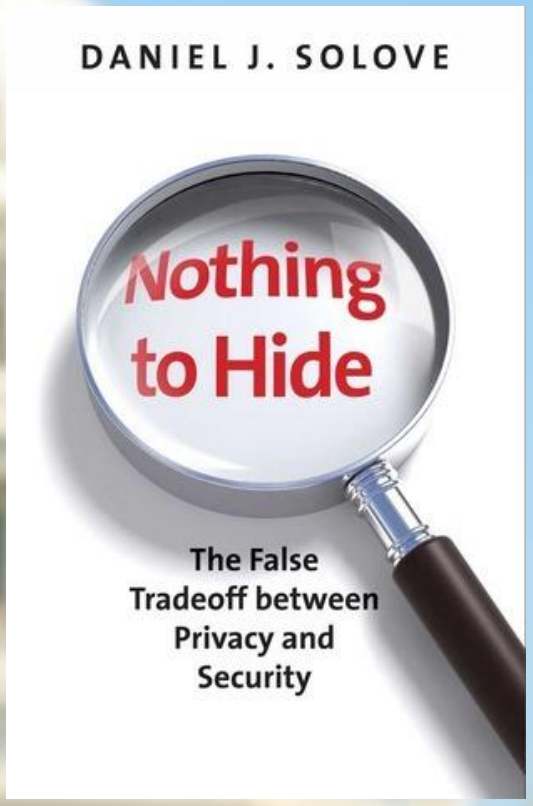
FACEBOOK UNDER GLOBAL PRESSURE AFTER DATA MISUSE BY CAMBRIDGE ANALYTICA — **2017**

EU COURT ANNULLED EU-US AGREEMENT ON DATA TRANSFER — **2020**

PRES TRUMP BANNED CHINA-OWNED WECHAT AND TIKTOK IN THE US OVER PRIVACY CONCERNS — **2020**

Who is interested to your Data?

1. BIG Brother
2. BIG Data Aggregator
3. BIG Fans!



15 JULY 2020 – Trans-Atlantic Trade Issue

The EU Court of Justice decided that the EU-USA Privacy Shield Agreement, which allows 3000 US companies to repatriate European personal data to US, is null and void, putting trans-Atlantic trade in a halt

6 AUG 2020 – Sino-American Trade Issues

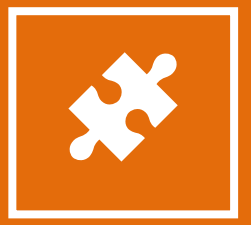
The US Government banned Chinese platforms TikTok and Wechat from operating in the US **due to data security and data privacy concern**.

APEC Privacy Framework (2015)

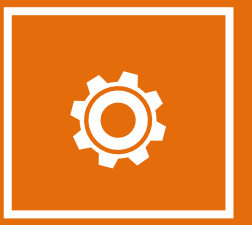
Preventing Harm

Notice

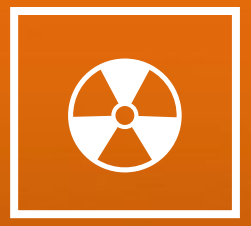
Collection Limitations



Uses of Personal Information



Choice



Integrity of Information

Security Safeguards

Access and Correction

Accountability

European Union (EU) General Data Protection Regulation 2016

Fines of up to 4% of turnover
Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million.

Breach notification within 72 hrs
Breaches must be reported within 72 hours of first having become aware of the breach.

Increased territorial scope
Applies to any company processing personal data of EU citizens, regardless of location.

Privacy by design
Data protection from the onset of the designing of systems, rather than a retrospective addition.

Consent matters
Explicit consent must be provided in an intelligible and easily accessible form.

Right to be forgotten
Entitles the data subject to have the data controller erase his/ her personal data (and potentially third parties, too).

Right to access and portability
Users can inquire whether and how their personal data is being processed.

Mandatory data protection officers
Appointed in certain cases, to facilitate the company's need to demonstrate GDPR compliance.

