5 Regional Data Protection Trends in 2021

Jan 26, 2021

Kevin Shepherdson
CEO Straits Interactive
FIP, CIPP/E, CIPP/A, CIPM, CIPT, GRCP, Certified DPO (Exin)

William Hioe
Regional Head Consulting
Straits Interactive
FIP, CIPP/E, CIPP/A, CIPM, CIPT, GRCP, Certified DPO (Exin)

Lyn Boxall
Lyn Boxall LLC
FIP, CIPP/E, CIPP/A, CIPM, GRPC, GRCA, LLM, LLB

Publication

…provides practical solutions to current global privacy challenges/

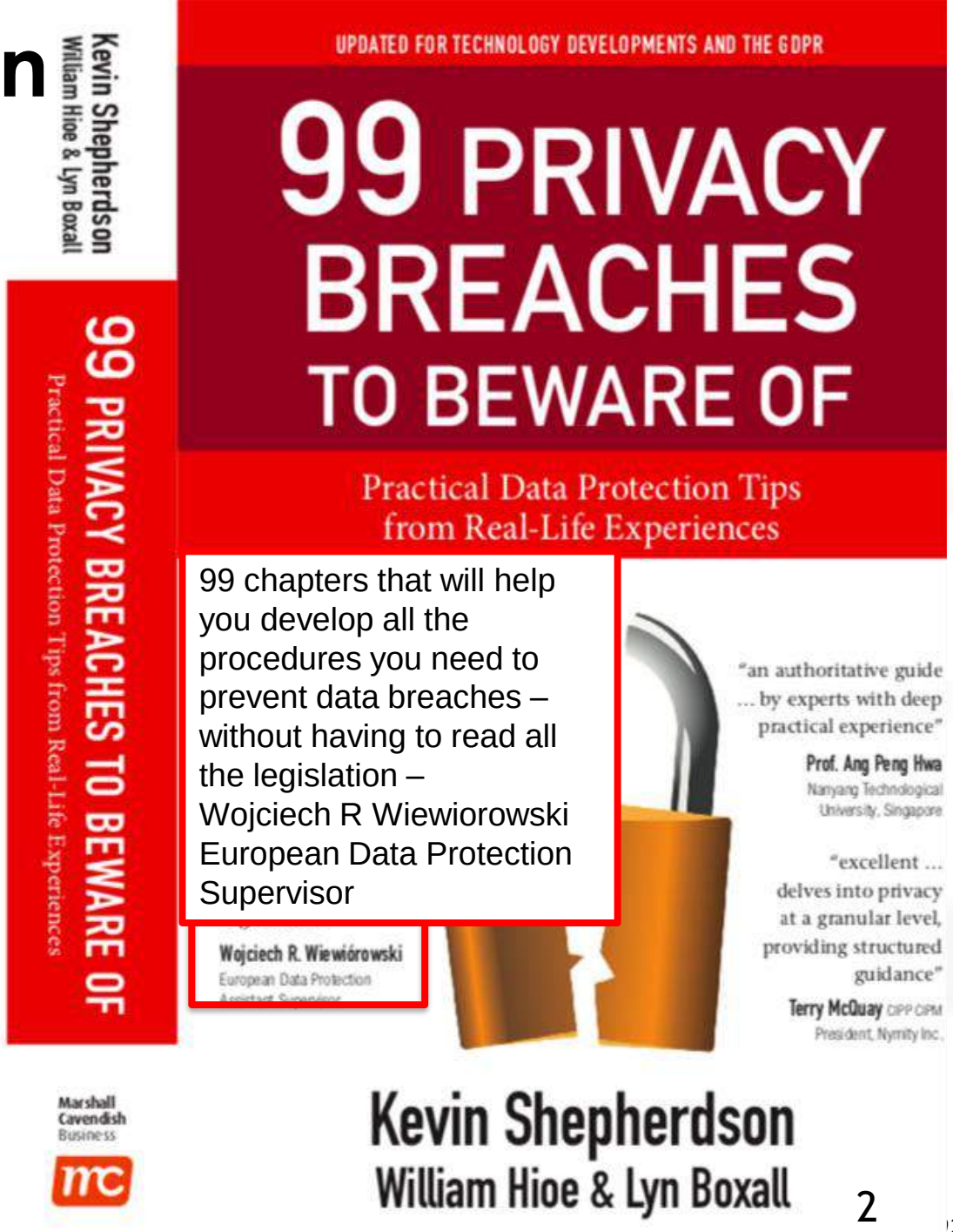
Patricia Poku,
Privacy Commissioner,
Ghana

Provides even more comprehensive coverage and analysis of data protection breaches and cases……..written for the layman and presented in a professional manner.....

Stephen Kai-yi Wong
Commissioner PCPD,
Hong Kong, China

For sure, this book you hold now will be remembered in the coming generations as another seminal work, contributing to the growing reservoir of knowledge on data privacy and security, and providing a solid foundation for the constant forward movement of global discourse.

Raymund Liboro
Commissioner, NPC
Philippines



1. Organisations to shift from predominantly a legal approach to data protection requirements towards a holistic GRC perspective in their operations relating to personal data.

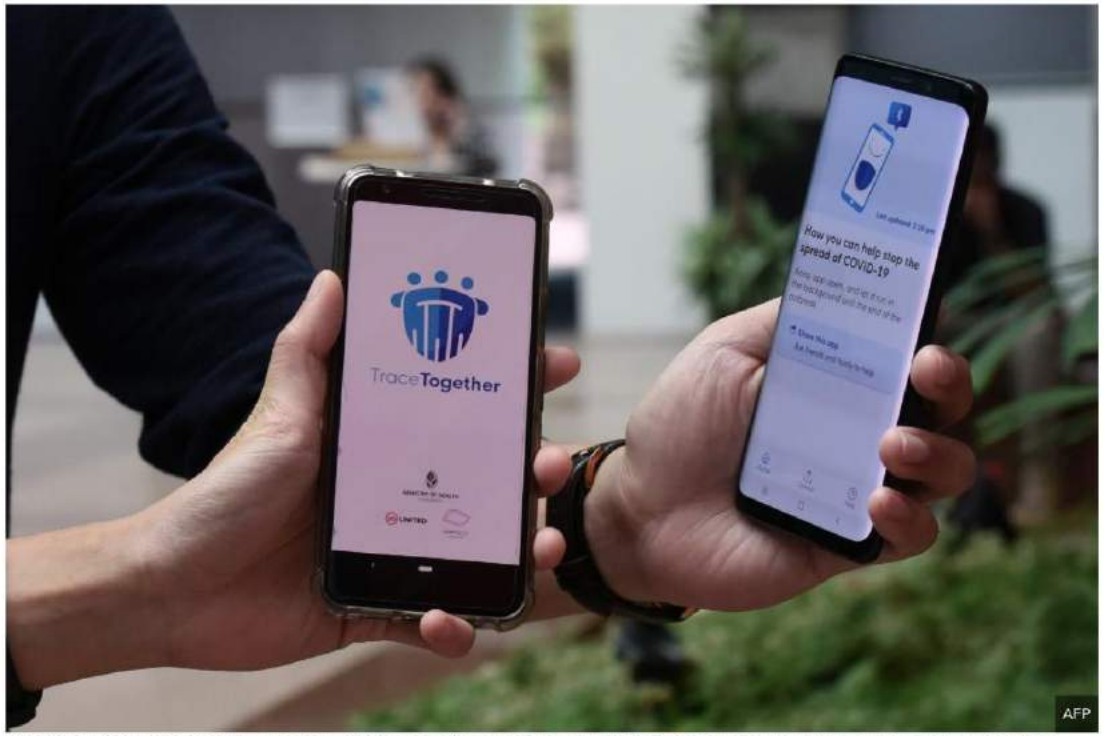
today

Singapore World Big Read Gen Y Speaks Commentary Voices Videos Brand Spotlight 8 DAYS

Some TraceTogether users upset with Govt's revelation on police access to data, say they'll use it less

By NAVENE ELANGOVAN, TAN YIN LIN

Published JANUARY 07, 2021
Updated JANUARY 07, 2021
670 SHARES



The TraceTogether mobile application, used for contact tracing to prevent the spread of Covid-19, uses Bluetooth technology to inform users who had close contacts to confirmed coronavirus cases.

- **Since it was made known that TraceTogether data can be used for criminal investigations, some users react by limiting use of app or token**
- **Political observers noted that the news may have eroded trust in the Government**
- **Others believe users will still keep their eye on the greater goal of beating the pandemic and continue using it**
- **The jury is still out among MPs on whether data should be exempted from police use for solving crimes**

WhatsApp responds to concerns over privacy policy update

This follows calls from concerned users for people to ditch the Facebook-owned app for Signal.

c|net

Abrar Al-Heeti Jan. 12, 2021 1:55 p.m. PT

LISTEN - 02:16

WhatsApp is looking to clarify some concerns about its privacy policy.
Angela Lang/CNET

WhatsApp this week published an FAQ clarifying the terms of its updated privacy policy and responding to concerns that the firm behind the text-messaging app shares personal information with parent company Facebook. WhatsApp noted the update doesn't affect the privacy of messages with friends and family, and instead relates to messaging businesses through the platform. The company also said the update "provides further transparency about how we collect and use data."

Shift from emphasis on purely legal approach to holistic GRC of personal data

Drivers

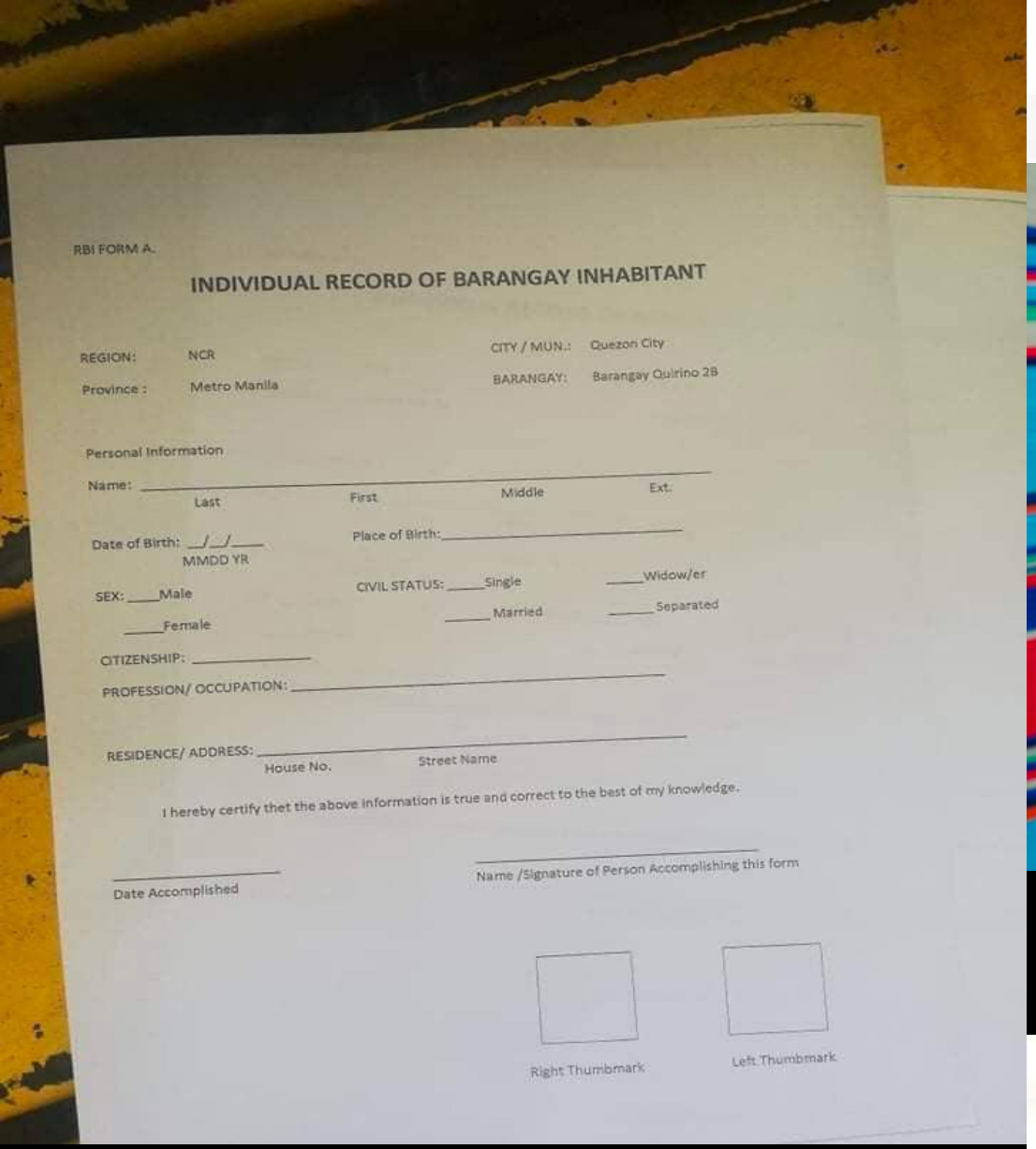
- Effect of COVID19 & surveillance
- Stricter public and private sector DP requirements in the region
- New amendments in PDPA /data breach notification.
- Importance of audits and emphasis of DPMP

Shift from emphasis on purely legal approach to holistic GRC of personal data

Effect of COVID19 & surveillance

Rush to enable WFH measures, and digitisation efforts

- IT Vulnerabilities especially to non-tech savvy SMEs
- Susceptible to phishing, scams, social engineering
- Over-intrusive surveillance
- Abuse of contact tracing data


RBI FORM A.

INDIVIDUAL RECORD OF BARANGAY INHABITANT

REGION: NCR
Province : Metro Manila
CITY / MUN.: Quezon City
BARANGAY: Barangay Quirino 2B

Personal Information

Name: _____
Last First Middle Ext.

Date of Birth: __/__/____ Place of Birth: _____
MMDD YR

SEX: ____Male ____Female
CIVIL STATUS: ____Single ____Married ____Widow/er ____Separated

CITIZENSHIP: _____

PROFESSION/ OCCUPATION: _____

RESIDENCE/ ADDRESS: _____
House No. Street Name

I hereby certify thet the above information is true and correct to the best of my knowledge.

