

Cybersecurity Act and Personal Data Protection Act Series

Personalized Marketing vs. Data Privacy

PRINYA HOM-ANEK

CISSP, CSSLP, SSCP, CASP, CFE, CBCI, CGEIT, CRISC, CISA, CISM, CSX, ITIL Expert,
COBIT 5 Foundation, COBIT 5 Implementation

Eisenhower Fellowships 2013, Member of (ISC)² Asian Advisory Council,
ISACA Bangkok, Thailand Information Security Association (TISA) Board Member,
Cybertron Co., Ltd. – CEO & ACIS Professional Center – Chairman of Executive Committee

ACIS/Cybertron Privacy & Cybersecurity Research LAB



ACIS PROFESSIONAL CENTER
YOUR SATISFACTION IS OUR PRIDE



We have been certified to

ISO 22301:2012 (BCMS)
ISO/IEC 27001:2013 (ISMS)
ISO/IEC 20000-1:2011 (IT-SMS)

standards.

Personalization VS Privacy

Unleashing The Privacy Paradox



Credit : <https://www.sooperarticles.com/>

IT-GRC and Cybersecurity 4.0 in Digital Economy

**Digital
Economy**

**Data
Economy**

**Data
Science**

**Data
Privacy**

**Data
Governance**

**Data
Residency**

**Digital
Literacy**

**Mobile/
Social Media
Services**

**Internet of
Things (IoT)**

**Information of
Things**

**Big Data
Analytics**

**Data
Sovereignty**

**Cyber
Literacy**

Cloud Service

Cloud Security

Blockchain

**Crypto-
currency**

**Over-the-Top
Regulation
(OTT)**

**Cyber
Resilience**

**Cyber Drill
Cyber Range**

**Cyber
Sovereignty**

**Information &
Technology
(I&T)**

**Operational
Technology
(OT)**

**Shadow Data
Shadow IT**

Dark-side Cybersecurity, Big Data and AI

Thailand Update 2019/2020

- ▶ Privacy and Cybersecurity are Converging around the World (and in Thailand)
- ▶ Thailand Cybersecurity Act : 28 May 2019
- ▶ Thailand Data Protection Act (Thai GDPR) : Phase 1: 28 May 2019; Phase 2: 28 May 2020
- ▶ Thailand SEC 's Digital Asset Business Law : 14 May 2018
- ▶ NIST Cybersecurity Framework Implementation for Thai CI/CII
- ▶ ISO/IEC TR 27103 : Cybersecurity and ISO and IEC Standards (ref. NIST CSF)
- ▶ ISO/IEC 27001 (ISMS) as Fundamental Standard for Information Security and Cybersecurity
- ▶ ISO/IEC 27701, ISO/IEC 29100, GDPR, NIST Privacy Framework as Reference Principle Knowledges
- ▶ Thailand Industry is moving from Cybersecurity to Cyber Resilience
- ▶ NICE Framework (NIST SP800-181) for Cybersecurity Workforce Development
- ▶ Digital Transformation needs Cybersecurity Transformation