G-20: Osaka Track on Data Free Flow with Trust (DFFT) - 2019

Privacy & Data Protection Rules on the Global and Regional Timeline

1948
- UN UDHR

1953
- ECHR

1976
- ICCPR

1980
- OECD Guidelines

1981
- CoE Conv. 108

1995
- EU Directive

2000
- CFREU

2007
- Lisbon Treaty

2015
- APEC Privacy Framework

2016
- EU GDPR

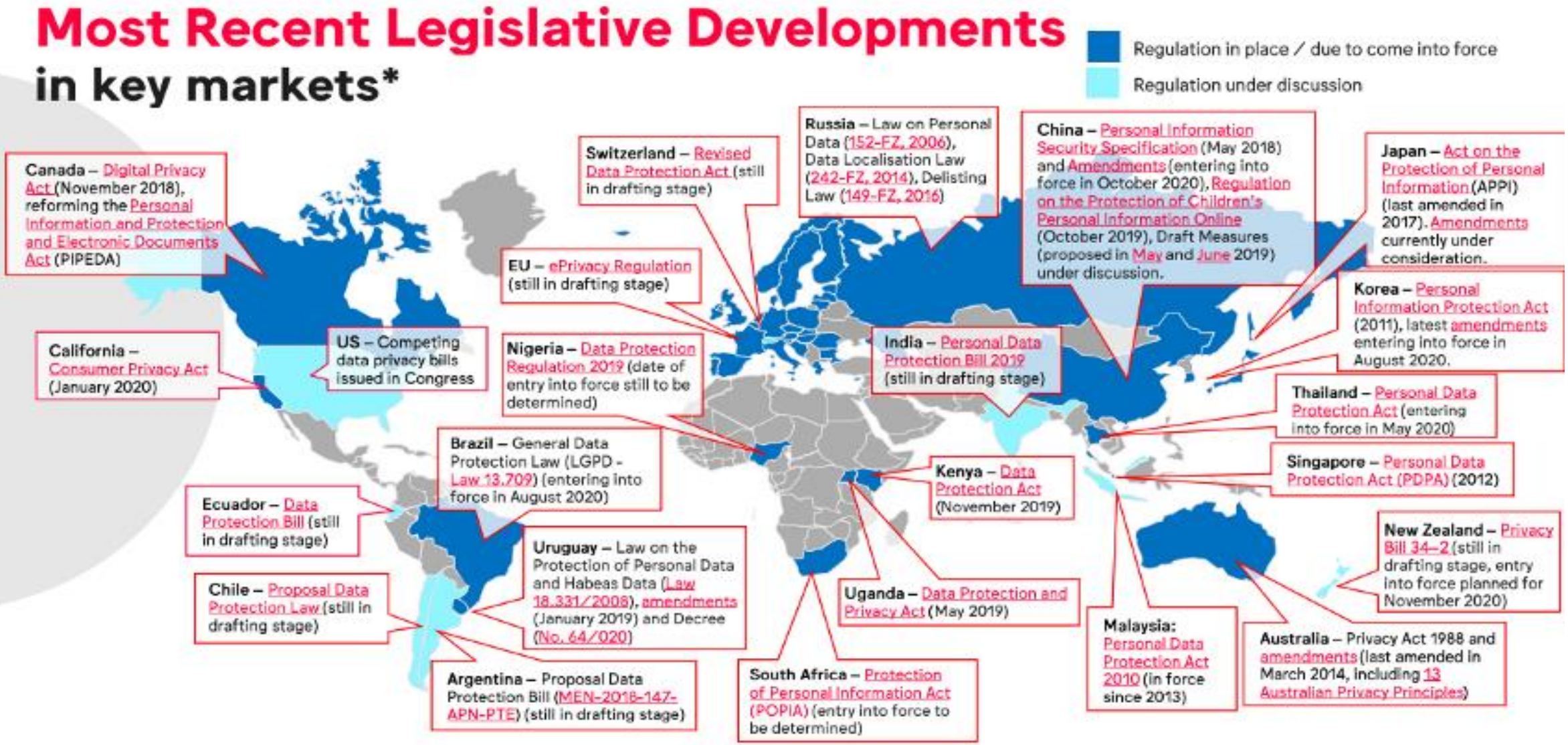
2016

ASEAN Framework on PDP

2020

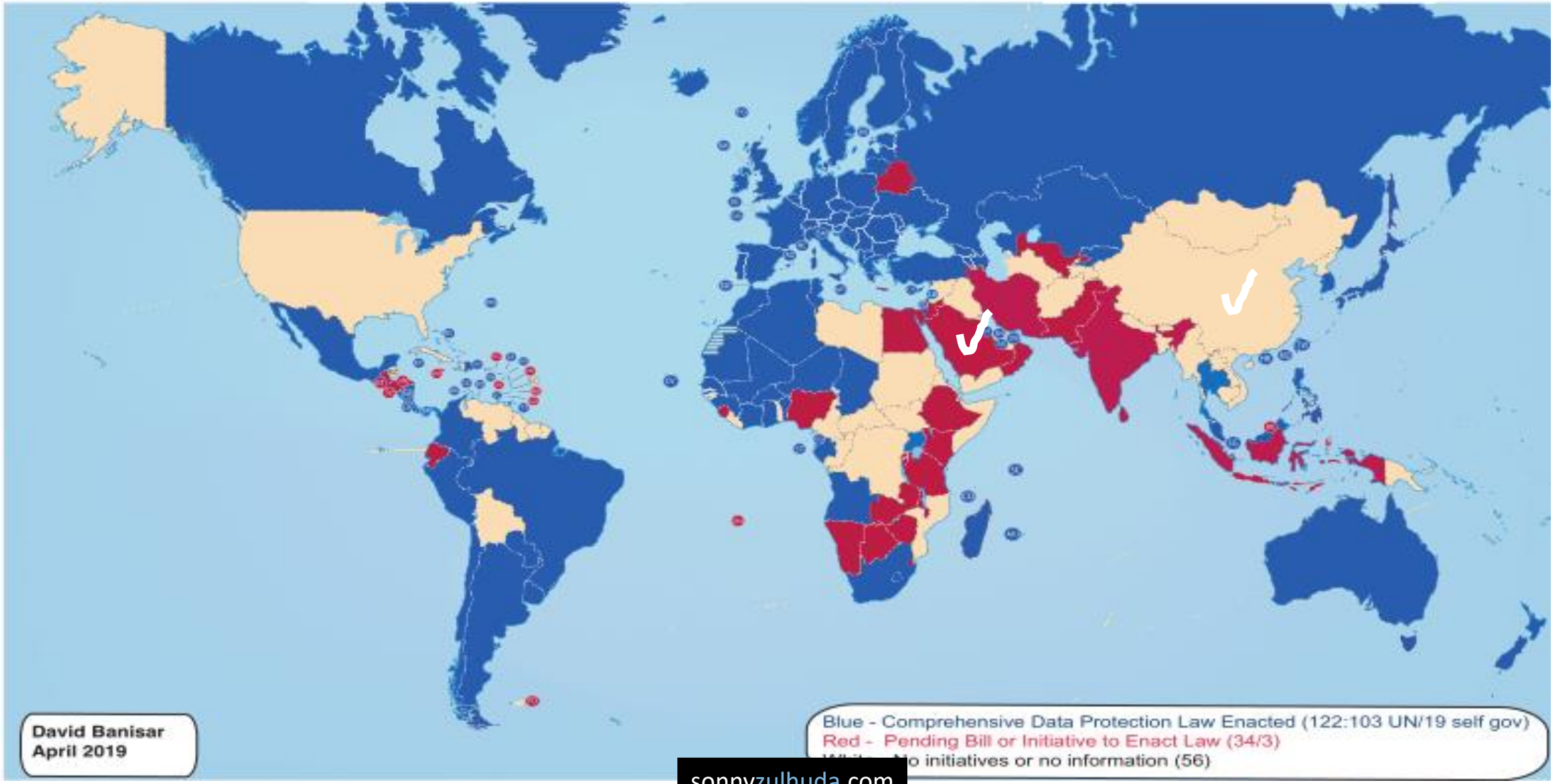
RCEP Agreement

A Quick Check on Other Jurisdictions



https://medium.com/credify/data-regulations-for-business-743c69ee327b

National Comprehensive Data Protection/Privacy Laws and Bills 2019



PDP LAW

KEY ISSUES OF DATA PROTECTION

Data Protection Principles in Indonesian Draft PDP Law – Article 17(2)

a. The collection of personal data shall be limited, specific, lawful, fair and transparent.