_____ _____
Date Accomplished Name /Signature of Person Accomplishing this form

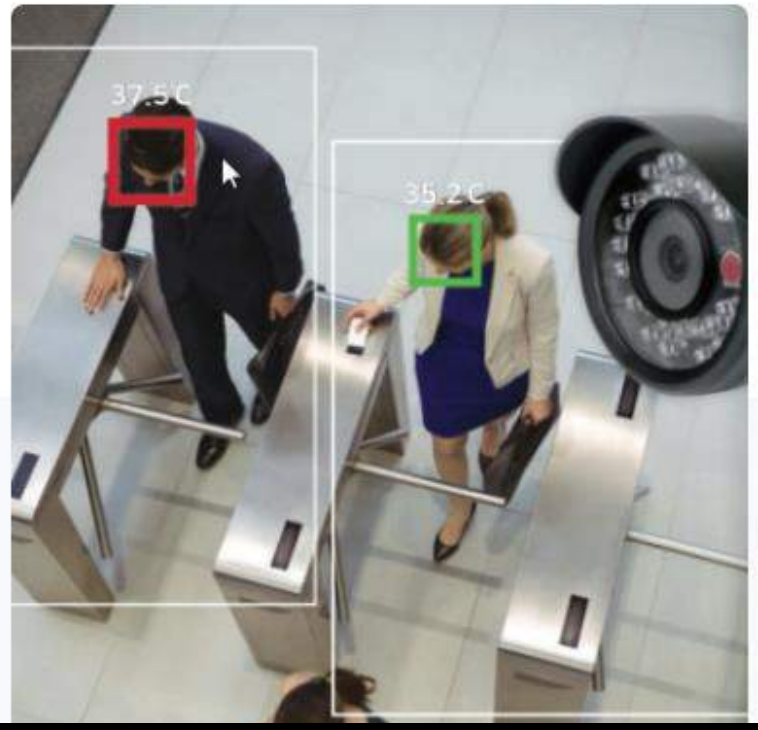
Right Thumbmark Left Thumbmark

Excessive collection of data

Register with gaming app to get a free mask
(Is there another motive?)

OPTOELECTRONICS

Coronavirus detecting CCTV cameras are here



Is there transparency, privacy notice?

Installation of Smart Coronavirus CCTV cameras are being investigated for large office buildings to try and pro-actively isolate those with the virus. As bosses struggle to get their heads around how to cope with an employee in a large office building or factory coming down with Coronavirus, some are looking to invest in smart CCTV with built in temperature sensors.

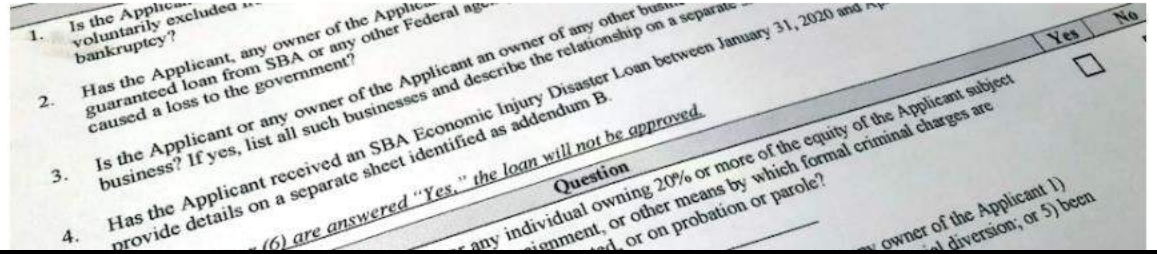
Sections

The Washington Post
Democracy Dies in Darkness

Get 1 year for $29 | Gift Subscriptio

Data breach may have exposed personal information of thousands of SBA emergency loan applicants

Nearly 8,000 applicants may have seen identifiable details of other applicants before the Small Business Administration fixed and relaunched the site



Are your collection procedures safe?

STRAITS INTERACTIVE DPEX DATA PROTECTION EXCELLENCE NETWORK

Do you caution staff on what they download?

ZDNet VIDEOS EXECUTIVE GUIDES SECURITY CLOUD INNOVATION CXO HARDWARE MORE NEWSLE

PART OF A ZDNET SPECIAL FEATURE: CORONAVIRUS: BUSINESS AND TECHNOLOGY IN A PANDEMIC

Coronavirus: They want to use your location data to fight pandemic. That's a big privacy issue

Why Deutsche Telekom's data donation to fight the spread of COVID-19 sets a potentially troubling precedent.

Do you track your staff?

THE STRAITS TIMES

Beware of fake apps with malware mimicking TraceTogether

Your Boss May Soon Track You At Work For Coronavirus Safety

Friday, May 8, 2020

Shannon Bond / NPR

PHOTO BY GETTY IMAGES

Another Coronavirus Side Effect: In-Home Surveillance By Remote Workers' Employers

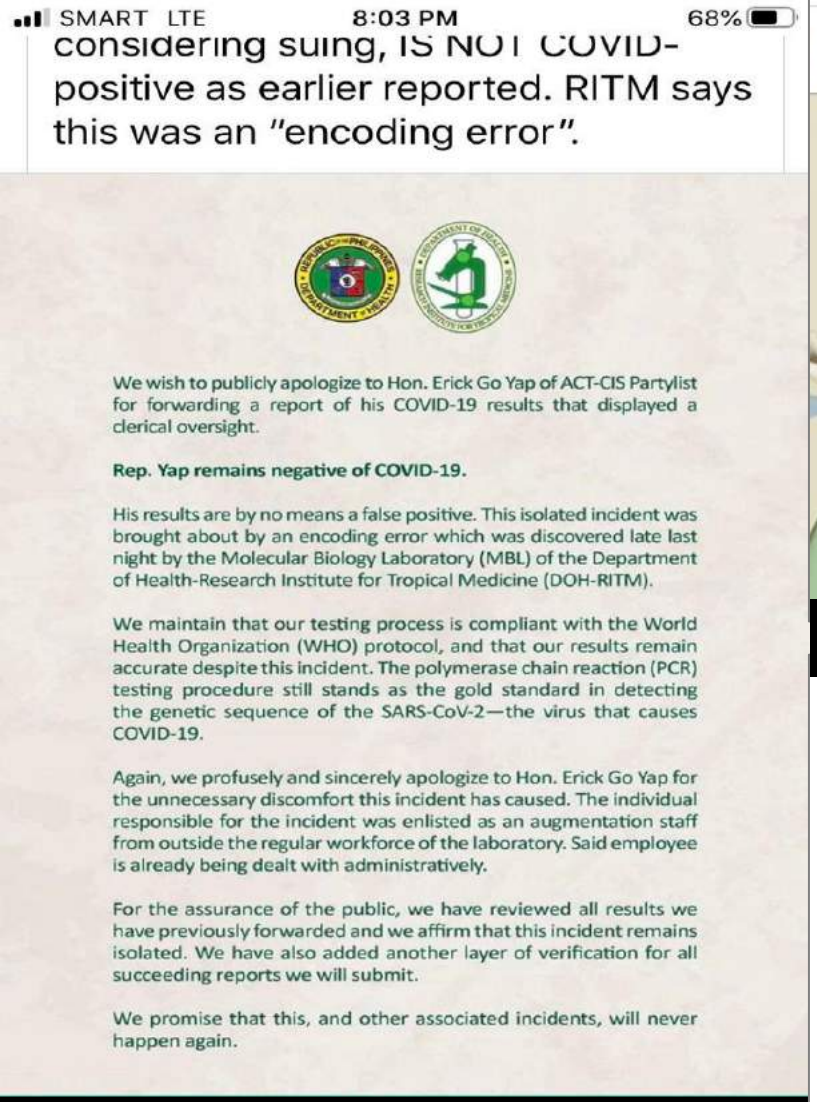
(Mis)Uses of Technology

from the *spyware-but-for-people's-faces* dept

Wed, Apr 8th 2020 3:47am — **Tim Cushing**

Well, it took a pandemic to normalize **domestic surveillance** by [checks notes] employers. Not sure if this is the dystopia we needed or the one we deserved, but the shelter-in-place policies that have turned lots of office workers into telecommuters has led to **incredible growth in one particular market sector**.

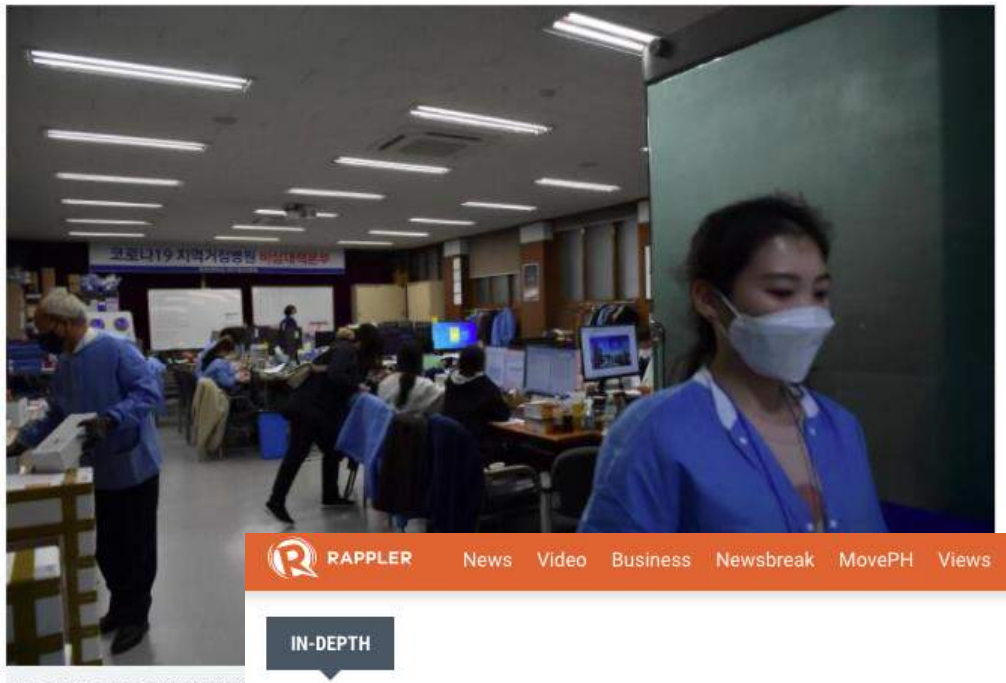
Spokesman Gregory Frost said in a statement that "the enhanced monitoring of at-home employees we implemented will ensure that those members of our workforce who work from home will continue" to meet quality and productivity standards that are expected from all workers.



A congressman mistakenly reported as Covid19 positive due to clerical error

Inaccurate processing / algorithms

Coronavirus: Giving out patient details - a case of serving public good or invasion of privacy?



In a photo taken on March 10, 20
in Daegu. PHOTO: AFP

PUBLISHED MAR 12, 2020, 1

ST VIDEOS

Officials shut down

RAPPLER News Video Business Newsbreak MovePH Views Life & Style Entertainment Sports Tech Hustle BrandRap

IN-DEPTH

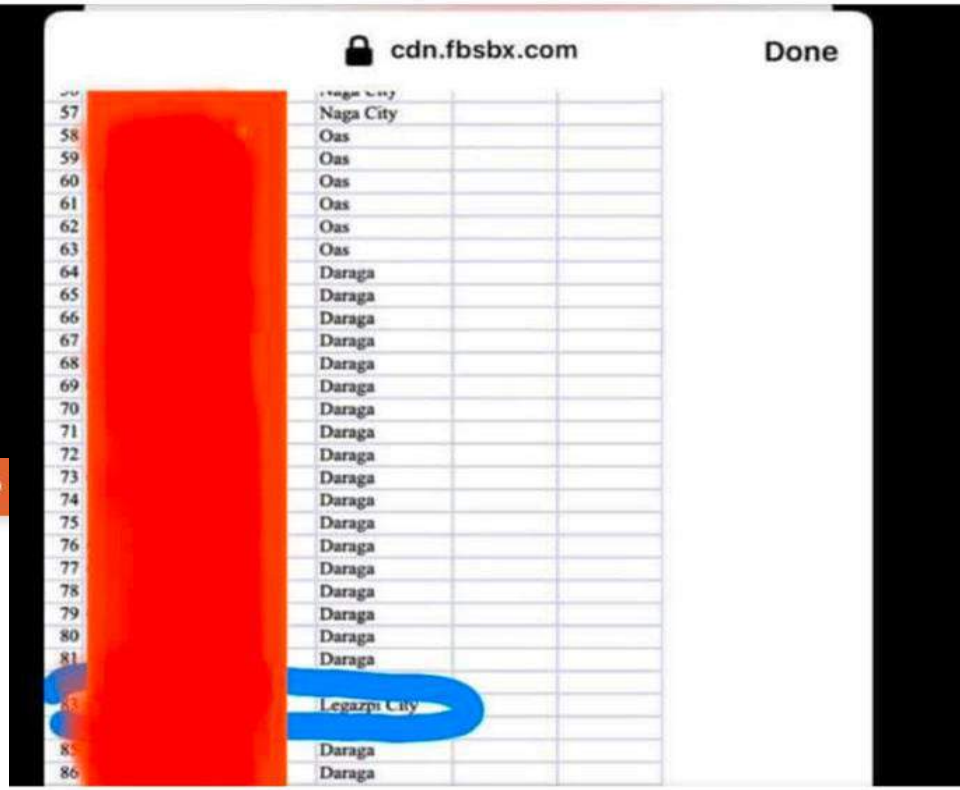
Unauthorized disclosure of COVID-19 patients' identities continues

Privacy breaches are committed by health workers, local government units, ordinary citizens, says the National Privacy Commission, which is investigating cases

Nikko Dizon

Published 9:00 AM, June 28, 2020

😖 contact-tracing done, disclosed & shared irresponsibly, on the names of potential pums/puis in the concert of mulatto band in a certain province.