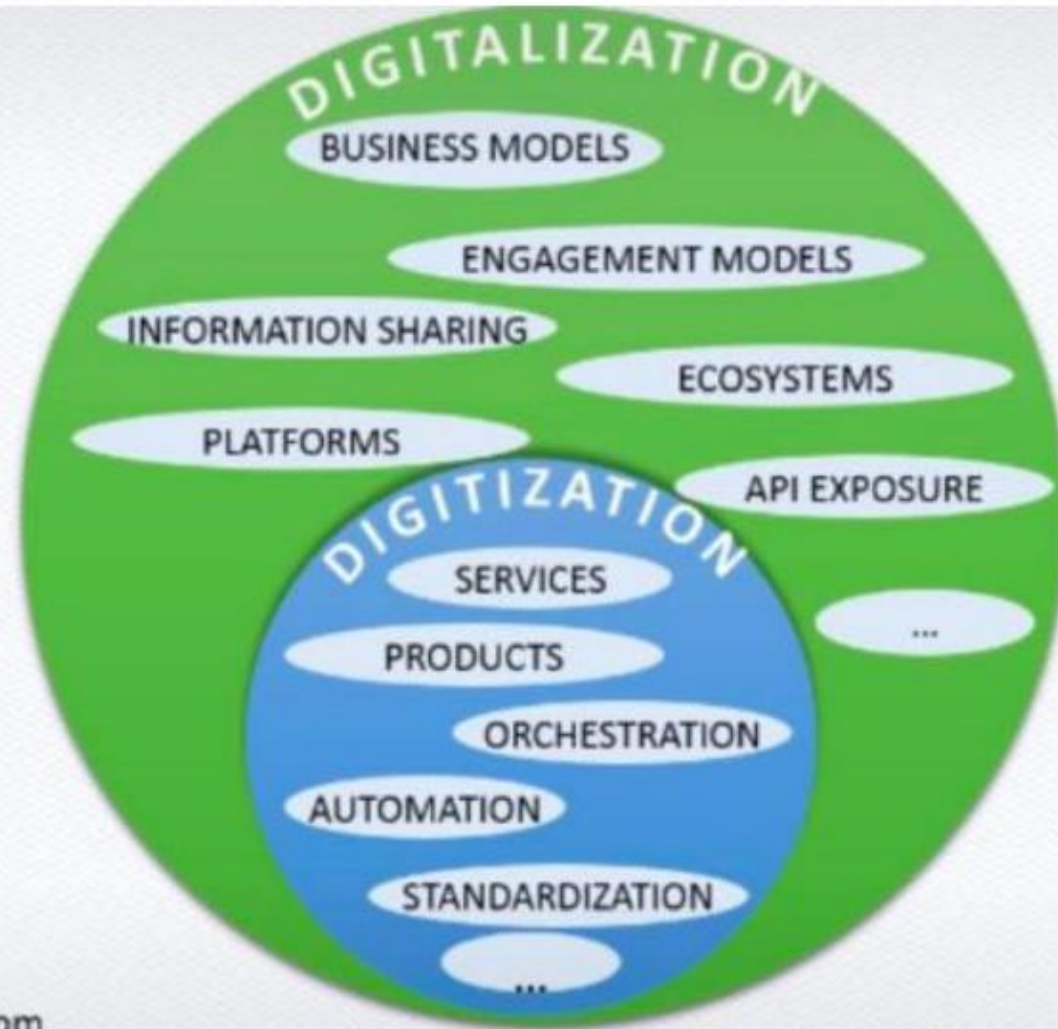
**DISRUPTIVE
TECHNOLOGY**

**THE DIGITAL
TRANSFORMATION**

Digitization

or

Digitalization



© <http://nuel.otchere.com>

IT

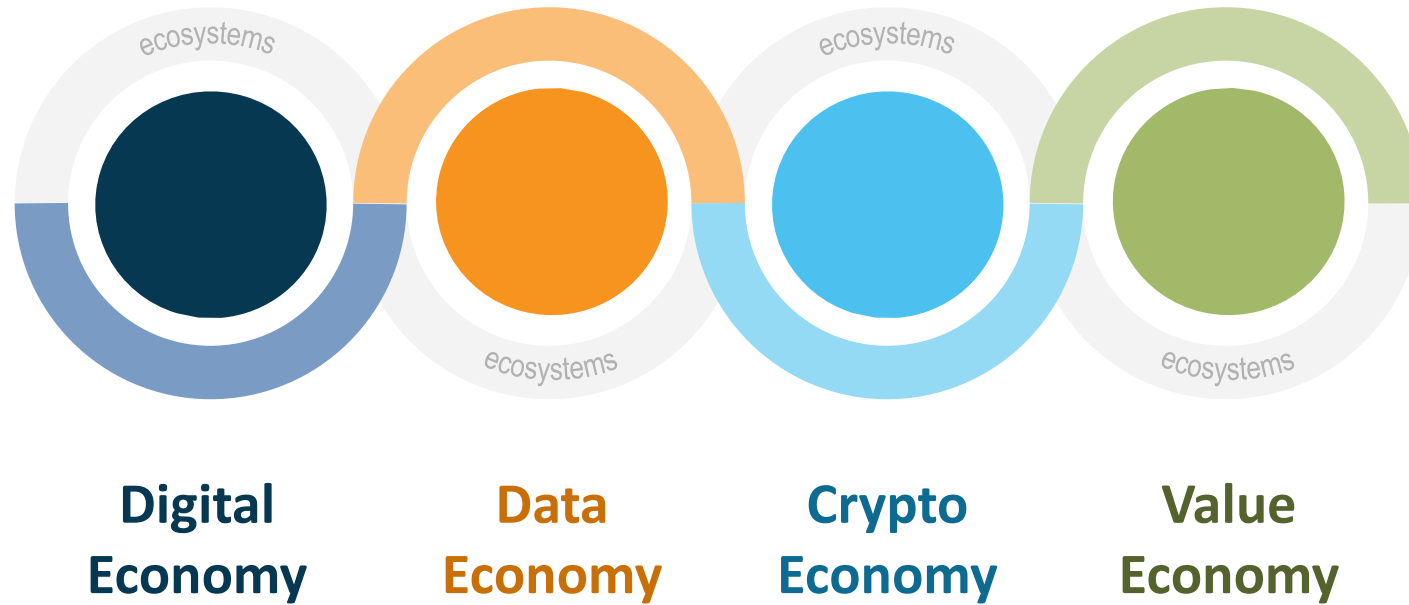
VS.

I & T

From Digital Economy to Data Economy



Digital Economy and Ecosystems



Source: ACIS Research

China's Vision of Cyber Sovereignty

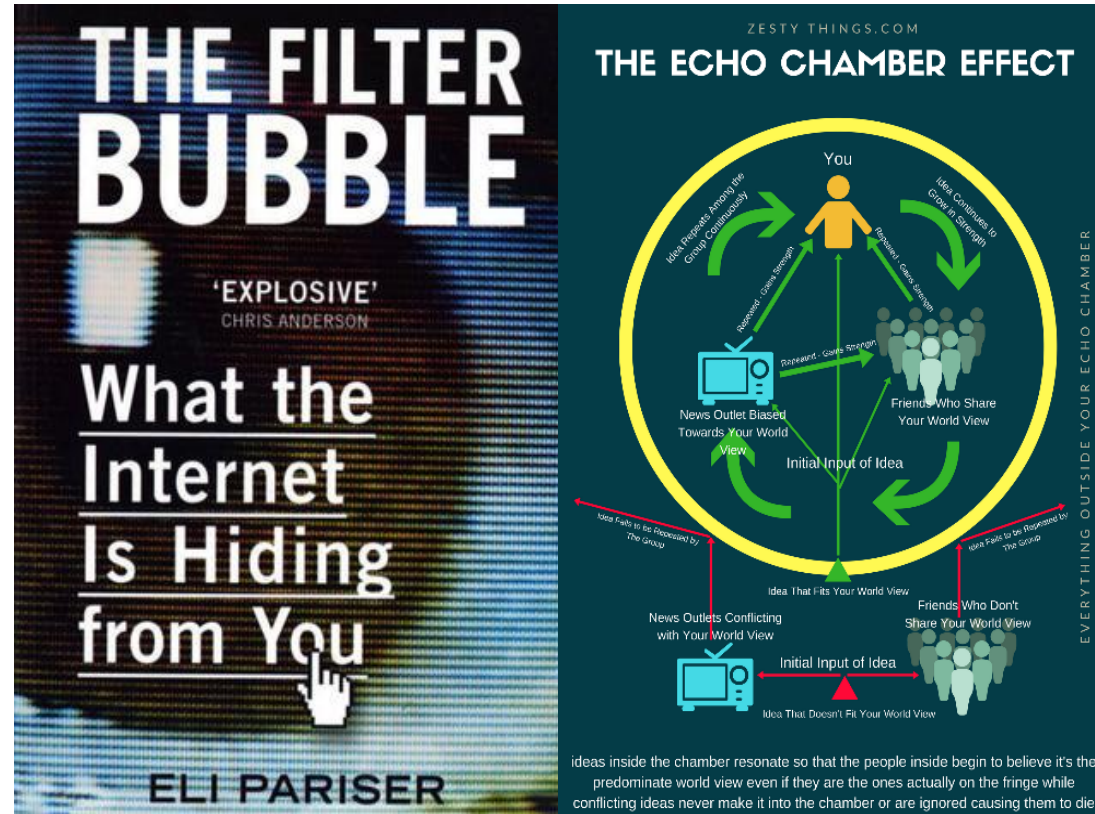
President Xi asked for China Cyber Sovereignty



"About Nation Cyber Sovereignty and Hidden Privacy Threats"



“Filter Bubble Effect and Echo Chamber Effect”



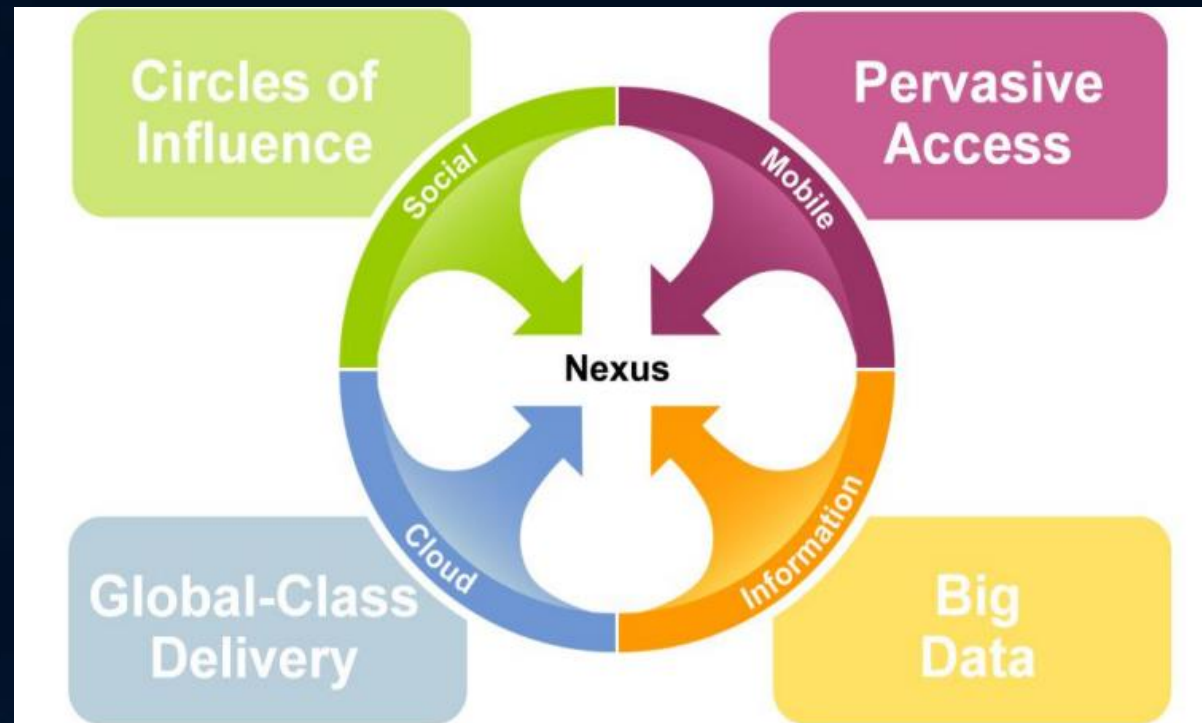
Is your Smartphone hijacking your mind?