b. Personal data shall be processed only for the purpose it is collected.

c. Data is processed with ensuring rights of data subjects.

d. Personal data processed shall be accurate, complete, not misleading, update, and accountable.

e. Personal data shall be protected from unlawful access, disclosure, and modification; and shall be protected against misuse, damage, and loss.

f. Data subject must be informed of the processing purpose and activities, and of any breach of data protection.

g. Personal data shall be disposed of/deleted after the end of retention time or as requested by the data subject.

h. Personal data processing shall be conducted responsibly in compliance of the principles of data protection principles.

Data Protection Principles in the European General Data Protection Regulation (GDPR) – Article 5

1. Lawfulness Principle – Art. 5(1)(a)
2. Fairness Principle – Art. 5(1)(a)
3. Transparency Principles – Art. 5(1)(a)
4. Purpose Limitation Principle – Art. 5(1)(b)
5. Data Minimisation – Art. 5(1)(c)
6. Accuracy Principle – Art. 5(1)(d)
7. Storage Limitation – Art. 5(1)(e)
8. Data Security (Integrity and Confidentiality) Principle – Art. 5(1)(f)
9. Accountability Principle – Art. 5(2)

Data Protection Principles in Indonesian Draft PDP Law – Article 17(2)

a. The collection of personal data shall be limited, specific, lawful, fair and transparent.

b. Personal data shall be processed only for the purpose it is collected.

c. Data is processed with ensuring rights of data subjects.

d. Personal data processed shall be accurate, complete, not misleading, update, and accountable.

e. Personal data shall be protected from unlawful access, disclosure, and modification; and shall be protected aganst misuse, damage, and loss.

f. Data subject must be informed of the processing purpose and activities, and of any breach of data protection.

g. Personal data shall be disposed of/deleted after the end of retention time or as requested by the data subject.

h. Personal data processing shall be conducted responsibly in compliance of the principles of data protection principles.