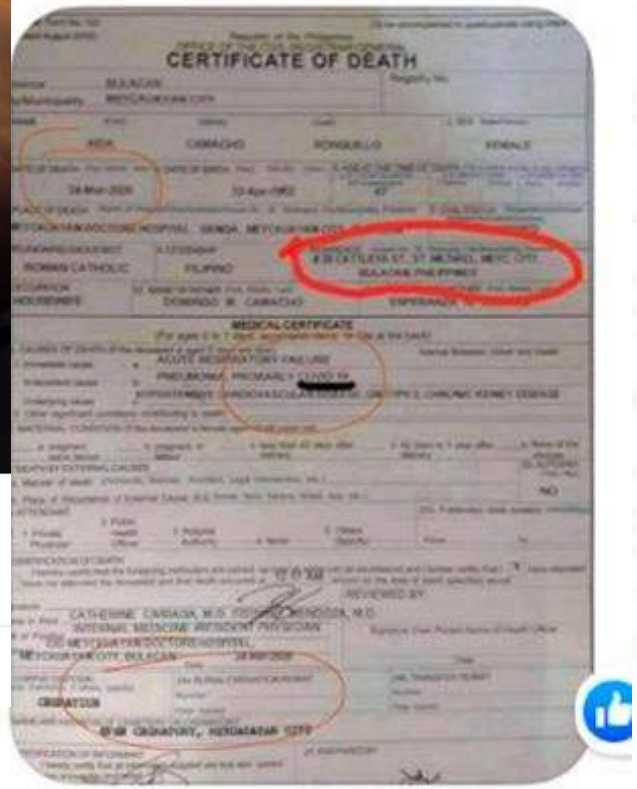
Covid-19 patients become victims of Indonesia's lack of privacy protection

INDONESIA

Thursday, 05 Mar 2020

12:08 PM MYT

JAKARTA (The Jakarta Post/ANN): Indonesia's first two confirmed Covid-19 patients claim that media coverage and discussion on social media have taken a greater toll on them than the disease itself, saying that numerous breaches of privacy and the resulting stigma have left them "mentally drained".



Post called out by a Filipino doctor on social media of a patient's death with no consent given

Potential impact of COVID-19 on Data Breaches

Key findings

54%

Share of organizations that required remote work in response to COVID-19

76%

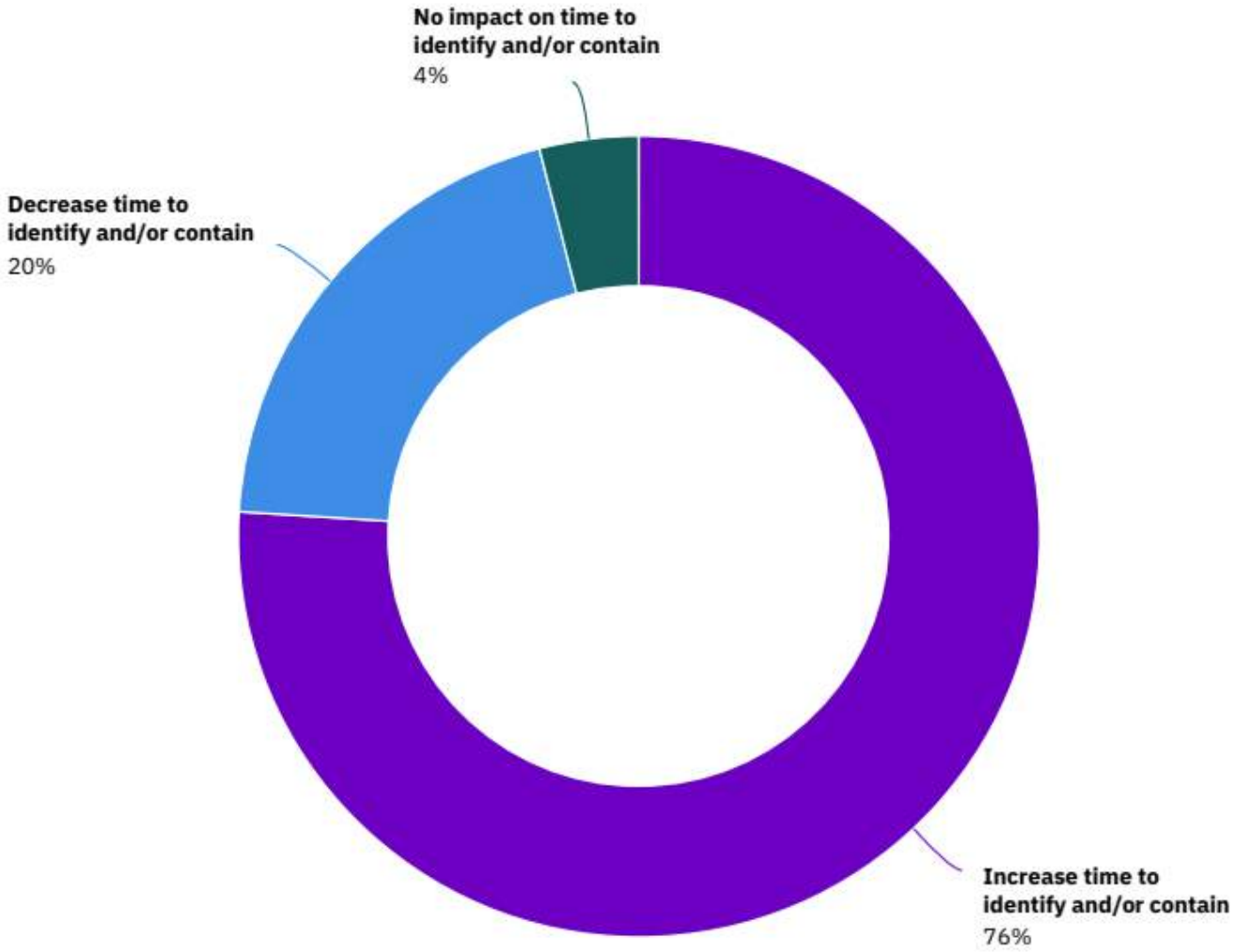
Share of participants who said remote work would increase the time to identify and contain a data breach

70%

Share of participants who said remote work would increase the cost of a data breach

***2020 Cost of a Data Breach** Report - **Ponemon** Institute*

How would remote work impact your ability to respond to a data breach?



COVID 19 and Remote Working

Time to identify and / or contain

- ❑ Increase (76%)
- ❑ Decrease (20%
- ❑ No Impact on time (4%)

***2020 Cost of a Data Breach** Report - **Ponemon** Institute*

Shift from emphasis on purely legal approach to holistic GRC of personal data

Effect of COVID19 & surveillance

Rush to enable WFH measures, and digitisation efforts

- **IT Vulnerabilities especially to non-tech savvy SMEs**
- **Susceptible to phishing, scams, social engineering**
- **Over-intrusive surveillance**
- **Abuse of contact tracing data**

Shift from emphasis on purely legal approach to holistic GRC of personal data

Stricter Public sector and Data Protection Requirements

Philippines DPA (2021 New Amendments)

Power to impose financial sanctions directly

Thailand PDPA (2021 June goes into effect)

Postponed from May 2020 by one year

Indonesia PDP Bill (2021 – Scheduled to be Passed as law)

Protection of PII already in electronic transactions act

Malaysia PDPA (Review in progress)

Review of PDPA – includes Applicability to public sector being evaluated

Singapore PDPA (2021 – New Amendments in effect)

Breach Notification
Heavier fines
SG: Public Sector Data Security Review Committee: Recommendations implemented

Countries with Comprehensive Laws covering the public sector

Shift from emphasis on purely legal approach to holistic GRC of personal data

Singapore PDPA Amendments

Key amendments include:

- Accountability
- Mandatory data breach notification
- Revised consent framework
- New data portability obligation
- Enhanced rules on telemarketing and spam
- Section 29 - Maximum fine
  - **$1 million or *10 % of annual turnover.***

Sensitive data – Government ID
- 2019 NRIC rules

Shift from emphasis on purely legal approach to holistic GRC of personal data

Singapore: Data Breach Notification

	Current	New
Definition - Data Breach	a)the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data	a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data or b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur
To notify PDPC	Not mandatory, but encouraged	Mandatory if it results in • Significant harm • Significant scale >500
Assessment needed	NA	Org to assess if notifiable data breach – PD in possession and processed by org DI to notify org without undue delay – PD in possession and processed by DI of Org
Notification	NA	• no later than three days • To PDPC (before or at same time as individuals) • To individuals

Shift from emphasis on purely legal approach to holistic GRC of personal data

Amendments in Philippines DPA

- Breach **notification requirements for processors** (outside of the Philippines)
- **Broader definition of sensitive data** (financial data, ID numbers, genetic, biometric data)
- **Extra Territorial Application** - where the processing activities involves offering of goods or services or monitoring of behavior within the Philippines.
- **Administrative fines** without prejudice to the filing of criminal charges.

Shift from emphasis on purely legal approach to holistic GRC of personal data

New Thai PDPA

- **Adaptation of GDPR principles**
  - Sensitive – including Government IDs
  - Extra-territorial application
  - Lawful processing and consent requirements
  - Right of individuals
  - Appointment of DPO
  - Records of processing
  - Data Breach Notification

Shift from emphasis on purely legal approach to holistic GRC of personal data

Indonesian Data Protection Bill

- Law and Regulation on Electronic Information and Transaction- Article 14 on GR 71 covers data protection principles and legal basis of Processing. (copied from the DP Bill), Breach Not*ification*
- Adaptation of GDPR principles
  - Sensitive – including financial data
  - Lawful processing and consent requirements
  - Right of individuals
  - Appointment of DPO
  - Records of processing
  - Data Breach Notification
- **Prohibition of visual data processing installed in a public place and/or public service facilities**

Shift from emphasis on purely legal approach to holistic GRC of personal data

Summary of Data Breach Notification Requirements

(Country Comparison)

Country	Notify Regulator
European Union	Yes – 72 hours (Risks to Rights and freedoms of data subjects)
Singapore	Yes – 3 calendar days (Significant harm/scale, > 500 individuals)
Philippines	Yes – 72 hours (no delay if 100 data subjects) Full report submitted within 5 days from notification
Indonesia	Yes – 72 hours Written notice to data subject and minister.
Thailand	Yes - 72 hours (Risks to rights and freedoms of Persons)

Shift from emphasis on purely legal approach to holistic GRC of personal data

Governance, Risks Management & Compliance

Organisations should ensure GRC of personal data

<u>Governance</u>

- Management buy in & Appointment of DPO
- Data Protection Committee
- Consider impact to stakeholders

<u>Risks Management</u>

- Data inventory & Sensitive data
- Data flows (CUDS) & third party risks

<u>Compliance</u>

- Regional DP laws / legal & operational compliance
- New amendments **/** Data breach notification

2. A renewed focus on the importance of third party management of personal data due to automation, digitalisation and WFH initiatives resulting from COVID-19.

Renewed Focus on Third party management

- COVID19 - Need for diversification in supply chains,
- Sourcing of new partners for digitization & automation
- With business systems and processes so intertwined, an incident inside a supplier's system can greatly impact outside organisations associated with

You can delegate the task to a third party but ***not the responsibility***

Renewed Focus on Third party management

- **Responsibility lies with the organisation / controller**
  - ***Important to understand if you are a controller / processor***

Controller / organisation expected to take steps:

- Put in relevant security measures when appointing processors
- To make contractual arrangements
- Keep register of third parties
- Comply with cross border transfer requirements

ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows

Share

On 22 January 2021, the 1st Association of Southeast Asian Nations (ASEAN) Digital Ministers' Meeting (ADGMIN) approved the ASEAN Data Management Framework (DMF) and Model Contractual Clauses for Cross Border Data Flows (MCCs). The initiatives were developed by the Working Group on Digital Data Governance chaired by Singapore.

Renewed Focus on Third party management

- **Responsibilities of processor**

  Process PII :
  - based on instruction of controller
  - with due regard to the provisions of personal data processing under applicable law

  Implement protection measures
  - Ensure data protection by design
  - Conduct DPIA

  Comply with retention principle

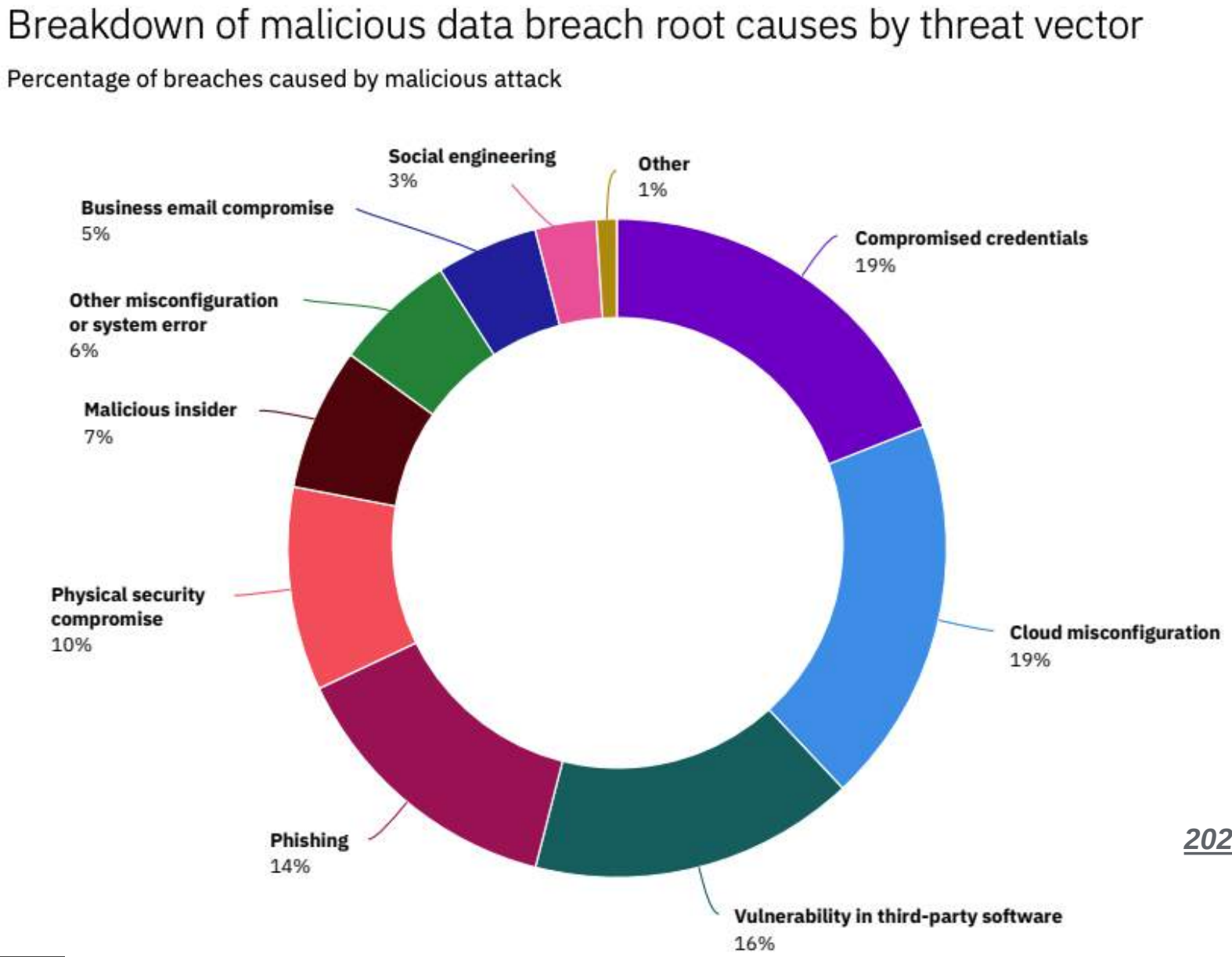
  Extra-territorial applicability:
  - Thailand PDPA
  - Philippines PDA (upcoming amendment)

  Data Breach notification to controller

If data processor conducts the processing of personal data outside the instructions of the personal data controller then it will be considered as a controller and held liable under the law.