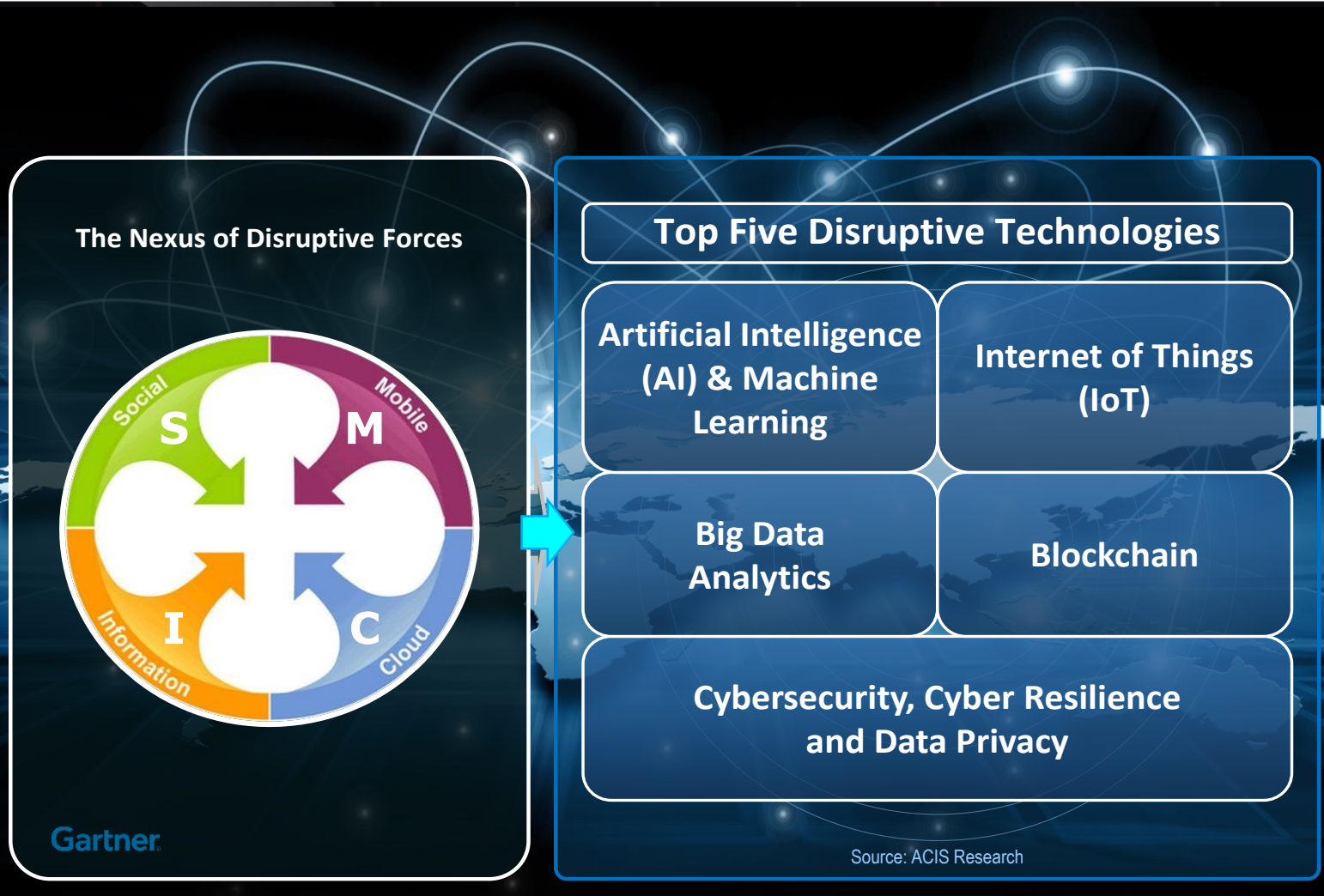
IT Trend and challenging to business

The Four IT Mega Trends : S-M-C-I Era

The Nexus of Disruptive Forces



Disruptive Technologies for Value Economy



Source: ACIS Research

Disruptive Technologies for Value Economy

Top Five Digital Disruptive Technologies

Digital Technologies

IoT
(Internet
of Things)

Big Data
Analytics

AI &
Machine
Learning

Blockchain

Cybersecurity, Cyber Resilience and Data Privacy

Regulatory Compliance

Source: ACIS Research

Top Ten Cybersecurity and Privacy Trends

2020

Top Ten Cybersecurity and Privacy Trends 2020

1. Cyber Fraud with a Deepfake

(Cyber Fraud with the Deepfake and the Dark side of AI)

2. Beyond Fake News

(It's a Real News based-on a True Story that intentionally attack someone/some organization)

3. Cyber Sovereignty and National Security Issues in the Long Run

(That include rising in state sponsor attacks; Data Sovereignty: What's Next for Data Privacy)

4. 'Cyberattack and Data Breach' : A New Normal in Cybersecurity

(Cybersecurity Mindset of Top Managements need to be changed)

5. Tighten in Cybersecurity and Data Protection Regulatory Compliance

(Focus on Cyber Resilience, Data Governance, Data Sovereignty when Value Preservation is crucial topic)

Source: ACIS / Cybertron Research LAB

Top Ten Cybersecurity and Privacy Trends 2020

6. “Data Breaches” as Top Concerns for Business

(Zero Day Exploitation, Cloud Misconfigurations including Human Errors/Digital Footprint in the Clouds)

7. Orchestration & Automation Boosting Security Staff Effectiveness

(From MSSP to MDR, Using AI and Automation to improve IR Capability)

8. Increasing on Impact of State-Sponsored Cyberattacks

(Cyberattack on Critical Infrastructure for example Energy Grids are at risk)

9. The Cybersecurity Skills Gap Crisis

(More CISOs Earning a Seat at the Table)

10. 5G Networks require New Approaches to Cybersecurity


(EU Report Highlights Cybersecurity Risks in 5G Networks: Securing the Transition to 5G)