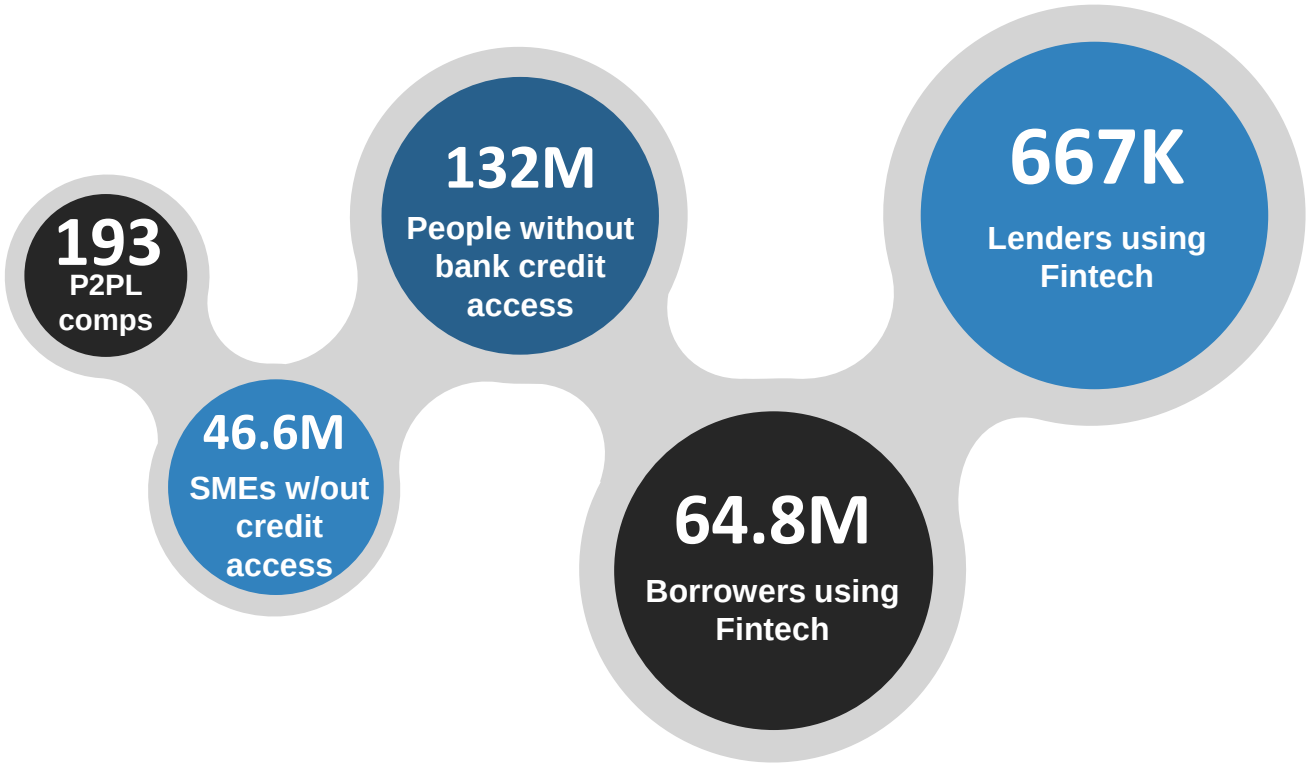
Data Protection Principles in the European General Data Protection Regulation (GDPR) – Article 5

1. Lawfulness Principle – Art. 5(1)(a)
2. Fairness Principle – Art. 5(1)(a)
3. Transparency Principles – Art. 5(1)(a)
4. Purpose Limitation Principle – Art. 5(1)(b)
5. Data Minimisation – Art. 5(1)(c)
6. Accuracy Principle – Art. 5(1)(d)
7. Storage Limitation – Art. 5(1)(e)
8. Data Security (Integrity and Confidentiality) Principle – Art. 5(1)(f)
9. Accountability Principle – Art. 5(2)

Fintech Lending Landscape in Indonesia

116
Registered Companies

77
Licensed Companies



Rp 221,000,000,000,000

Successfully distributed loan (Jun 2021)

Source: OJK, AFPI

Fintech Lending Landscape in Indonesia

The collection of personal data shall be limited, specific, lawful, fair and transparent.

In May 2019, a **German** police officer was fined by the country's Data Protection Authority EUR 1400 (Rp 23 million) for obtaining car license plate data via the official Central Traffic Information System of the Federal Motor Transport Authority and using it **for private contact**.

The police officer has processed personal data **outside the scope of the law**.

This infringement is attributable to him personally as he does not have sufficient legal basis for data processing contrary to Art. 6 GDPR.

Personal data shall be processed only for the purpose it is collected.

In September 2021, a restaurant owner in **Spain** was fined EUR 3,000 (he Spanish DPA (AEPD) has fined a bar owner EUR 3,000 (Rp 49 million) for distributing a CCTV **images through WhatsApp and online media** which shows an accident that involved one customer of the restaurant.

The CCTV was **meant for security purposes**, therefore the images/videos shall not be distributed publicly as it is not in line with the security purpose.

As the publication of the images was not related to the purpose of the video surveillance, the restaurant owner as data controller violated the Purpose Limitation principle under the GDPR.

Personal data shall be processed only for the purpose it is collected.

In April 2014, a **Malaysian** actress sued Malaysia Airlines over the publication of her flight details on a Facebook account. The posting of their boarding passes caused them to suffer emotional stress.

At the KL International Airport, the couple had given their boarding passes to the airliner staff at the departure gate. It appeared that the staff had subsequently taken the picture of the passes and uploaded them online.