3.While in 2021 will see continued sophisticated cyber threats and data breaches, expect more cases of data breaches involving Intrusive mobile apps as a result of COVID19 and ongoing automation.

More sophisticated cyber threats, increased data breaches…



Top 5 Malicious Attacks

- Compromised credentials (19%)
- Cloud misconfiguration (19%)
- *Vulnerabilities in 3rd party software (16%)*
- Phishing 14%
- Physical Security Compromise

2020 Cost of a Data Breach Report - Ponemon Institute

More sophisticated cyber threats, increased data breaches…

The New York Times

FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State

The Silicon Valley company said hackers — almost certainly Russian — made off with tools that could be used to mount new attacks around the world.

By David E. Sanger and Nicole Perlroth

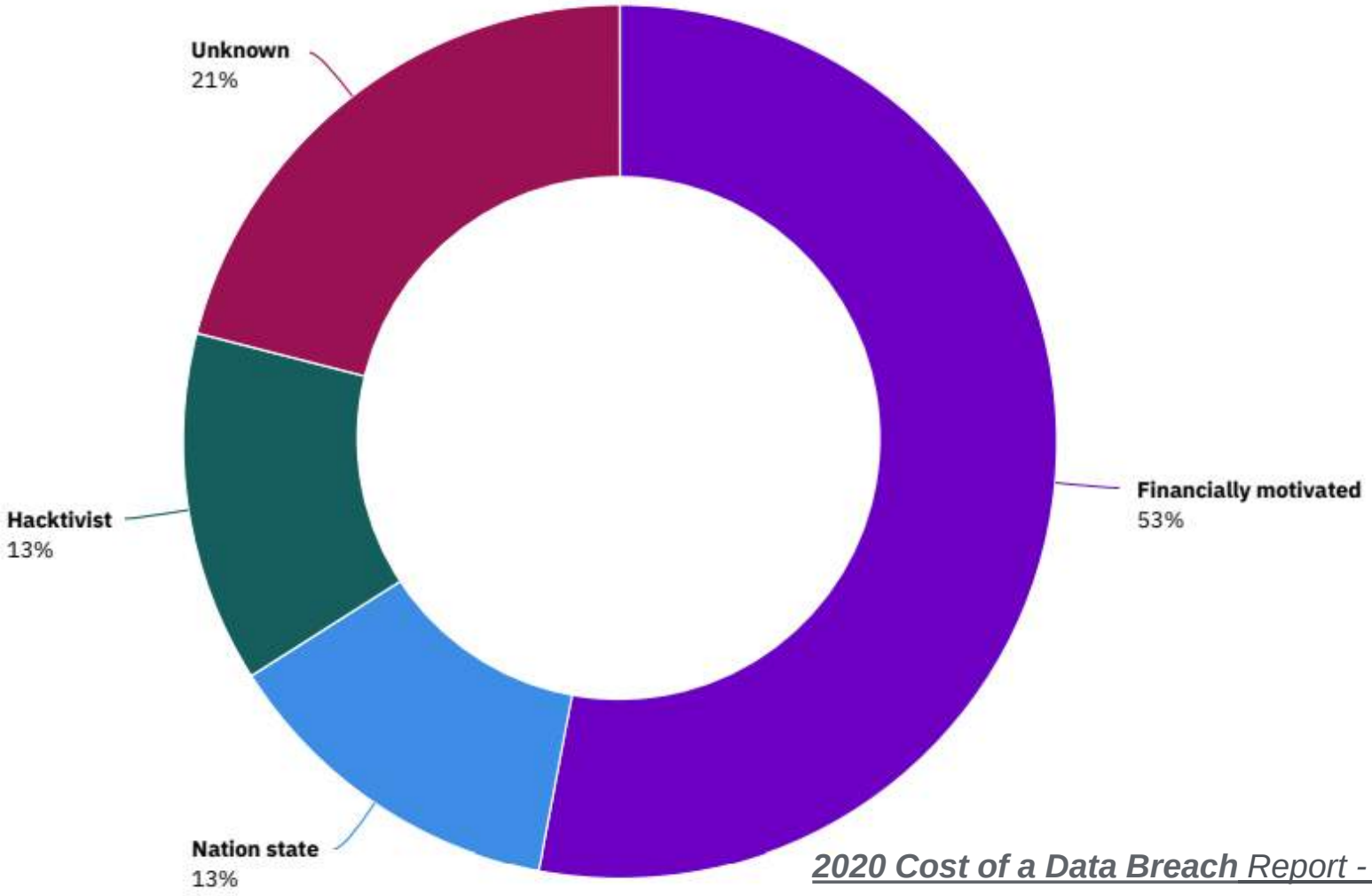
Published Dec. 8, 2020 Updated Dec. 31, 2020

WASHINGTON — For years, the cybersecurity firm FireEye has been the first call for government agencies and companies around the world who have been hacked by the most sophisticated attackers, or fear they might be.

Now it looks like the hackers — in this case, evidence points to Russia's intelligence agencies — may be exacting their revenge.

More sophisticated cyber threats, increased data breaches…

Malicious data breaches organized by threat actor type



Motivation of Attack

- Financially motivated (53%)
- Nation State (13%)
- Hacktivist (13%)
- Unknown (21%)

2020 Cost of a Data Breach Report - Ponemon Institute

More cases of privacy breaches (COVID19) …

MARCH 8, 2020 — APRIL 18, 2020

SOUTH KOREAN CONTACT TRACING APP BREACH.

The contact tracing app in South Korea was really easy to reverse and gain all of the user data. Officials were in such a hurry to release the app that they did not make time to properly secure it. “We were really in a hurry to make and deploy this app as quickly as possible to help slow down the spread of the virus. We could not afford a time-consuming security check on the app that would delay its deployment.” www.nytimes.com/2020/07/21/tec…

MARCH 1, 2020 – MARCH 17, 2020

COVID-19 TRACKER APP RANSOMWARE

The ransomware requests $100 in bitcoin in 48 hours on the ransom note. It threatens to erase your contacts, pictures and videos, as well as your phone's memory. It even claims that it will leak your social media accounts publicly. www.domaintools.com/resources/…

MAY 18, 2020

MALWARE IN COVID-19 APP STEALS SMS AND CONTACTS

Malware hiding inside COVID-19 apps is stealing personal data, including SMS messages, call logs, contacts, and more. labs.bitdefender.com/2020/05/a…

MAY 21, 2020 – MAY 22, 2020

QATAR CONTACT TRACING APP BREACH

Researchers identified a security flaw in Qatar's mandatory COVID-19 contact tracing app. The vulnerability disclosed ID, health status, and location date for every user. www.amnesty-usa.org/press-relea…

More cases of privacy breaches (mobile apps) …

Los Angeles Times

Subs
$1.

Muslims reel over a prayer app that sold user data: 'A betrayal from within our own community'

JANUARY 9, 2020 — JANUARY 15, 2020

WALGREENS MOBILE APP LEAK

Walgreens discovered an error within the Walgreens mobile app personal secure messaging feature. An investigation determined that an internal application error allowed certain personal information to be viewable by other customers using the Walgreens mobile app. oag.ca.gov/system/files/Walgre…(WAG%20version)-Final.pdf

MAY 24, 2020 — JUNE 15, 2020

DATING APPS LEAK DATA

845 gigabytes and close to 2.5 million records from 3somes, Cougary, Gay Daddy Bear, Xpal, BBW Dating, Casualx, SugarD, Herpes Dating, and GHunt leak via misconfigured S3 buckets. www.wired.com/story/dating-app…

MARCH 15, 2020 — APRIL 5, 2020

CASINO APP LEAKS ALL DATA

An unsecured Elasticsearch database leaked data on millions of global gambling app users. A casino app, Clubillion, left the database on the internet, exposing users' PII data, including IP addresses, email addresses, winnings, and private messages. If you use this app, be aware of very targeted phishing emails resulting from your data being exposed. www.vpnmentor.com/blog/report-…

JUNE 12, 2020

TIM HORTON'S APP TRACKING LOCATIONS

Financial Post reported the Tim Horton's app uses technology from Radar Labs, an American company that states on its website that it can check a phone's location in the background as often as every three to five minutes. Radar uses those GPS coordinates to infer the location of customers' homes, where they work, as well as every time the company thinks they visited one of their client's

APRIL 23, 2020 — MAY 23, 2020

INDIA BHIM PAYMENT APP DATA LEAK

A data leak from India's BHIM payment app exposed personal data of 7 million Indians including addresses, scans of Aadhar IDs, and caste certificates. A report from cybersecurity company VPN Mentor suggests that this 409GB database was stored in a misconfigured AWS S3 bucket, making all data publicly accessible. thenextweb.com/in/2020/06/01/i…

JUNE 9, 2020

BABYLON HEALTH APP BREACH

Babylon Health has acknowledged that its GP video appointment app has suffered a data breach. The firm was alerted to the problem after one of its users discovered he had been given access to dozens of video recordings of other patients' consultations. www.bbc.com/news/technology-52…

More cases of privacy breaches (mobile apps) …

JULY 3, 2020

EGYPTIAN APP, SWVL, HIT BY DATA BREACH

Swvl, a bus-booking app and operator of bus routes in Egypt, Kenya, and Pakistan, has been struck by a data breach. Swvl claims only names, email addresses, and phone numbers were accessed. portswigger.net/daily-swig/egy…

AUGUST 24, 2020

MESSENGER APP PROMOTED FOR MASS PROTESTS IS A PRIVACY DISASTER

Researchers recently revealed a litany of flaws and weaknesses that show that just about every claim of anonymity, privacy, and reliability is outright false. Researchers said that the app's design for use at concerts, sports events, or during natural disasters makes it woefully unsuitable for more threatening settings such as mass protests. arstechnica.com/features/2020/…

SEPTEMBER 4, 2020 — SEPTEMBER 22, 2020

KID TIPS OFF RESEARCHERS TO MALICIOUS APPS

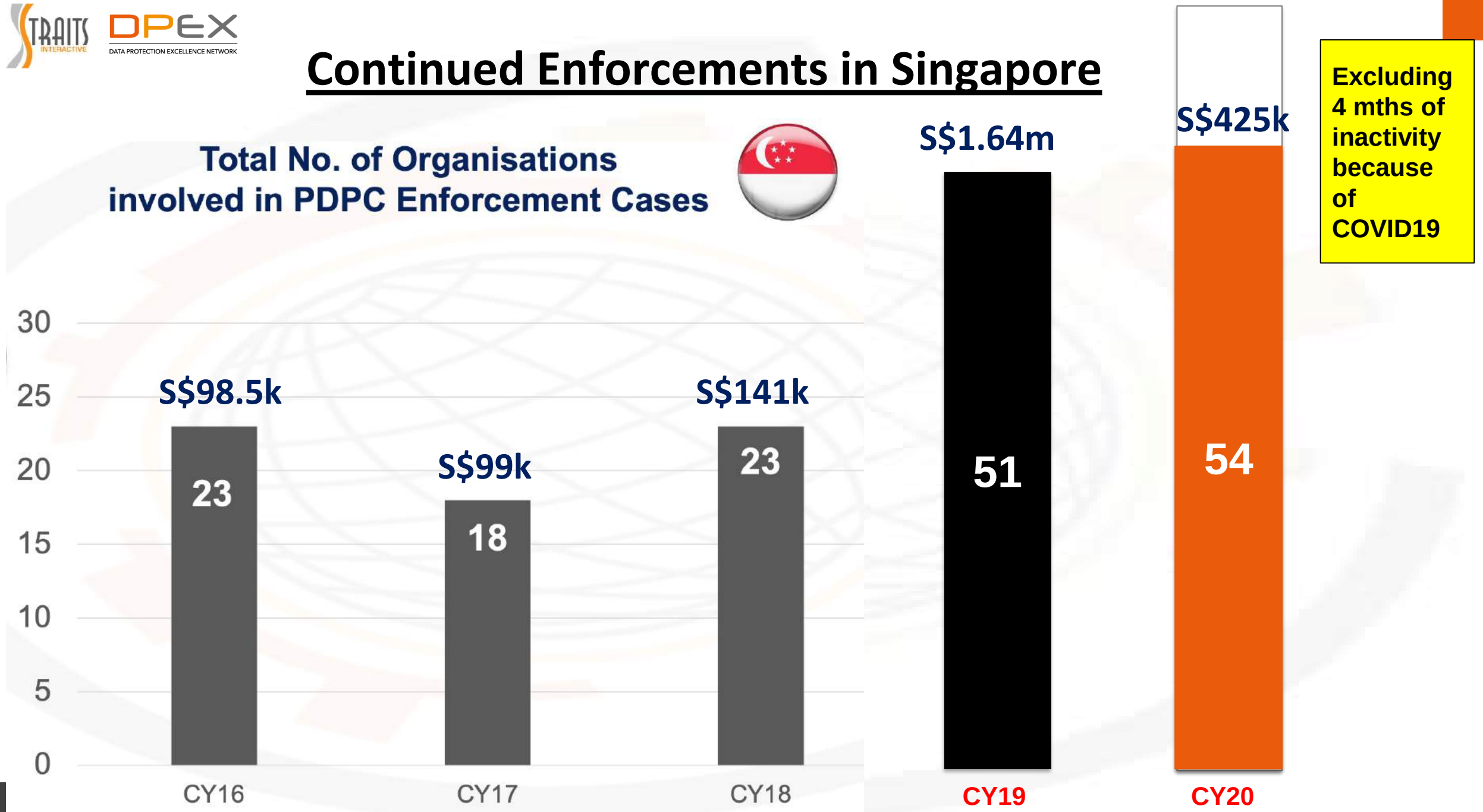
Information from a child led researchers to discover aggressive adware and exorbitant prices lurking in iOS and Android apps. The apps posed as entertainment, wallpaper images, or music downloads, and served intrusive ads even when an app wasn't active. To prevent users from uninstalling the apps, they hid their icon, making it hard to identify where the ads came from. Some apps generated revenue of more than $500,000. arstechnica.com/information-te…