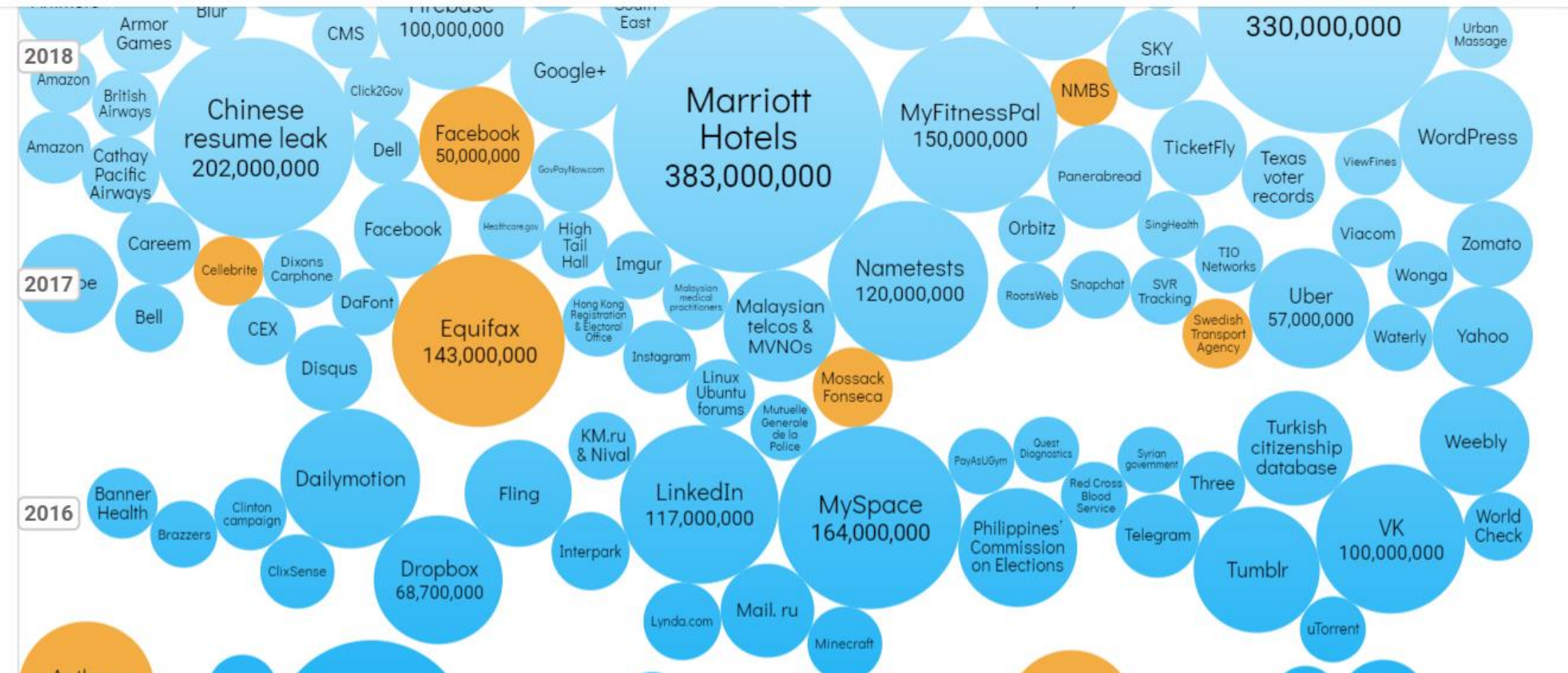
Source: ACIS / Cybertron Research LAB

1.

Top Ten Cyber Threats and Trends for 2019

information is beautiful
World's Biggest Data Breaches & Hacks

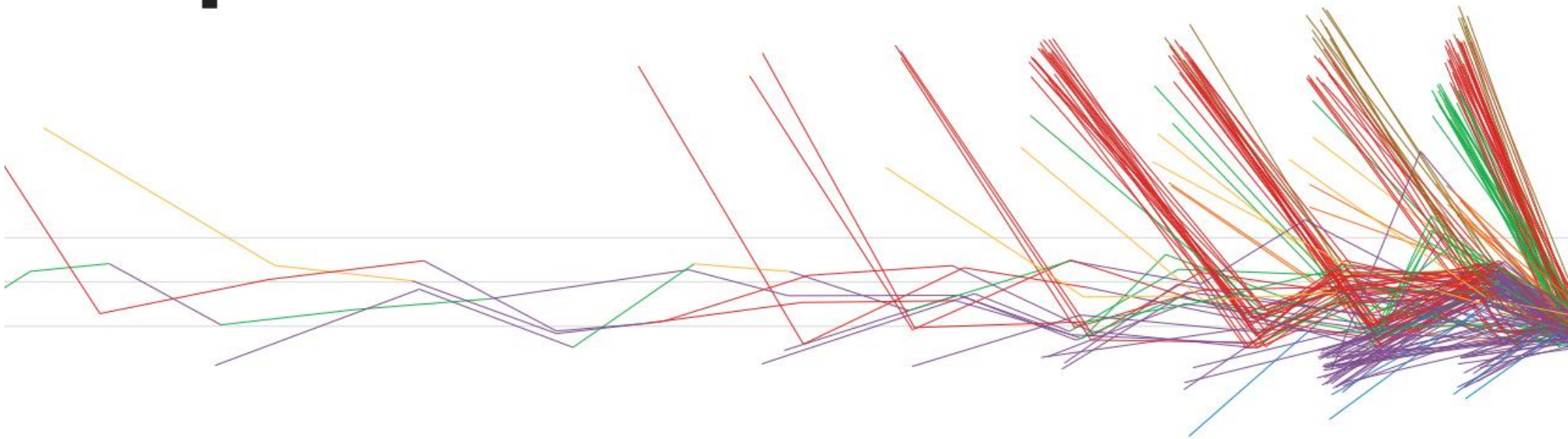
home everything about blog data training books contact 



Source <https://informationisbeautiful.net/>

2019 Data Breach Investigations Report

Executive Summary



Source <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

1.

Top Ten Cyber Threats and Trends for 2019

The Verizon Data Breach Investigations Report (DBIR) provides you with crucial perspectives on threats that organizations like yours face. The 12th DBIR is built on real-world data from 41,686 security incidents and 2,013 data breaches provided by 73 data sources, both public and private entities, spanning 86 countries worldwide.

Who is behind the attacks?

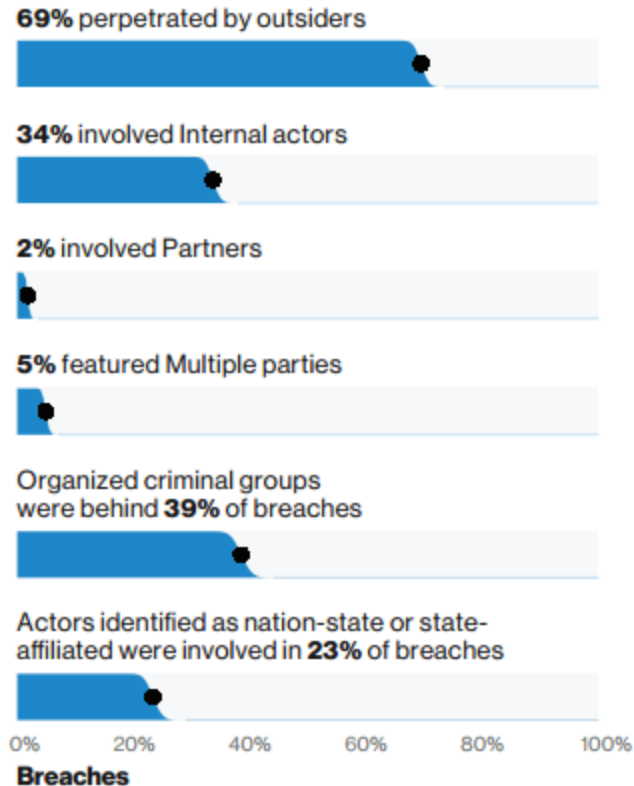


Figure 1.

What actions are being used?