In an out-of-court settlement, the couple received an undisclosed amount of compensation.

Legally, this would have potentially amounted to a violation of the purpose limitation principle of the PDP law.

Personal data shall be protected from unlawful access, disclosure, and modification; and shall be protected against misuse, damage, and loss.

A third party training vendor to **Singapore** Armed Forces was fined SGD 35,000 (Rp 367 million) in June 2021 for their **failure to apply security measures** to the data of more than 110,000 people in total.

- The database was affected by ransomware which locks up the data
- The vendor only applies a single, simple password, which was shared between few employees.
- Insufficient authentication method to protect the account from unauthorised log-ins.

Data subject must be informed of the processing purpose and activities, and of any breach of data protection.

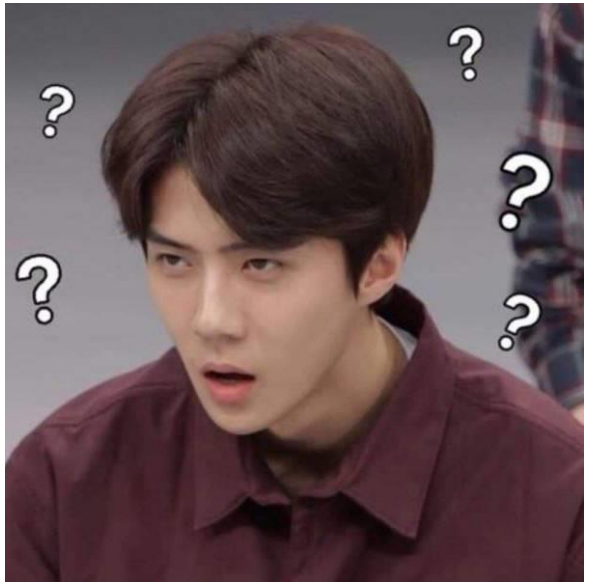
In June 2021, the authority in **Poland** imposed a fine of EUR 3,000 (Rp 49 milliono) on a legal education foundation.

The Foundation had earlier suffered from data breaches (i.e. data theft) and had **failed to notify the authority about the breach.**

The failure to notify the authority amounts to a violation of a breach notification duty. The data file that was stolen included the names, addresses and telephone numbers, and also the national ID numbers of 96 individuals.

Personal data processing shall be conducted responsibly in compliance of the principles of data protection principles.

1. The use of **P2P Lending customers'** personal information irresponsibly to intimidate the customers upon repaying their loan.
2. The **disclosure of Covid-19 patients** information without consent or necessary procedure.
3. **Discreet collection of facial information** from surveillance camera for commercial purposes.
4. Failure to **notify the detailed purposes** and usage of personal information collected from the Covid-19 tracking apps.