OCTOBER 5, 2020 — OCTOBER 6, 2020

FOOD DELIVERY APP NOTIFIES CUSTOMERS OF BIG DATA BREACH

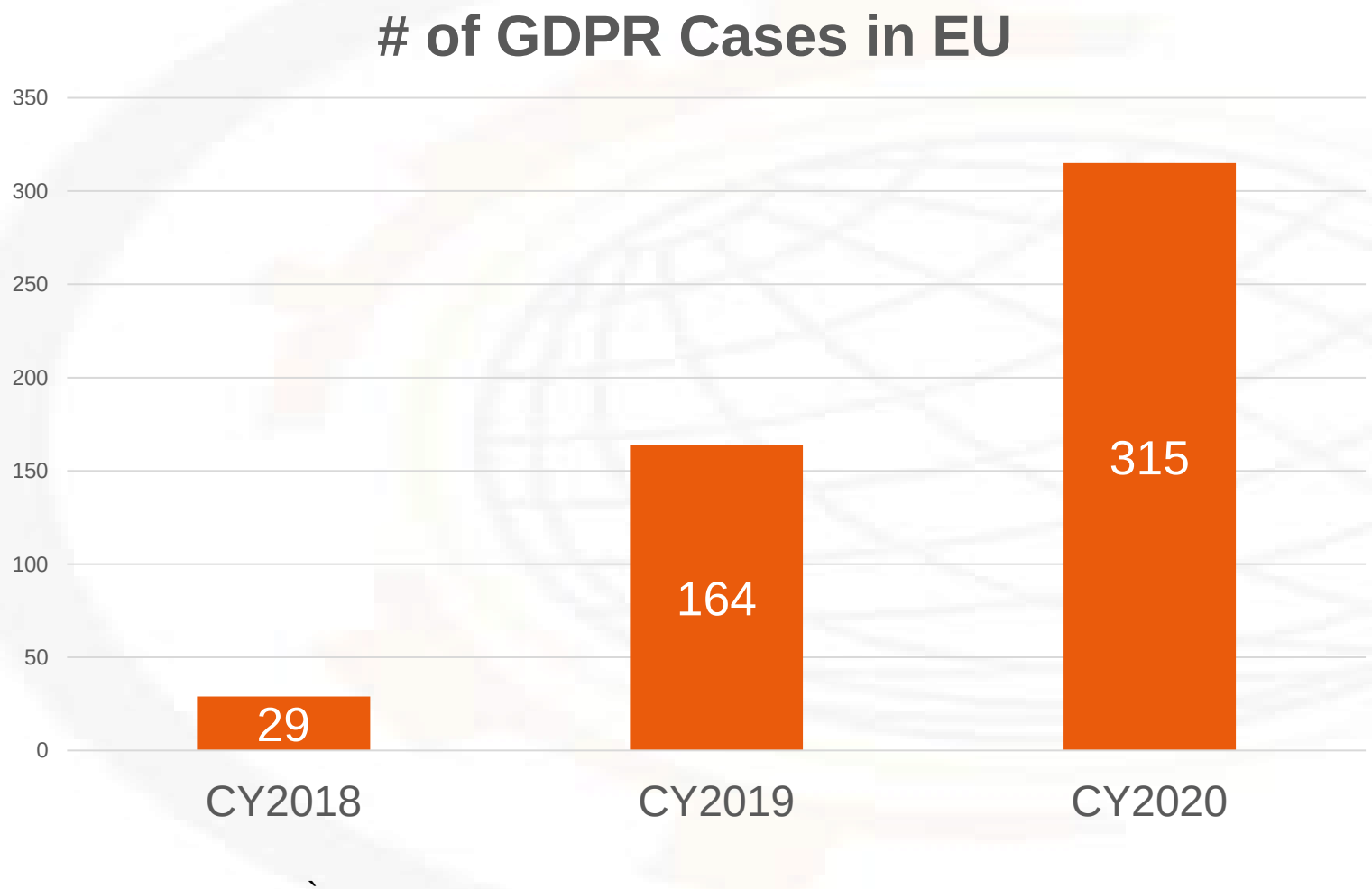
Two months after securing a $33 million funding round from investors, food delivery startup Chowbus is grappling with a breach that observers say exposed personal data on hundreds of thousands of customers. www.cyberscoop.com/chowbus-bre…

Continued Enforcements in Singapore



Excluding 4 mths of inactivity because of COVID19

Enforcement Cases Almost Double in EU (2020)



Top 10 EU Countries

EU Members	CY18	CY19	CY20
SPAIN	7	31	133
ROMANIA		21	26
ITALY		3	35
HUNGARY	1	21	13
GERMANY	5	19	3
BULGARIA	1	15	4
BELGIUM		6	14
POLAND		5	11
SWEDEN		2	14
NORWAY		2	10

Source: GDPR Enforcement Tracker

(to be discussed in a dedicated Webinar)

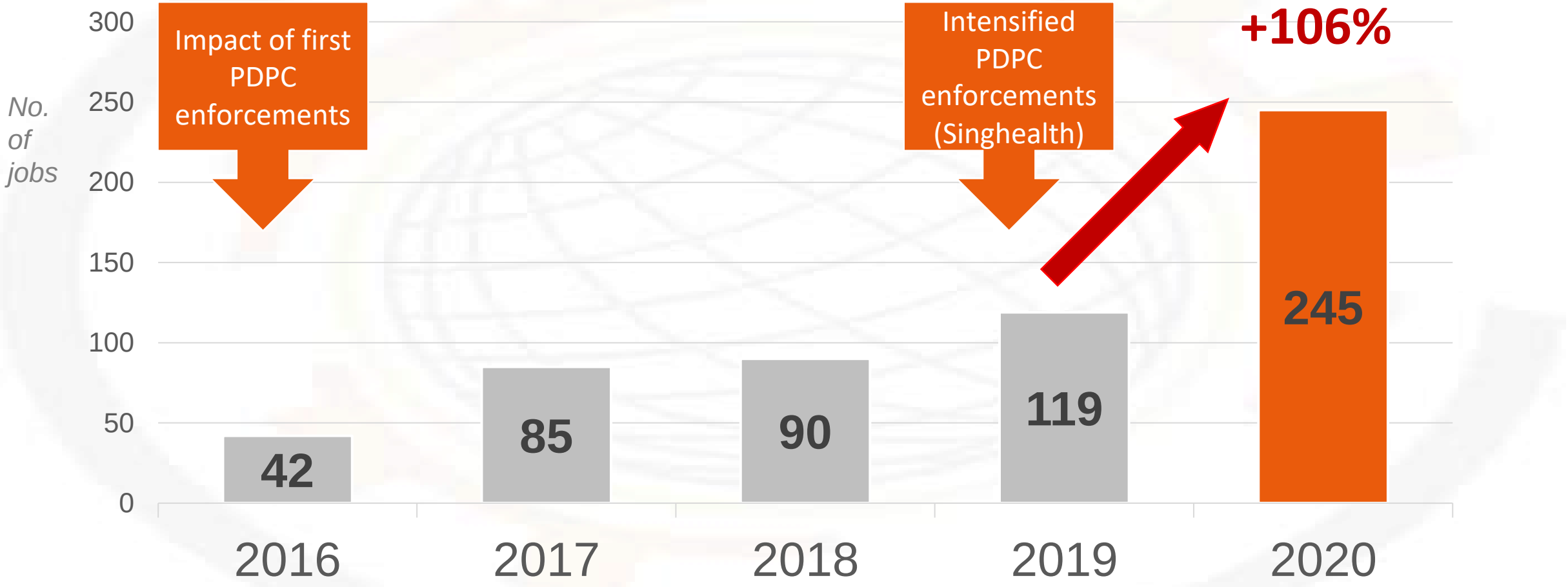
Increasing need to demonstrate accountability (Including developers)

- Need for organisations to demonstrate accountability (4Ds)

1. Data Protection Officer
2. Data Protection Impact Assessment
3. Data Protection by Design
4. Data Protection Management Programme

Growth in Data Protection Jobs (SG) – 1 month job postings

From 2019 to 2020, no. of positions doubled (increase of 105.9%)



Momentum for demand for Data Protection expertise continues

Source: DPEX Centre Job Survey 2020

4. 2021 will also see the European Union's GDPR and ISO 27701 firmly established as de facto standards used for operational compliance and data protection / privacy management.

GDPR established as de facto reference standard

General Data Protection Regulation (GDPR) in EU

New Upcoming Laws/ Amendments

Indonesia PDP Bill

.

Thailand PDPA

Philippines DPA

India PDP Bill

China PI Sec Specs / draft law

GDPR data protection principles being adopted and adapted for local context; concept of lawful/legal processing with focus on Lawful/legal processing.

GDPR established as de facto reference standard

Singapore's PDPA

Consent Obligation

- Deemed consent* - disclosure based on *contractual necessity*

Consent Exception

- Consent Exception: *organisations are required to comply with other legal obligations,*
- Consent Exception - Public interest (2nd / 3rd / 4th schedule), to participate in research, disclosed to any officer of a prescribed law enforcement agency,
- Respond to an emergency that threatens the life, health or safety of the individual or another individual;

- **Legitimate interests exception *and business improvement exception****

* New PDPA amendments

GDPR – Lawful Processing **

- **C**onsent
- **C**ontract Fulfilment / Performance
- **C**omply with legal obligation
- **I**nterests – Public, Public Authority performing task
- **I**nterests – Vital (life or death)
- **I**nterests – Legitimate business

** *Comparison is purely based from operational perspective (not human rights)*

GDPR established as de facto reference standard

Applicable to all ASEAN countries

- Lawfulness of processing with **stricter consent requirements**
- **Requirements for DPO**
- **Stricter requirements for processors**
- **Data Protection Impact Assessment**
- **Data Protection by Design**
- **Records of processing** (*INDO, TH)
- **Extra-territorial application** (*PHI, TH)

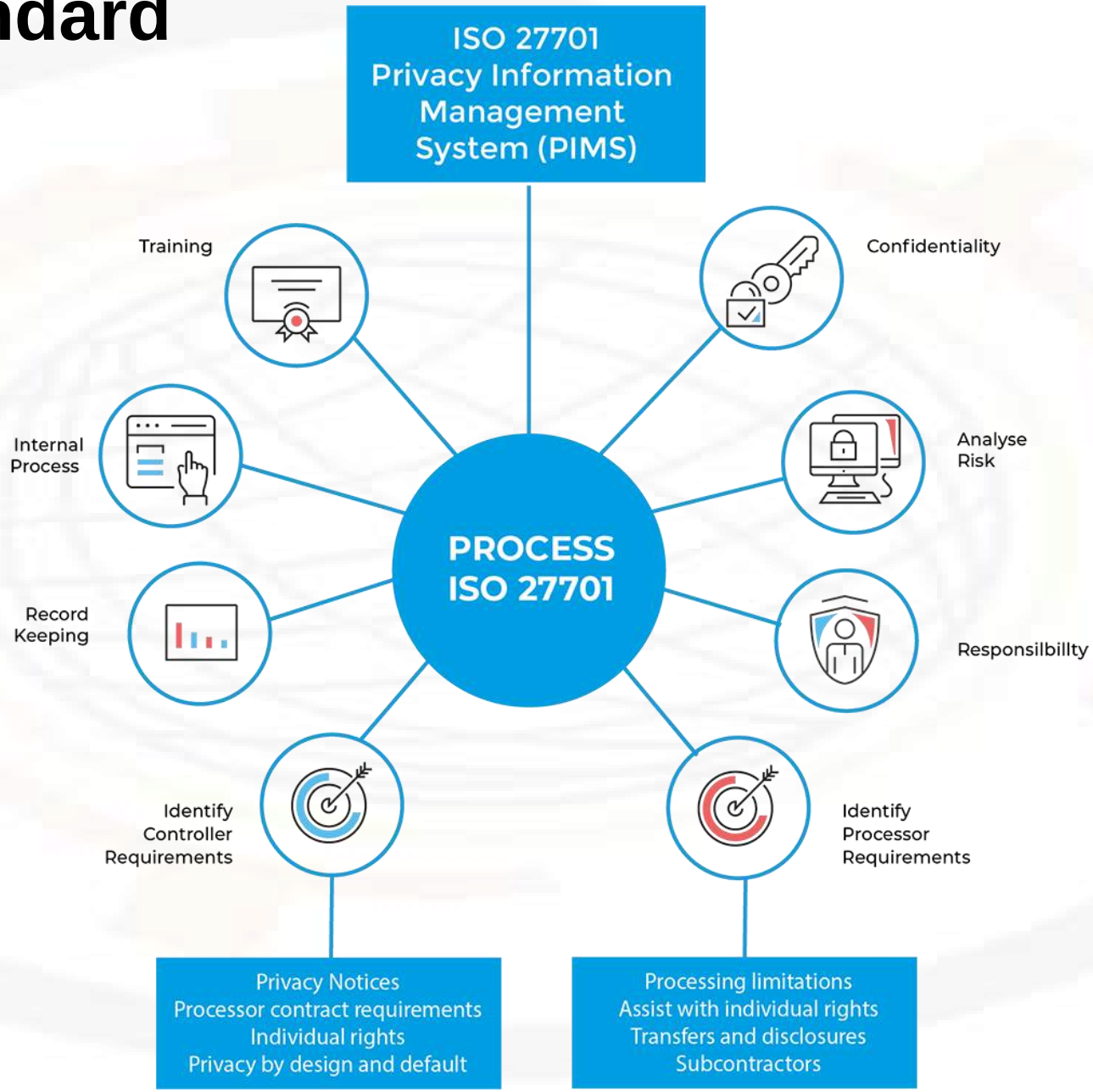
ISO 27701 established as de facto reference standard

About the ISO 27701

- First edition was published in August 2019.
- Extension to ISO/IEC 27001 and to ISO/IEC 27002 – information security requirements and guidelines
- The standard specifies a Privacy Information Management System based on ISO/IEC 27001(ISMS), 27002 (security controls) and 29100 (privacy framework).
- Applicable to both controllers and processors of Personally Identifiable Information (PII).