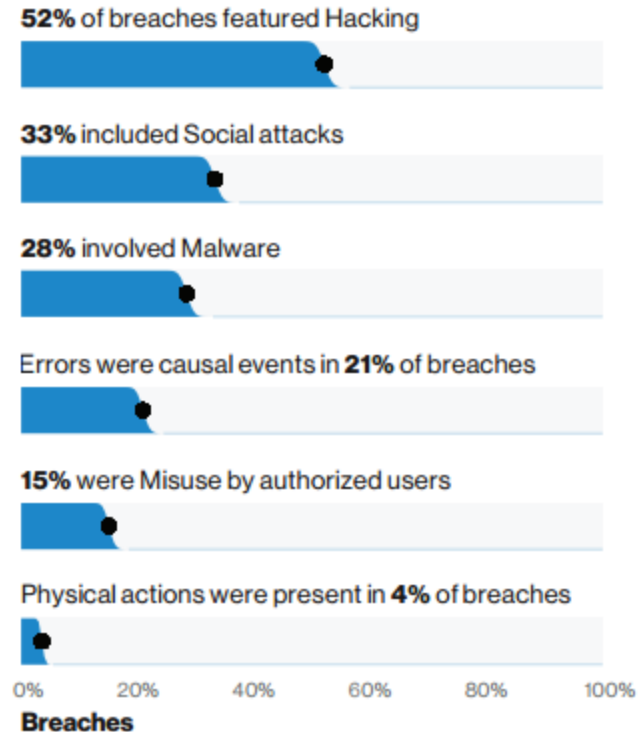
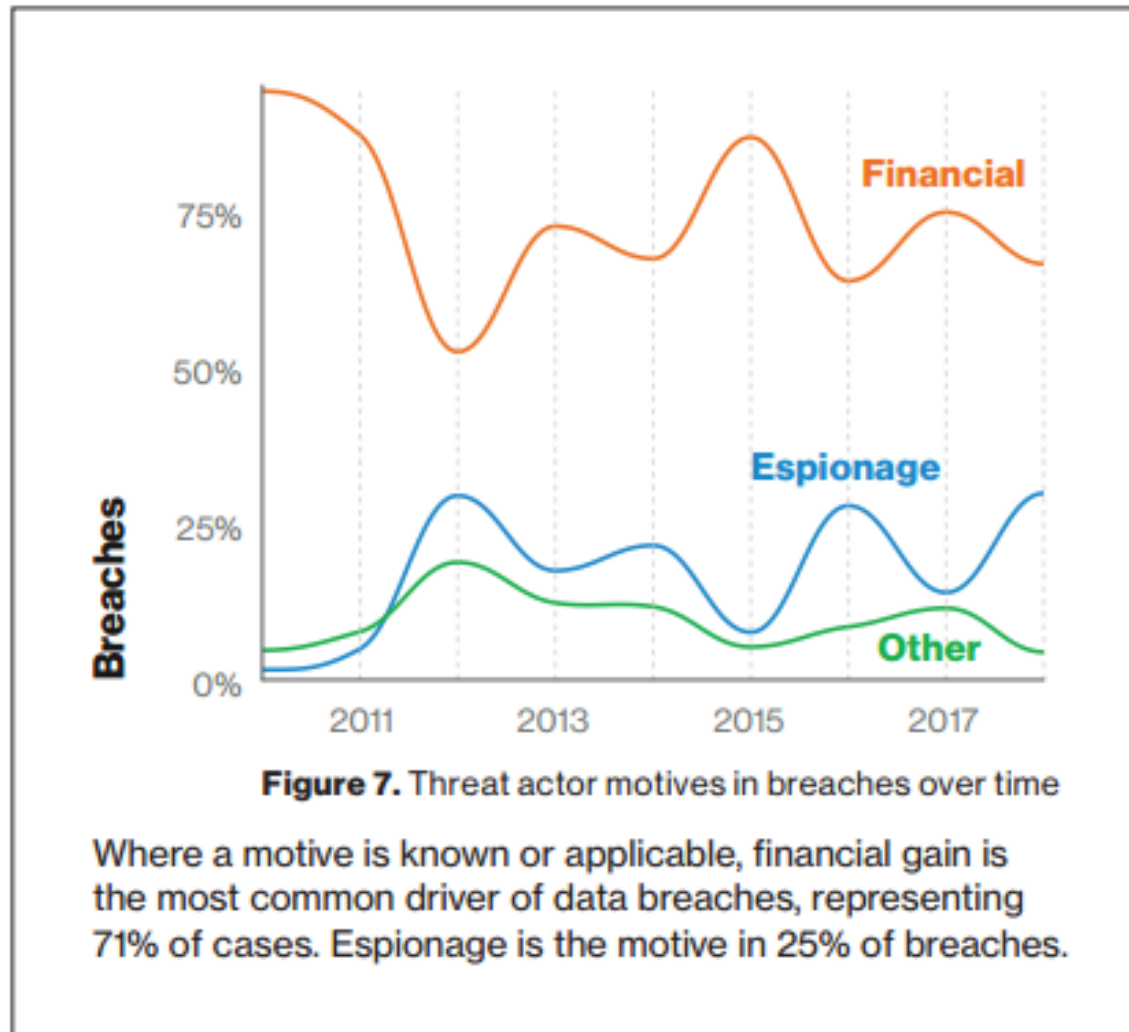


Figure 3.

Source <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>



Source <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

Financial and Insurance

Denial of Service and use of stolen credentials on banking applications remain common. Compromised email accounts become evident once those attacked are filtered. ATM Skimming continues to decline.

Frequency	927 incidents, 207 with confirmed data disclosure
Top 3 patterns	Web Applications, Privilege Misuse, and Miscellaneous Errors represent 72% of breaches
Threat actors	External (72%), Internal (36%), Multiple parties (10%), Partner (2%) (breaches)
Actor motives	Financial (88%), Espionage (10%) (breaches)
Data compromised	Personal (43%), Credentials (38%), Internal (38%) (breaches)

Source <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

1.

Top Ten Cyber Threats and Trends for 2019

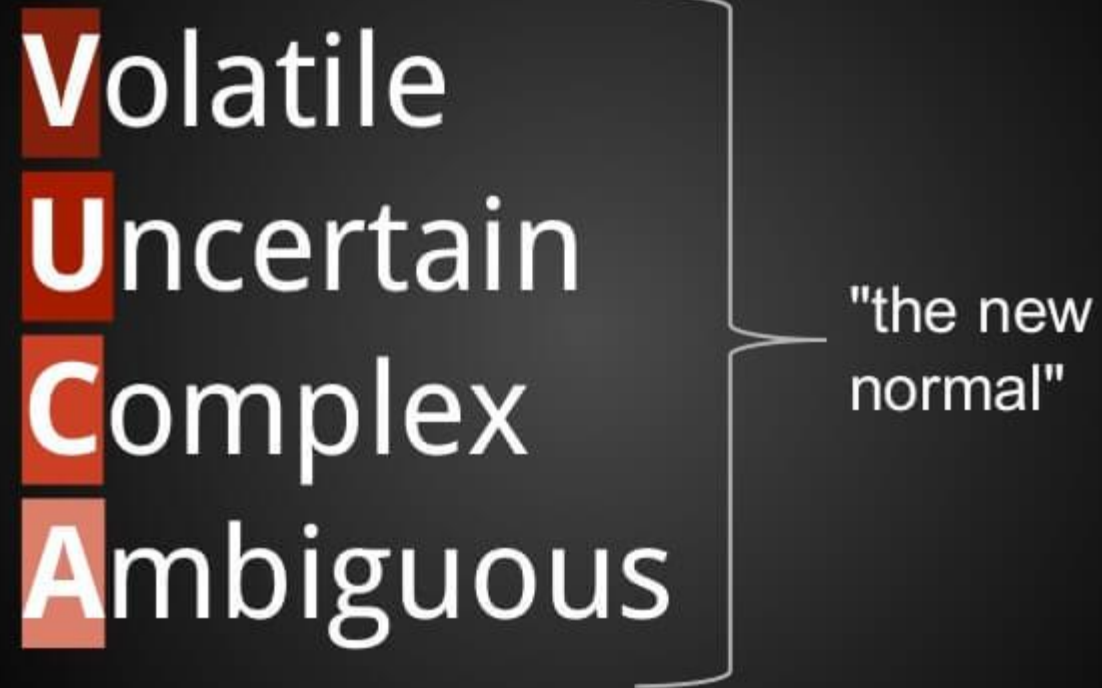
		Incidents									Breaches								
		Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)	Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)
Pattern	Crimeware	17	31	52	76	206	58	60	4,758	21	3	3	7	1	3	5	8	8	3
	Web Applications	14	30	76	71	75	40	79	93	92	14	24	70	65	45	36	73	33	88
	Privilege Misuse	1	19	100	110	14	36	13	13,021	16	1	9	45	85	7	14	10	40	14
	Everything Else	7	24	29	39	23	23	59	61	14	3	20	12	27	17	8	26	37	8
	Denial of Service		226	575	3	684	163	408	992	54							1		
	Cyber-Espionage	1	6	32	3	22	16	9	143	2	1	5	22	2	20	13	8	140	2
	Miscellaneous Errors	5	37	36	104	69	14	30	1,515	12	2	35	34	97	65	12	28	58	11
	Lost and Stolen Assets	4	9	9	62	4	5	14	2,820	7	1	3	2	28	1	2	5	16	3
	Point of Sale	40			2					10	38			2					9
	Payment Card Skimmers			21		1				10			18		1				4