LESSON LEARNED

KEY TAKEAWAYS

PDP Law the New Norms

RESETTING DATA CULTURE

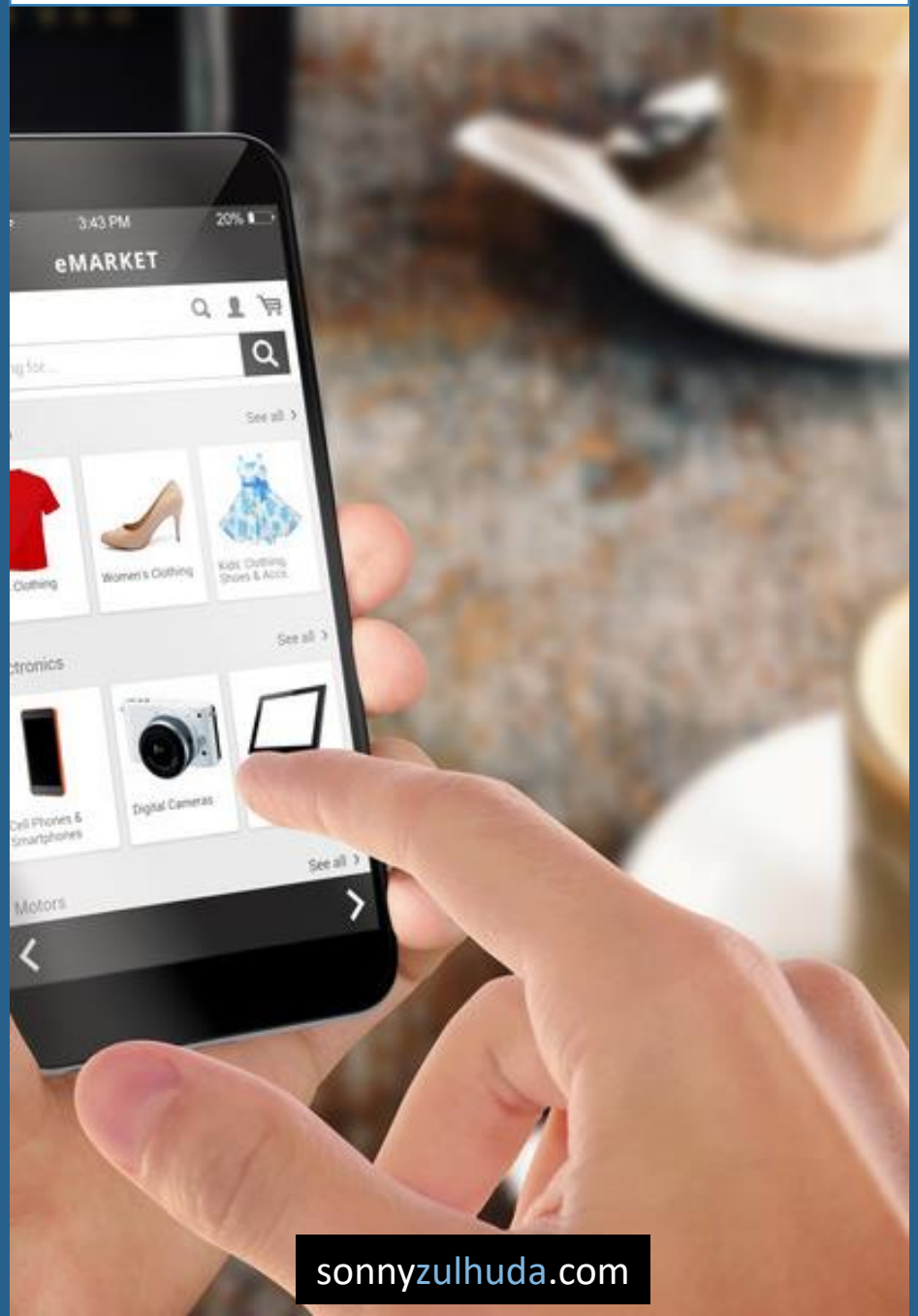
Information society requires a resetting of ethical and cultural adjustment towards data

DATA DUE DILIGENCE

Data is viewed as assets that have to be managed and protected within appropriate measurable steps

NEW OFFENCES

Restrictions are introduced to reshape the new expected behaviour on data



sonnyzulhuda.com

FULL DATA LIFECYCLE

PDP deals with the full processing from collection to disposal. Confidentiality or security is only a component of it.

DATA STAKEHOLDERS

Data Is not “owned” by the data user. Individuals’ rights are involved.

DATA ACCOUNTABILITY OVER SOVEREIGNTY

While it is important to preserve data sovereignty, data accountability is the priority

Key debates on Indonesian Draft PDP Law

Supervisory & Enforcement Authority?

Legal and Institutional Harmonisation

Ensuring efficient sanctions: Criminal, civil & administrative

Data Sovereignty

Closing Remarks

01 PDP Law is about respect and dignity of every human being – fundamental rights to privacy

02 PDP Law seeks to strengthen national security and economic resilience

03 PDP Law sets a new norm in international trade

04 PDP Law governs data across sectors and industries

05 PDP Law evolves, changes and complicates alongside the technology

THANK YOU

DR SONNY ZULHUDA

Associate Professor at the International Islamic University Malaysia

sonny@iium.edu.my

sonnyzulhuda.com

twitter.com/zulhuda