ISO 27701 established as de facto reference standard

Applications of ISO 27701



Source:

ClearComm
part of Moore Kingston Smith

ISO 27701 established as de facto reference standard

Why is it important to ASEAN?

- Already mapped to GDPR
- Many organisations already adopting ISO 27701
- Standards-based and Jurisdictional neutral
- Increasingly relevant to data protection audits
  - Expected to be used as a referent standard by auditors in the region
- Emerging reference standard for regional compliance teams

5. As public awareness of data protection / privacy grows, the importance of certification both at the corporate and individual level will continue to gain momentum driven by the local data protection / privacy authorities.

Continued momentum of certification both at corporate and individual level

Drivers in ASEAN

- Data protection laws in all founding ASEAN members
- GDPR as a de facto standard
- Shortage of Data Protection Officers and expertise
- Active enforcement and data protection breaches
- Requirements for regional compliance and audits
- Opportunities in data protection

Continued momentum of certification both at corporate and individual level

Corporate Data Protection Frameworks and Trustmarks

Asia-Pacific Economic Cooperation

APEC CROSS BORDER PRIVACY RULES SYSTEM SINGAPORE

ASEAN DP Framework

Singapore Data Protection Trustmark

DATA PROTECTION ASSURED

Philippines Trustmark (in discussions)

APEC Cross-Border Privacy Rules & Privacy Recognition for Processors

- APEC Privacy Framework
  - Cross border Privacy Rules (CBPR 2011) – Controllers
  - Privacy Recognition of Processors (PRP 2015) - Processors
  - The Privacy Enforcement Authorities (Cross Border Privacy Enforcement Arrangement (CPEA); has the ability to take enforcement actions under applicable domestic laws and regulations consistent with the CBPR program requirements.
  - Certification is awarded through an Accountability Agent (AA). For CBPR, PRP to take off - Accountability Agent needs to be appointed locally

- Only 9 participating members in CBPR.
  - USA, Canada, Mexico, Australia, Japan, South Korea, Taiwan, Singapore, Philippines
  - Truste /TrustArc (2013), JIPDEC (2016), Schellman & Company (2019)
  - 2019 - Singapore IMDA appointed as AA - DPTM to segway to CBPR; Philippines to appoint an AA soon

Asia-Pacific Economic Cooperation

APEC CROSS BORDER PRIVACY RULES SYSTEM SINGAPORE

The CBPR System consists of four elements
(1) self-assessment;
(2) compliance review;
(3) recognition/acceptance ; and
(4) dispute resolution and enforcement

6 foundational components of the DMF

These 6 foundational components aim to enable the organisation to leverage on a corporate governance structure to define, manage and monitor its data management processes.

https://asean.org/storage/2-ASEAN-Data-Management-Framework_Final.pdf

1	2	3	4	5	6
Governance and oversight	**Policies and procedural documents**	**Data inventory**	**Impact / Risk assessment**	**Controls**	**Monitoring and continuous improvement**
Provide direction for employees across the organisation in implementing and executing the DMF and oversee the function to confirm it is operating as designed.	Develop data management policies and procedures based on the DMF throughout the data lifecycle, to ensure a clear mandate within the organisation.	Identify and gather the data used and collected as well as storage type, so as to enable understanding of data taxonomy and data purpose.	Assess the impact using different impact categories if confidentiality (C), integrity (I) or availability (A) parameters are compromised.	Design and implement protection controls within the systems according to the categories assigned and data lifecycle.	Monitor, measure, analyse and evaluate the DMF components implemented to keep it up-to-date and optimised.

ASEAN
Data Management Framework

Singapore's PDPA & Trustmark Certification (2018)

Data Protection Trustmark momentum to gather in 2020

Singapore

- 42 organisations with DPTM (2020) - expected to increase in 2021 but growth may be restricted to stringent operational requirements and longer process needed to achieve certification that might discourage many organisations
- Misconception that DPTM certification can be achieved easily,
- Also high expectations to maintain quality of safeguards could be another barrier. It takes at least 3 months or more to attain DPTM certification;
- Emergence of many service providers offering DPTM services including law firm but lack the practical know-how and experience

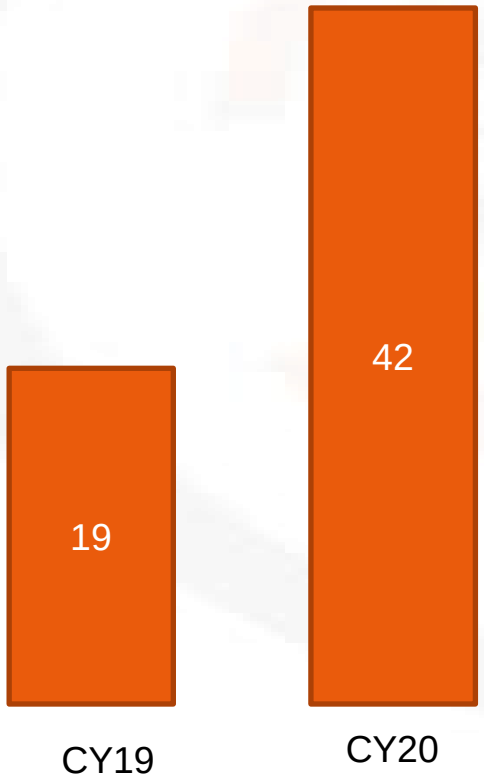
Philippines
Trustmark certification currently in discussions and planning.

Strong Adoption of Data Protection Trustmark but not CBPR

SINGAPORE

# of Organisations Awarded with DPTM (cumulative)

Number Doubles +121%

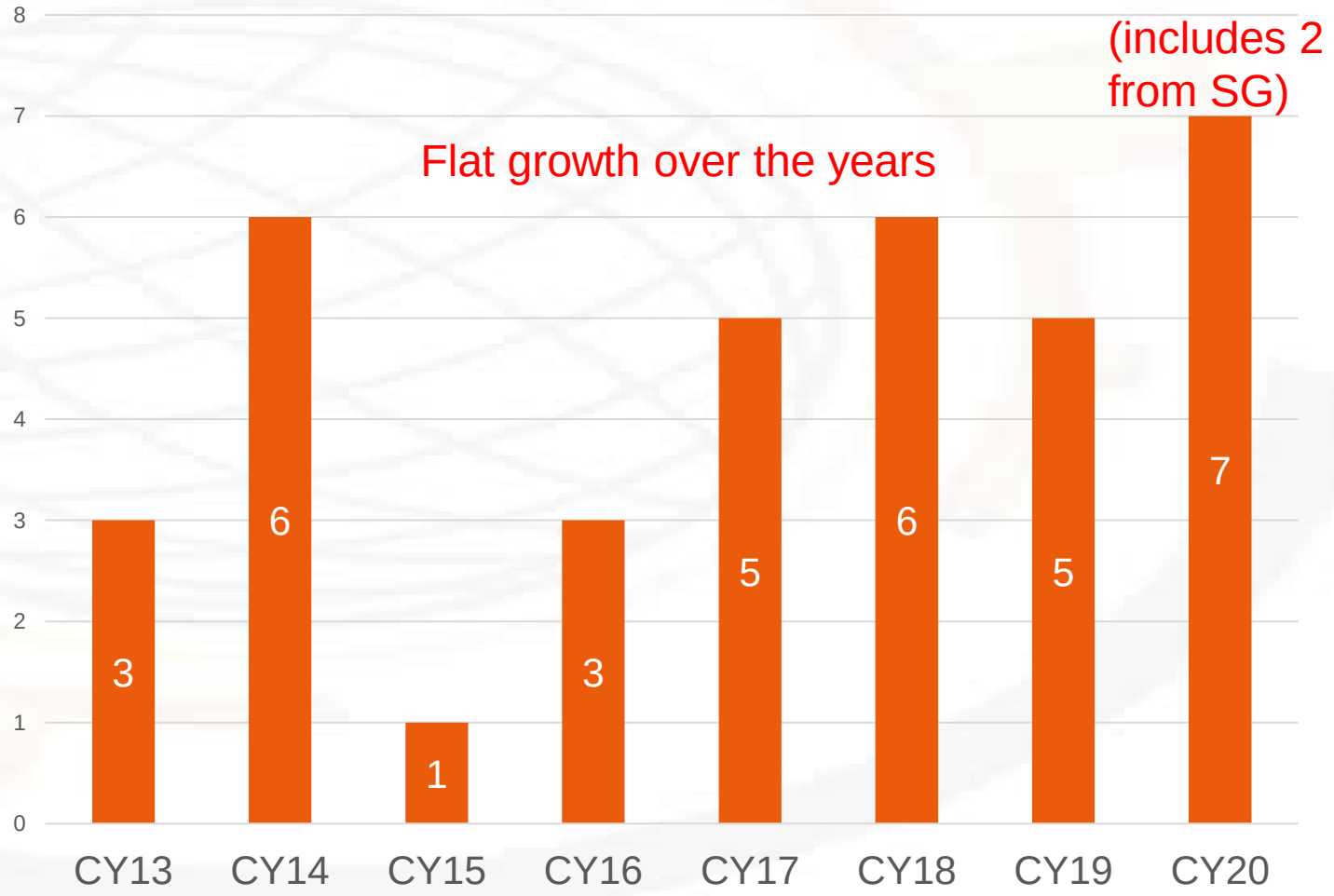


APEC

# of Orgs with CBPR Certifications

Flat growth over the years

(includes 2 from SG)



Continued momentum of certification both at corporate and individual level

Individual Professional Certification / Qualifications

National Education Programmes for DPOs

Singapore - Practitioner Certificate in Personal Data Protection
To enhance the capabilities of Data Protection Officers (DPOs) in organisations, a two-day preparatory course - "Practitioner Certificate in Personal Data Protection (Singapore)" - has been developed to equip them with practical data governance and data protection knowledge and skills, and learn to utilise risk-based tools to establish a robust data protection infrastructure for their organisation.

Includes computer-based examination that participants can take after the completion of their course to obtain the Practitioner Certificate for Personal Data Protection (Singapore), co-issued by the PDPC and the International Association for Privacy Professionals (IAPP).

Philippines – The National Privacy Commission (NPC) today unveiled its DPO Accountability, Compliance, and Ethics (ACE) Program, aimed at establishing a skills benchmark for local privacy professionals, amid the spike in demand for high-quality data privacy trainings in the country.

The ACE DPO Program has three levels and comprises advanced case studies, practical, and written exams. Those who successfully passed will be issued a certificate reflecting their DPO skills level. Thus, ACE-1, ACE-2, and ACE-3.

ISO 27701 Courses available

ISO/IEC 27701 Lead Auditor (Privacy Information Management System) - 5 days (Self-learning)

This self-learning programme will provide the knowledge and skills to plan and carry out audits in compliance with ISO 19011 and ISO/IEC 17021-1 certification process. Acquire knowledge on the protection of privacy in the context of processing personally identifiable information (PII), as well as master audit techniques and become competent to manage an audit program, audit team, establish communication with customers and resolve potential conflicts.

Days **USD 1200.00**

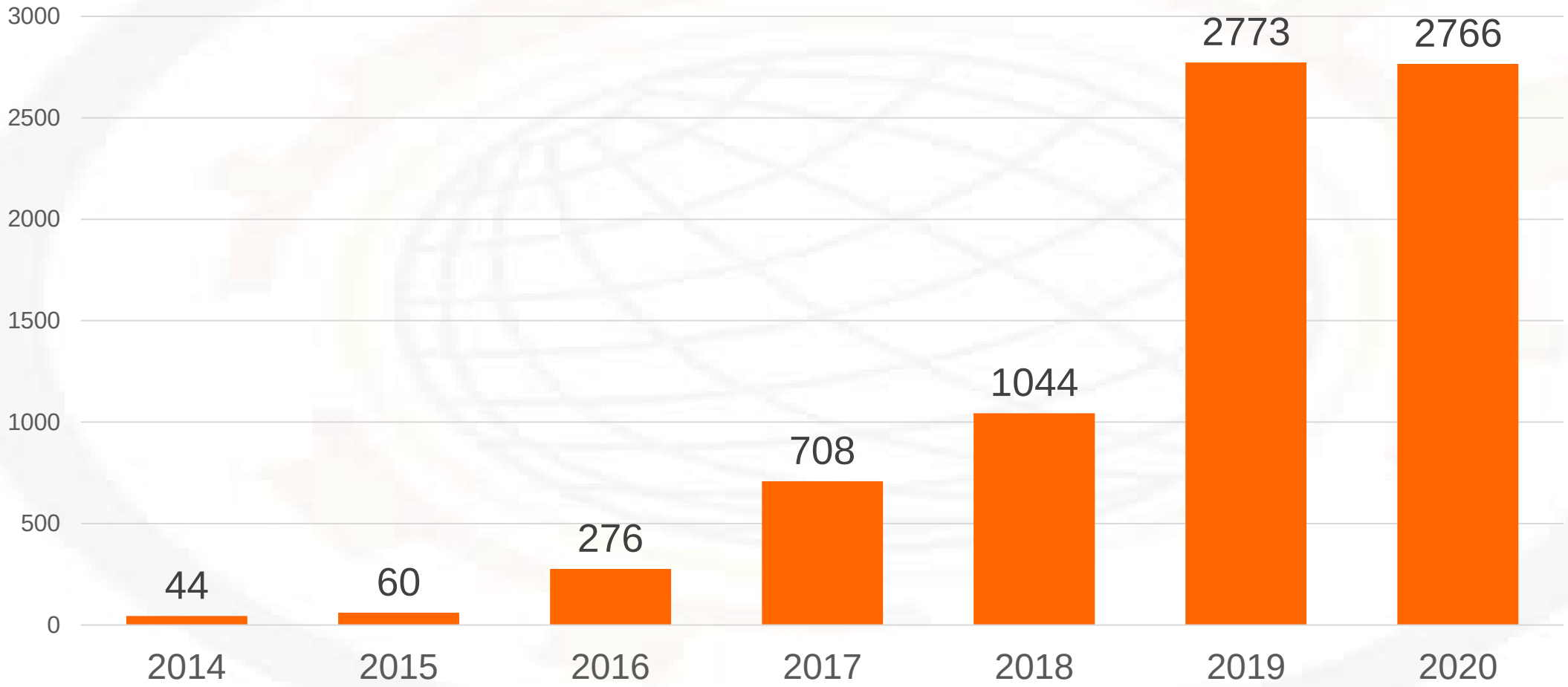
ISO/IEC 27701 Lead Implementer (Privacy Information Management System) - 5 days (Self-learning)

This self-learning programme is designed to prepare its candidates to implement a Privacy Information Management System (PIMS) in compliance with the requirements and guidance of the ISO/IEC 27701. Gain a comprehensive understanding of the best practices of privacy information management and learn how to manage and process data while complying with various data privacy regimes.