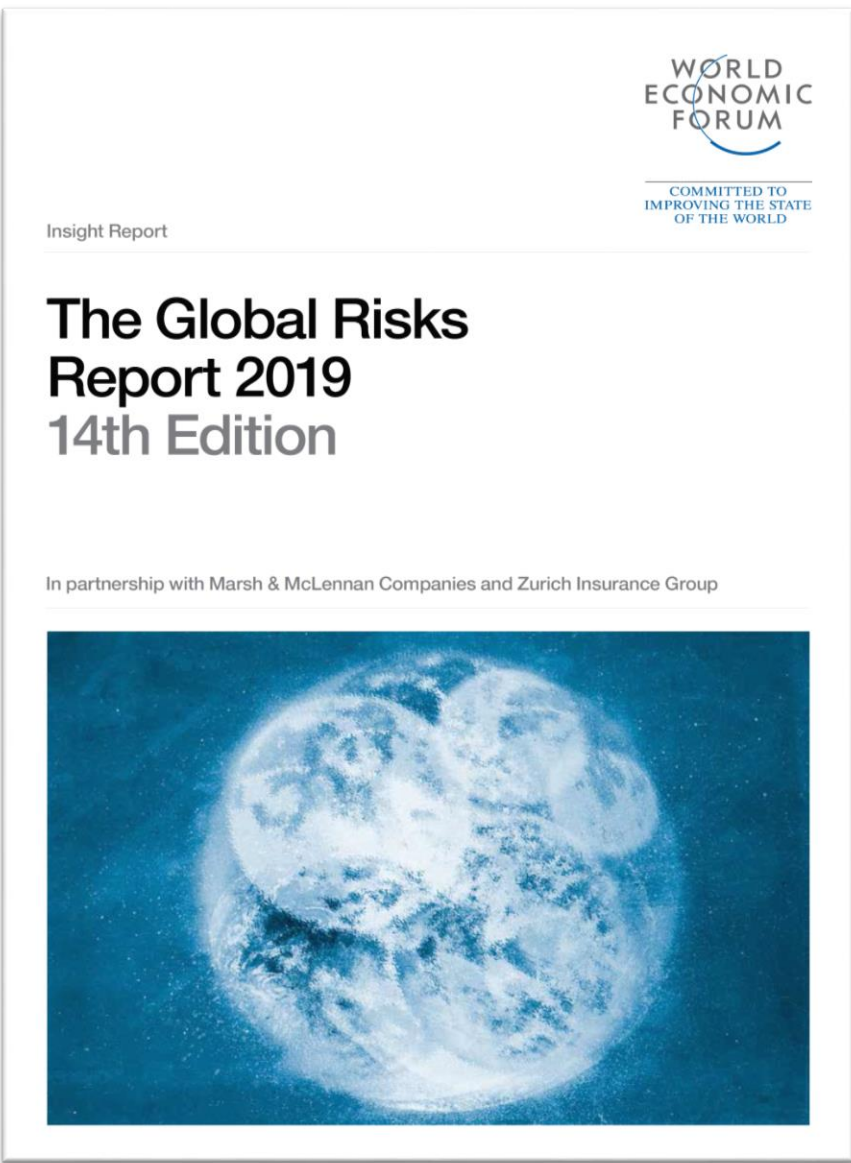
Source <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

We live in VUCA World

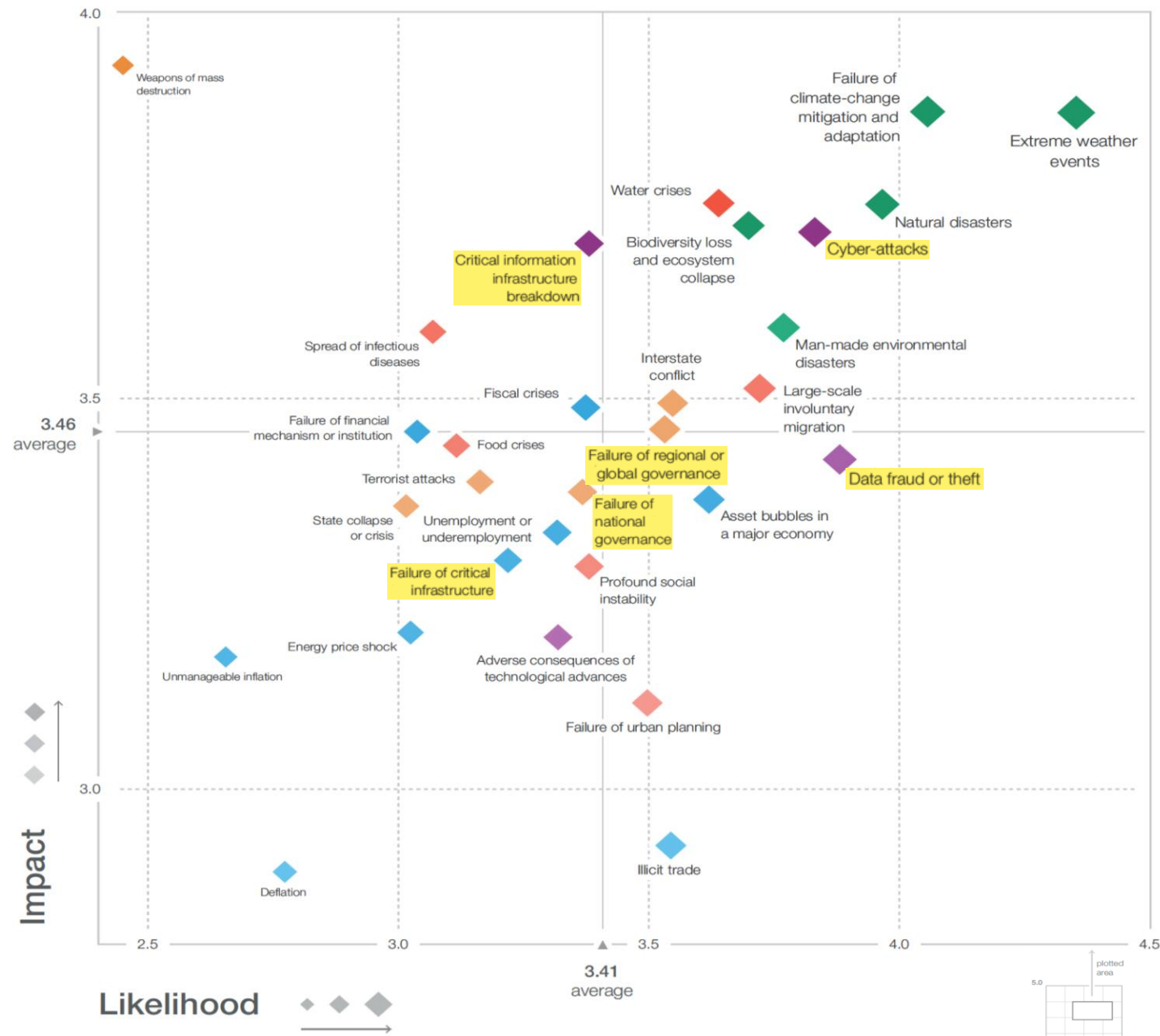
Volatile
Uncertain
Complex
Ambiguous

"the new normal"