Days **USD 1200.00**

Data Protection Learning Roadmap - 3 Different Routes

Number of Participants in Adult Learning on Data Protection – Singapore Management University & Straits interactive



Despite impact of COVID19 & Circuit Breaker in SG

Advanced Certificate in Data Protection Operational Excellence (AC-DPOE)

For DPO/Career Advancement

START HERE

1. Data Protection Trends & the Rise of the DPO

2. A Practical Approach to Data Protection for DPOs

Practitioner Cert + PDPA Ops Or Hands-On DPO

Exempt

3. Data Protection and Privacy Programme Management

IAPP CIPM

Exempt

4. Information & Cyber Security for Managers - EXIN Certification

IAPP CIPT CISM/CISSP

Exempt

5. Adv Tech and Appln for Data Protection by Design, DPIA, DPTM

ADV CERT

(Optional)

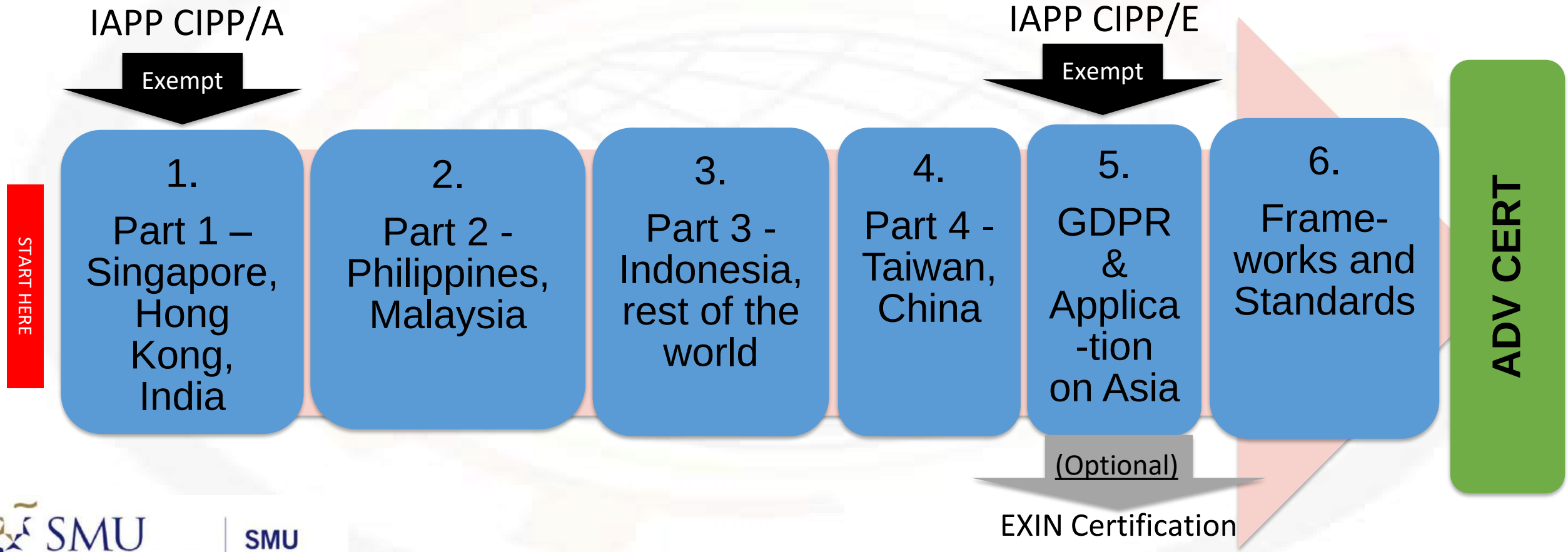
EXIN Certification

SMU SINGAPORE MANAGEMENT UNIVERSITY | SMU Academy

Note - Modules can be taken in any sequence or as separate modules

Advanced Certificate in Data Protection Principles (AC-DPP)

For Regional DPOs & Legal/Compliance



Note - Modules can be taken in any sequence or as separate modules

GRC Route

Advanced Cert in Governance, Risk, Data Compliance

Advanced Cert in GRC

Professional Certification

Auditors, Risks Mgrs
Those involved in GRC

OCEG
International Certification

GRC P

Professional Certification Route

Awarded by International Association of Privacy Professionals (IAPP)

DPO

CIPM

The "how"
Operations

The CIPM says that you understand how to use process and technology to manage privacy in an organization—regardless of the industry or jurisdiction.

Data Protection Officers

CIPT

The "how"
Technology

The CIPT shows that your know how to manage and build privacy requirements and controls into technology.

Info-comm Professionals

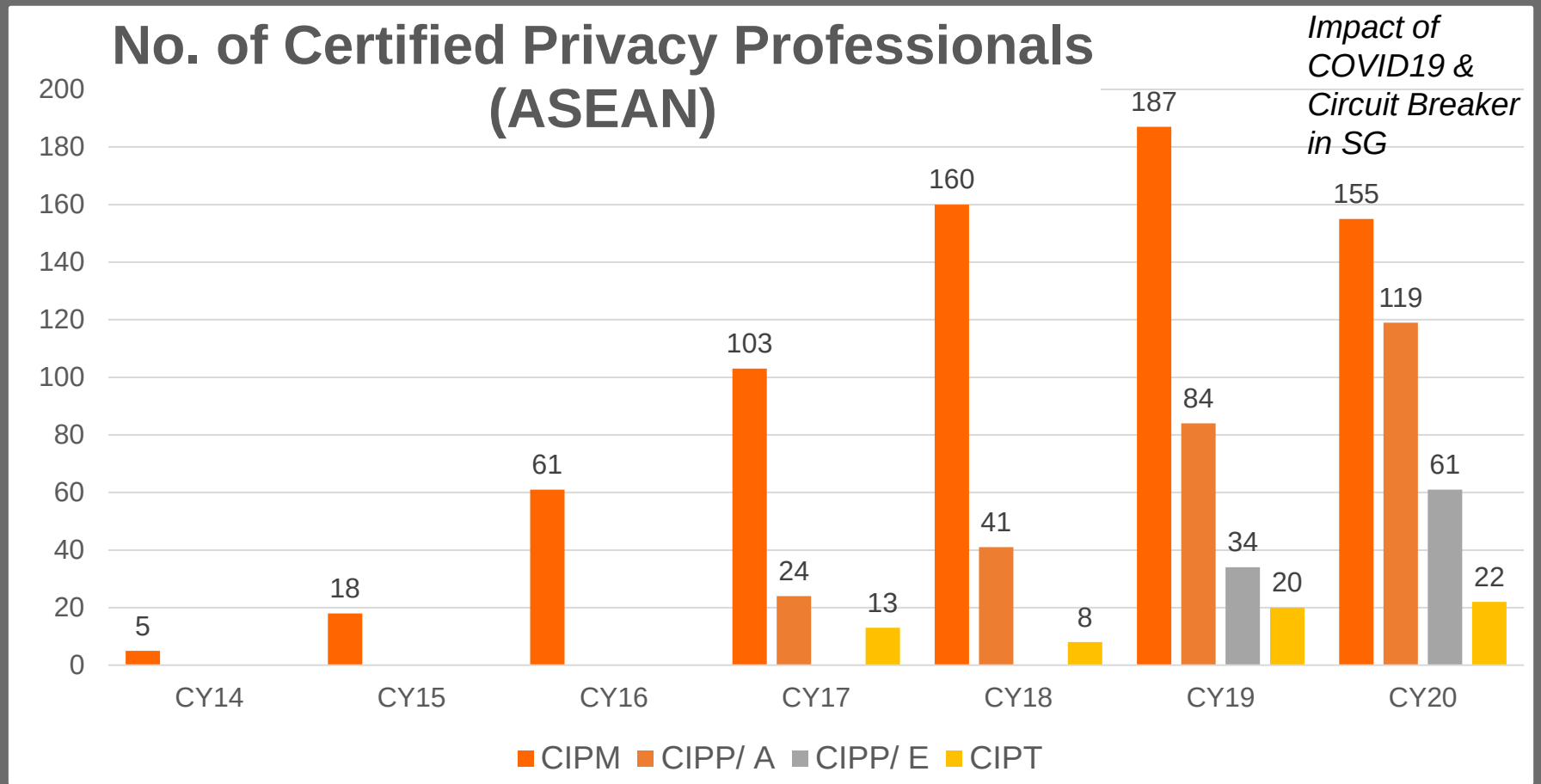
CIPP /A/E

The "what"
Laws and regulations

The CIPP shows that you understand the laws, regulations and standards of privacy in your jurisdiction or discipline.

Legal Professionals

IAPP Courses Conducted by DPEX Centre



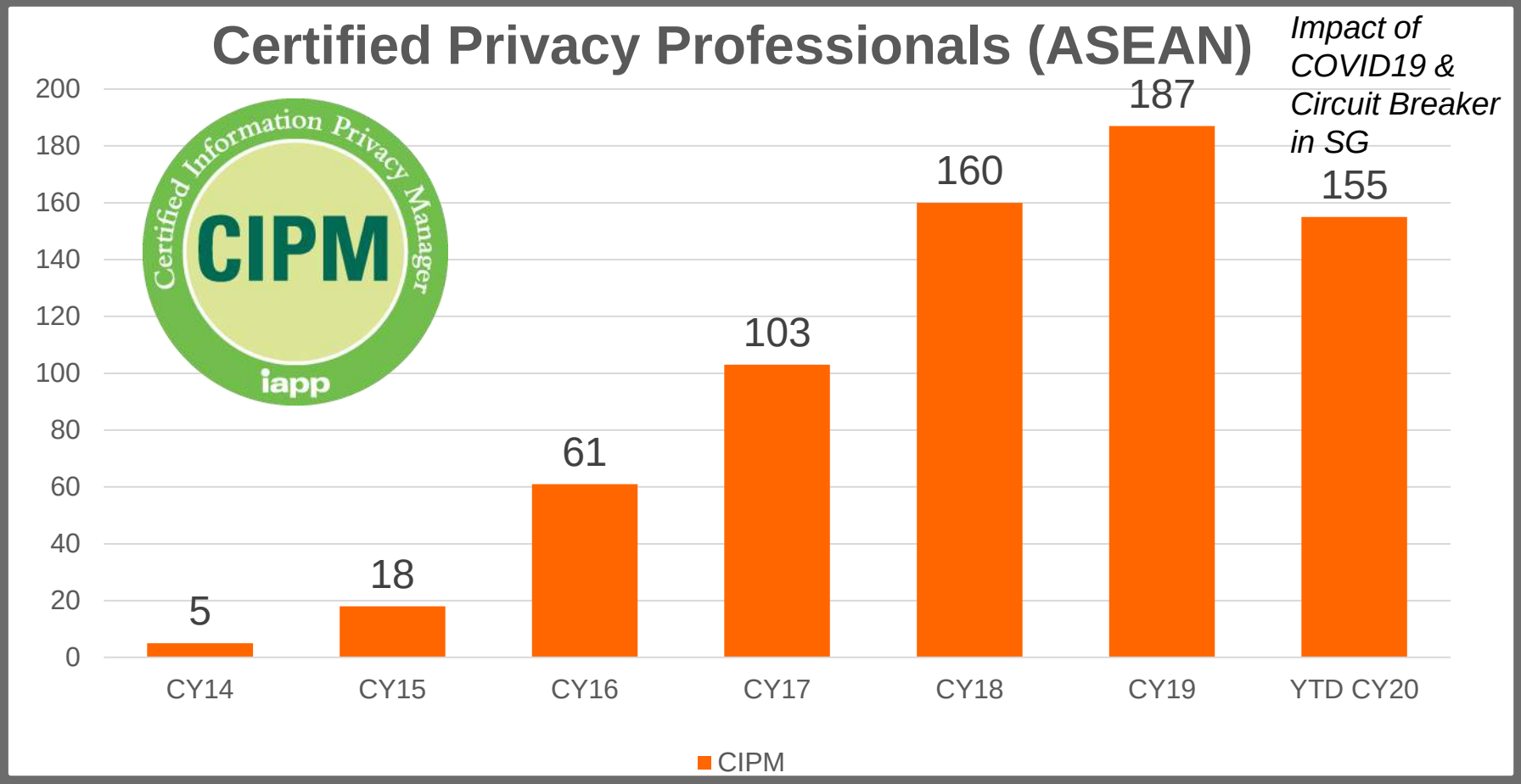
Registered participants by year with Straits Interactive/ Data Protection Excellence Centre

DPEX
DATA PROTECTION EXCELLENCE CENTRE

IAPP Courses: Distribution by Country

	CIPM	CIPT	CIPP/ A	CIPP/ E
Total	689	63	268	95
Singapore	585	62	254	70
Philippines	69	1	5	21
Malaysia	17	-	-	1
Indonesia	9	-	2	-
Others	9	-	7	3

IAPP Courses Conducted by DPEX Centre



Registered participants by year with Straits Interactive/ Data Protection Excellence Centre

DPEX
DATA PROTECTION EXCELLENCE CENTRE

5 Regional Trends in Data Protection

1. Organisations to shift from predominantly a legal approach to data protection requirements towards a holistic GRC (Governance, Risk Management and Compliance) perspective in their operations relating to personal data.
2. A renewed focus on the importance of third party management of personal data due to automation, digitalisation and WFH initiatives resulting from COVID-19.
3. While in 2021 will see continued sophisticated cyber threats and data breaches, expect more cases of data breaches involving Intrusive mobile apps as a result of COVID19 and ongoing automation.
4. 2021 will also see the European Union's GDPR and ISO 27701 firmly established as de facto standards used for operational compliance and data protection / privacy management.
5. As public awareness of data protection / privacy grows, the importance of certification both at the corporate and individual level will continue to gain momentum driven by the local data protection / privacy authorities.