Source: www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf



The Global Risk Outlook for 2019

THE GLOBAL RISK OUTLOOK FOR 2019

Types of Risks: ● ENVIRONMENTAL ● GEOPOLITICAL ● SOCIETAL ● TECHNOLOGICAL ● ECONOMIC

Top 5 Global Risks in Terms of **Impact**

- 1  Weapons of mass destruction
- 2  Failure of climate-change mitigation and adaptation
- 3  Extreme weather events
- 4  Water crises
- 5  Natural disasters

Top 5 Global Risks in Terms of **Likelihood**

- 1  Extreme weather events
- 2  Failure of climate-change mitigation and adaptation
- 3  Natural disasters
- 4  Data fraud or theft
- 5  Cyber-attacks

SOURCE: World Economic Forum – Global Risks Report 2019

The Global Competitiveness Index 4.0 2019 Rankings

	2018	2019
Thailand	Ranking: 38	Ranking: 40
Total score	Score: 67.5	Score 68.1

Global Competitiveness Report 2019

The 2019 edition of The Global Competitiveness Report series, first launched in 1979, features the Global Competitiveness Index 4.0 (GCI 4.0). As the decade concludes and we look towards the dawn of the 2020s, the GCI 4.0 offers insights into the economic prospects of 141 economies.

Published: Tuesday 24th of September 2019

Read Online

http://reports.weforum.org/global-competitiveness-report-2019/?doing_wp_cron=1573741998.0783989429473876953125



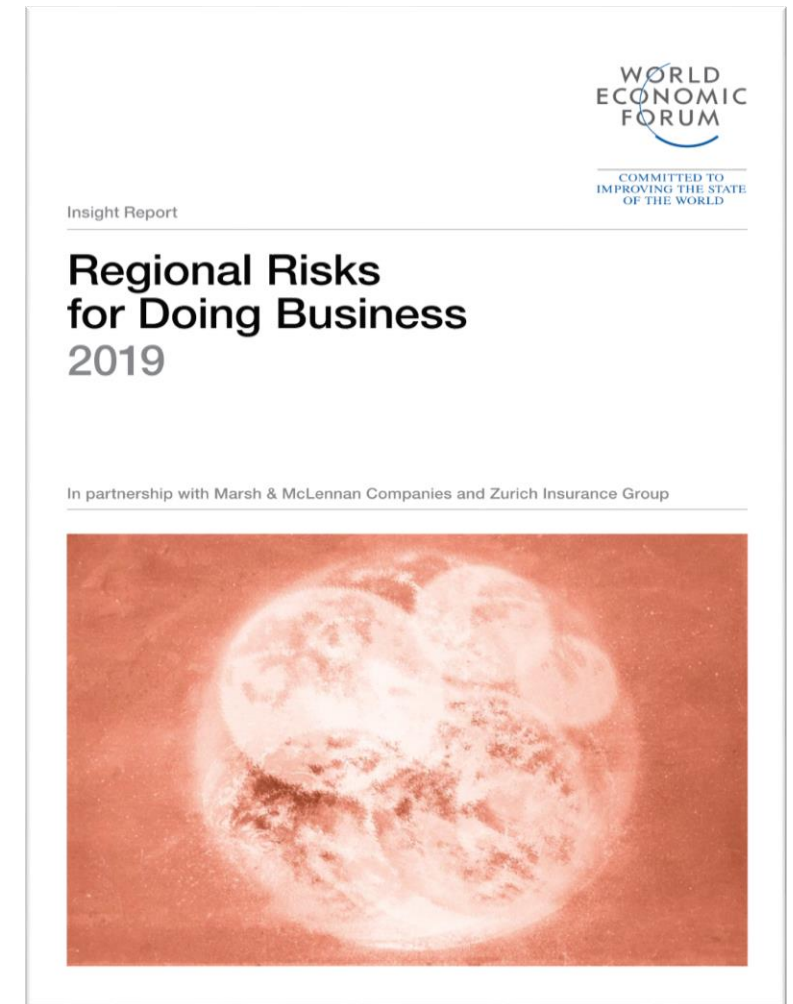
Regional Risks for Doing Business 2019

The Regional Risks for Doing Business report offers a business perspective on the impact of global risks and illustrates how they are experienced differently across regions. In an increasingly complex and intertwined world, this report helps shape the agenda for those regions aiming to play a pivotal role in the years ahead.

Published: Monday 30th of September 2019

Read Online

http://reports.weforum.org/regional-risks-for-doing-business-2019/?doing_wp_cron=1573745341.4205269813537597656250