DPEX
DATA PROTECTION EXCELLENCE NETWORK

www.dpexnetwork.org

LEARN EVENTS DISCUSSIONS NEWS BLOG RESOURCES PRESS

Join us as a member and continue the chat

Welcome to the Data Protection Excellence (DPEX) Network

Asia's Largest Network of Data Protection Officers and Professionals

THANK YOU!

Please refer any queries to
kevin@straitsinteractive.com

7 Regional Trends in Data Protection

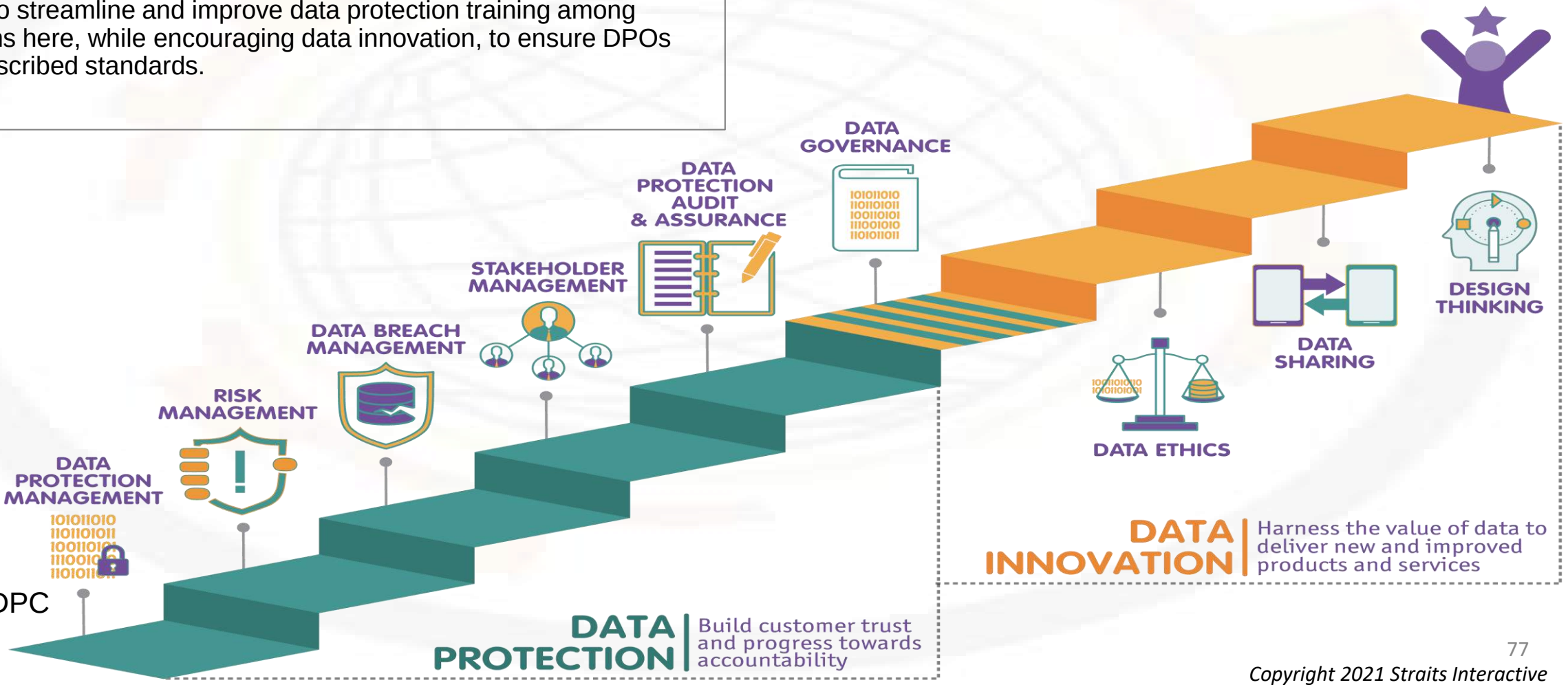
1. More intensive enforcements with increased emphasis on operational compliance amid data breaches arising from mass digitisation and improper use of privacy-intrusive technologies
2. Both the public and private sectors will continue to grapple with data protection issues and new privacy requirements
3. Continued importance and applicability of GDPR to ASEAN
4. Shift from local to regional compliance for organisations with multiple regional presence
5. Significant rise in demand for data protection expertise and professional certification
6. Emphasis on data protection audits as well as increased adoption of data protection certification frameworks and trustmarks.
7. Emergence of established and new players in the ASEAN region offering data protection services and solutions

Competency Framework & Training Roadmap for DPOS

World-first framework spells out role, training for data protection officers

Published17 JULY, 2019UPDATED 18 JULY, 2019

The aim is to streamline and improve data protection training among organisations here, while encouraging data innovation, to ensure DPOs achieve prescribed standards.



Source: PDPC

Competency and Proficiency Level for Each Job Function

Competency	Job Function		
	DP Executive	DPO	Regional DPO
Data Protection Management	Level 1	Level 2	Level 3
Risk Management (Data Protection)	Level 1	Level 2	Level 3
Data Breach Management	Level 1	Level 2	Level 3
Stakeholder Management	Level 1	Level 2	Level 3
Data Protection Audit & Assurance*	Level 1	Level 2	Level 3
Data Governance		Level 2	Level 3
Data Ethics*		Level 1	Level 2
Data Sharing*		Level 1	Level 2
Data-driven Design Thinking*		Level 1	Level 2

**Competency may not be required depending on the organisation's needs.*

Source: PDPC

Amendment of the DPA

Amendment Bills Introduced

- House Bill No. 1188 Rep. Michael L. Romero (increasing penalties)
- House Bill No. 5612 Rep. Victor A. Yap (substantive amendments) Referral to the Committee on Information and Communications Technology on 2019-11-27

Definition of Terms

Item	Current	Amendment
Personal Data Breach (IRR Rule I Sec 3 k)	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information transmitted, stored or otherwise processed.
Notification requirement (IRR Rule V Sec 15)		PIP to notify NPC and data subjects if PIC is outside of the Philippines and unable to comply with notification requirement

Definition of Terms

Item	Current	Amendment
Personal Information Controller (IRR Rule I Sec 3 m)	Personal information controller refers to a NATURAL OR JURIDICAL person, or any other body who controls the processing of personal data or instructs another to process personal data on its behalf.	Personal information controller refers to a NATURAL OR JURIDICAL person, PUBLIC AUTHORITY, AGENCY OR OTHER ENTITY WHICH, ALONE OR JOINTLY WITH OTHERS, DETERMINES THE PURPOSES AND MEANS OF THE processing of personal information, including a person or organization who instructs another person or organization to process personal information on his or her behalf.

Definition of Terms

Item	Current	Amendment
Sensitive personal information (IRR Rule I Sec 3 t)	(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) Specifically established by executive order or an act of Congress to be kept classified.	(1) About an individual's RACIAL or ethnic origin, religious, philosophical BELIEF, LABOR or political affiliations; (2) About an individual's health, genetic DATA, BIOMETRIC DATA, sexual life, SEXUAL ORIENTATION OR GENDER IDENTITY, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) ABOUT AN INDIVIDUAL'S FINANCIAL DATA; (4) Issued by government agencies peculiar to an individual which includes, but not limited to, IDENTIFICATION NUMBERS, social security numbers, previous or current health records, licenses and tax returns; (5) Specifically established by LAW, REGULATION OR executive order to be classified OR CONFIDENTIAL, INCLUDING THOSE THAT CONSTITUTE PRIVILEGED COMMUNICATION.

Scope

Item	Current	Amendment
Scope (IRR Rule II Sec 4) This act does not apply to the following: (new provisions)		(F) Processing of information necessary in order to carry out the functions of law enforcement or regulatory authorities, including the performance of the functions of the independent, central monetary authority and information sharing necessary for the investigation and prosecution of child pornography and other forms of child exploitation, in accordance with their constitutionally or statutorily mandated function: Provided, That protection of fundamental freedoms are guaranteed; (G) Processing of information by courts acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks; (H) Processing of information by a natural person for purpose of a purely personal or household activity;
		Provided, that the reasonable freedom granted by this Act do not extend to PICs or PIPs, who remain subject to the requirements of implementing security measures for personal data protection: Provided further , that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity.

Scope

Item	Current	Amendment
Extraterritorial Application (new provision)		The processing of personal information relates to a Philippine citizen or resident who are in the Philippines, where the processing activities of a natural or juridical person outside the Philippines involves offering of goods or services or monitoring of behavior within the Philippines.
		Rationale: Provides clear instances when processing of personal information of Philippine citizens or residents which are done outside of the Philippines is covered by the law.

Functions

Item	Current	Amendment
Functions of the National Privacy Commission (IRR Rule III Sec 9) - new		The Commission shall have primary jurisdiction over cases involving violations of the DPA.
		Issue summons, subpoena and subpoena duces tecum and to hold and punish for contempt those who disregard orders or writs
		Impose administrative sanctions, including monetary penalties for the violation of the DPA, its IRR, and NPC issuances or for failure or refusal to comply with compliance orders/resolution
		Conduct seminars, conferences and trainings for awareness and capacity building in relation to its mandate, and for this purpose may collect reasonable fees.
		Perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection, to protect data subjects, and to ensure effective implementation of the DPA.
		Others: 1. Administrative fines not to exceed P5M/violation 2. Imposition of the administrative sanctions or award of civil indemnity – without prejudice to the filing of criminal charges.

Organizational Structure

Item	Current	Amendment
Organizational Structure (DPA Chapter II Sec 9)	The Privacy Commissioner and the two (2) Deputy Privacy Commissioners shall be appointed by the President of the Philippines for a term of three (3) years and may be reappointed for another term of three (3) years.	The Privacy Commissioner and the two (2) Deputy Privacy Commissioners shall be appointed by the President of the Philippines for a term of four (4) years and may be reappointed for another term of four (4) years.
		Vacancies in the Commission shall be filled in the same manner in which the original appointment was made: Provided, That in case of expiration of term and no Commissioner or Deputy Privacy Commissioner is appointed, the Commissioner or Deputy Privacy Commissioner, as the case may be, shall hold office in a hold-over capacity until such appointment shall have been duly issued.
		That in case a vacancy occurs before the expiration of the term of office, the appointment to such vacancy shall only be for the unexpired term of the predecessor.

Criteria for Lawful Processing

Item	Current	Amendment
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 12 a)	The data subject has given his or her consent;	The data subject has given his or her consent: Provided, That in the specific case of information society providers offering services directly to a child, the processing of the personal information of a child shall be lawful where the child is more than 15 years old. Where the child is 15 years old or below, such processing shall be lawful only if and to the extent that consent is given or authorized by persons exercising parental authority over the child.
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 13 a)	The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;	The data subject has given his or her consent, or in the case of privileged information, all parties to the exchange have given their consent prior to processing, except if a specific law provides that the prohibition from processing may not be lifted by the data subject;
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 12 b)	The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;	The processing of information is pursuant to a contract freely entered into by the data subject and personal information controller: Provided, That the performance of the contract or provision of the service is not made conditional on consenting to the processing of sensitive personal information that is not necessary to the object of the contract;

Criteria for Lawful Processing

Item	Current	Amendment
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 13 b)	The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information; Provided, further, that the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;	The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments or its implementing rules guarantee the protection of the sensitive personal information through appropriate security measures;
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 12)		The processing is carried out with appropriate safeguards by a foundation, association or any other not-for profit body with a charitable, religious, professional or similar purpose, in the course of its legitimate activities and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and that the personal information are not disclosed outside that body without the consent of the data subjects;
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 12)		The processing relates to information which are manifestly made public by the data subject: Provided that further processing shall not be contrary to law, morals, good customs, public order or public policy;

Criteria for Lawful Processing

Item	Current	Amendment
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 13 e)	The processing is necessary for purposes of medical treatment, is carried out a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured:	The processing is necessary for the purpose of medical diagnosis and treatment, preventive or occupational medicine, and the management and quality assurance of health or social care systems and services, and is carried out by a health care institution, health care provider, or a person under their responsibility bound by a professional or legal obligation of confidentiality;
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 13)		The processing is necessary for reasons of public interest in the area of public health or humanitarian emergencies: Provided, that such processing is covered by regulatory enactments ensuring necessity of processing and implementation of appropriate safeguards for data protection;
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 13)	The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.	The processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or WHENEVER COURTS ARE ACTING IN THEIR JUDICIAL CAPACITY;

Criteria for Lawful Processing

Item	Current	Amendment
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 13)		The processing is necessary solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, to the extent proportionate to the aim pursued and consistent with ethical principles, which shall provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
Criteria for Lawful Processing of Personal Information (DPA Chapter III Section 13)		The processing pertains to information originally collected from residents of foreign jurisdictions being processed in the Philippines: Provided, that the collection is in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws;

Administrative Sanctions

Item	Current	Amendment
Use of administrative fines and fees		For a more effective and expeditious implementation of this Act, the Commission shall be authorized to retain, without need of a separate approval from any government agency, subject only to the existing accounting and auditing rules and regulations, all the fees, fines, royalties and other charges, collected by the Commission, for use in its operations, like upgrading of its facilities, equipment outlay, human resource development, and the acquisition of the appropriate office space, among others, to improve the delivery of its services to the public.