Thailand

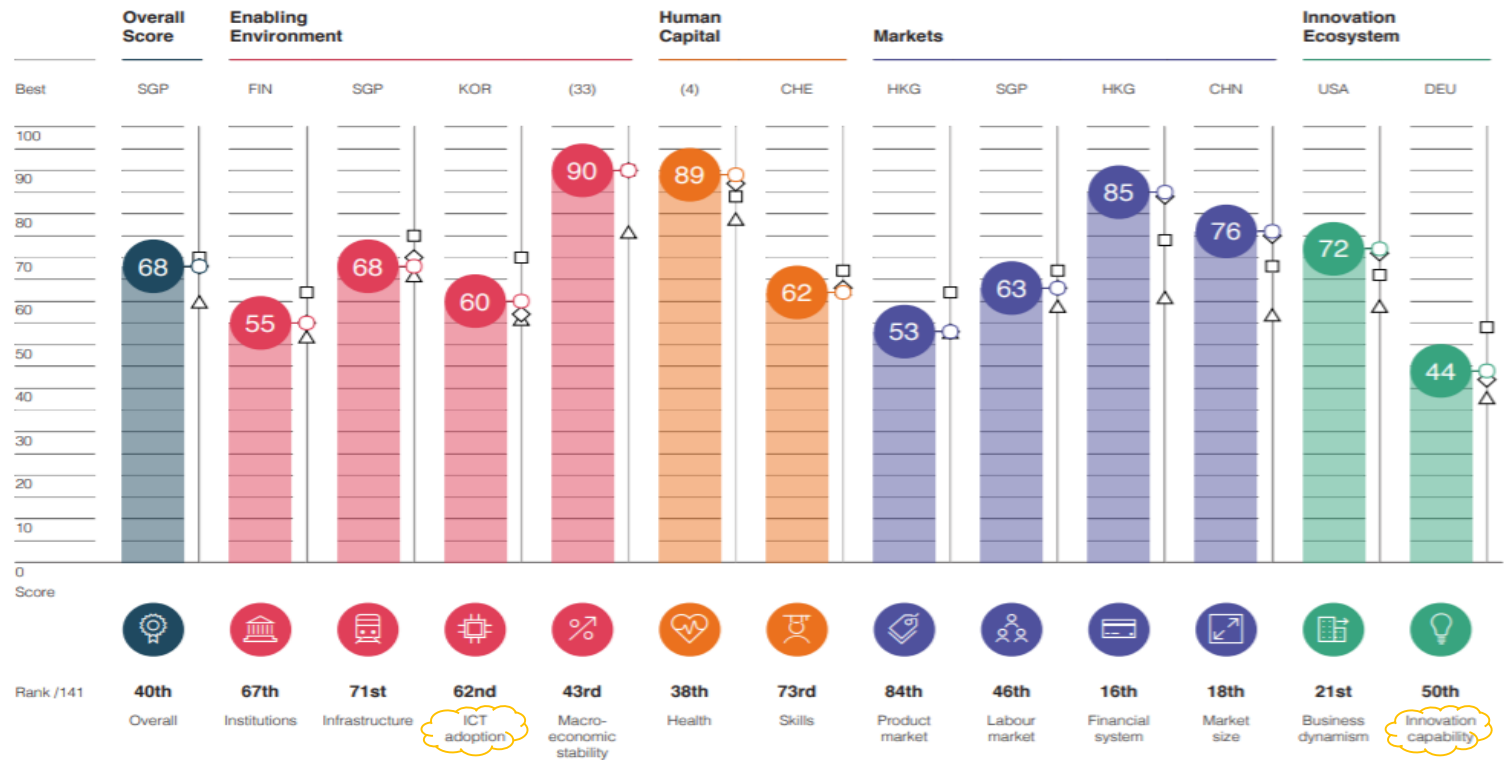
40th / 141

The Global Competitiveness Index 4.0 2019 Rankings

Global Competitiveness Index 4.0 2019 edition

Rank in 2018 edition: 38th/140

Performance Overview Key ◇ Previous edition △ Upper-middle-income group average □ East Asia and Pacific average 2019



Regional Risks for Doing Business 2019

	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Thailand	Asset bubble	Failure of national governance	Cyberattacks	Manmade environmental catastrophes	Profound social instability

Data Protection Law of The World

The screenshot displays the DLA Piper website's interface for comparing data protection laws. At the top, the navigation menu includes links for 'PRIVACY SCOREBOX', 'GDPR OVERVIEW', 'GDPR APP', 'BLOG', and 'DLA Piper Intelligence'. A prominent blue button labeled 'DOWNLOAD the full handbook' is visible on the right. The main heading reads 'Compare data protection laws around the world'. Below this, there is a search form with two dropdown menus: 'Please select: Country' and 'Compare to: Comparison country', followed by a 'GO' button. A world map is shown below the form, with countries color-coded to represent different data protection regimes. A vertical sidebar on the left contains icons for home, globe, search, and other navigation functions.

Data Protection Law of The World

The screenshot shows a web browser window with the URL <https://www.dlapiperdataprotection.com/index.html?t=law&c=CN>. The page features the DLA PIPER logo and the title "DATA PROTECTION LAWS OF THE WORLD". Navigation links include "PRIVACY SCOREBOX", "GDPR OVERVIEW", "GDPR APP", "BLOG", and "DLA Piper Intelligence". Two buttons are visible: "DOWNLOAD current countries" and "DOWNLOAD the full handbook".

The main content area is titled "Law" and includes a sidebar with navigation options: About, World map, Law (selected), Definitions, Authority, Registration, Data Protection Officers, Collection & Processing, and Transfer.

The main content area displays "CHINA" with a flag icon, a "Change country" dropdown menu, and a "Compare to" dropdown menu set to "Please select". Below this is a wide image of a modern city skyline, likely Shanghai.

The text below the image reads: "There is not a single comprehensive data protection law in the People's Republic of China (PRC). Instead, rules relating to personal data protection and data security are part of a complex framework and are found across various laws and regulations. Provisions found in laws such as the General Principles of Civil Law and the Tort Liability Law have generally been used to interpret data protection rights as a *right of reputation* or *right of privacy*. However, such interpretation is not explicit."

The text continues: "On June 1, 2017, the PRC Cybersecurity Law came into effect and became the first national-level law to address cybersecurity and data privacy protection. However, there remains quite a bit of uncertainty as to how the PRC Cybersecurity Law will be applied, and what practical steps need to be taken to achieve compliance and the regulatory environment continues to evolve rapidly. Draft guidelines are currently published almost weekly, however, it is expected that some guidelines and national standards will be finalized in the coming months. Further, some provisions in conflict with the data protection obligations imposed under the PRC Cybersecurity Law..."

A very good resources:

Data Protection Law of The World

<https://www.dlapiperdataprotection.com/>

**[https://www.dlapiperdataprotection.com/
index.html?t=law&c=CN](https://www.dlapiperdataprotection.com/index.html?t=law&c=CN)**

Source :
<http://www.digitaltransformationplaybook.com/>

The New Normal

New Normal ?
ความปกติแบบใหม่

The New Normal in Cybersecurity

“

But no matter how much attention (or budget) is lavished on cybersecurity, executives need to understand that

getting hacked isn't a matter of "IF" but "WHEN".

It changes the approach to preparation and risk management.

Mitigating Cyber Risk Means Understanding Time!

”

Source : <https://www.forbes.com>

The New Normal in Cybersecurity

But no matter how much attention (or budget) is lavished on cybersecurity, executives need to understand that

getting hacked isn't a matter of "if" but "when".

It changes the approach to preparation and **risk management**.

Mitigating Cyber Risk Means **Understanding Time**

Source : <https://www.forbes.com>

Towards: “Responsive Security”

Fortress Mentality

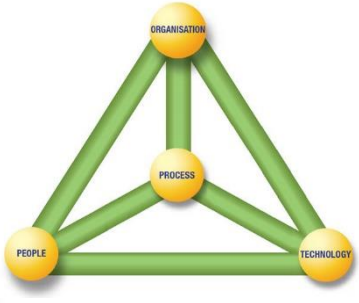
Are we Secure?



Responsive & Readiness Mentality

Are we Ready?

IT, INFORMATION SECURITY, CYBERSECURITY FRAMEWORK, STANDARDS & BEST PRACTICES AS OUR PRINCIPLE KNOWLEDGE



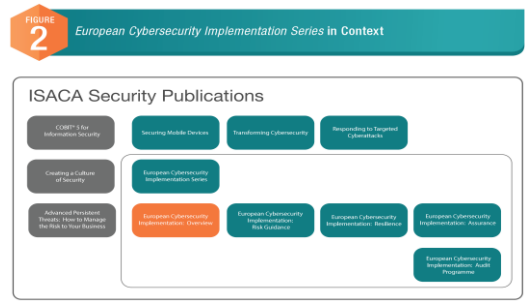
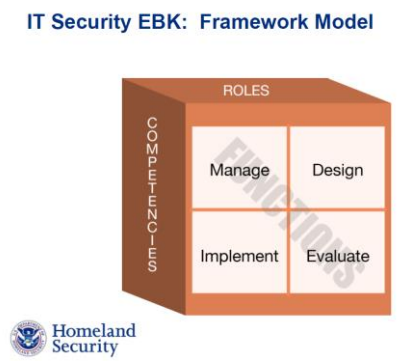
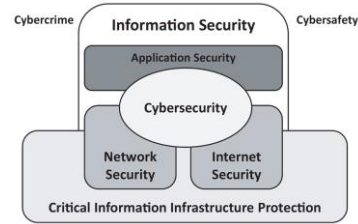
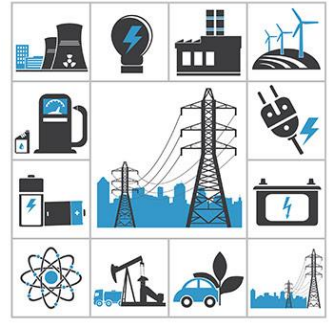
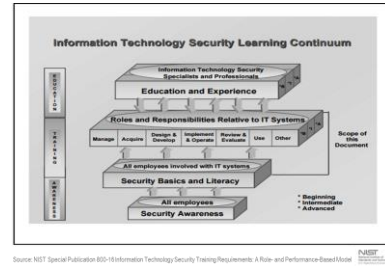
April 16, 2018 Cybersecurity Framework Version 1.1

Table 1: Function and Category Unique Identifiers

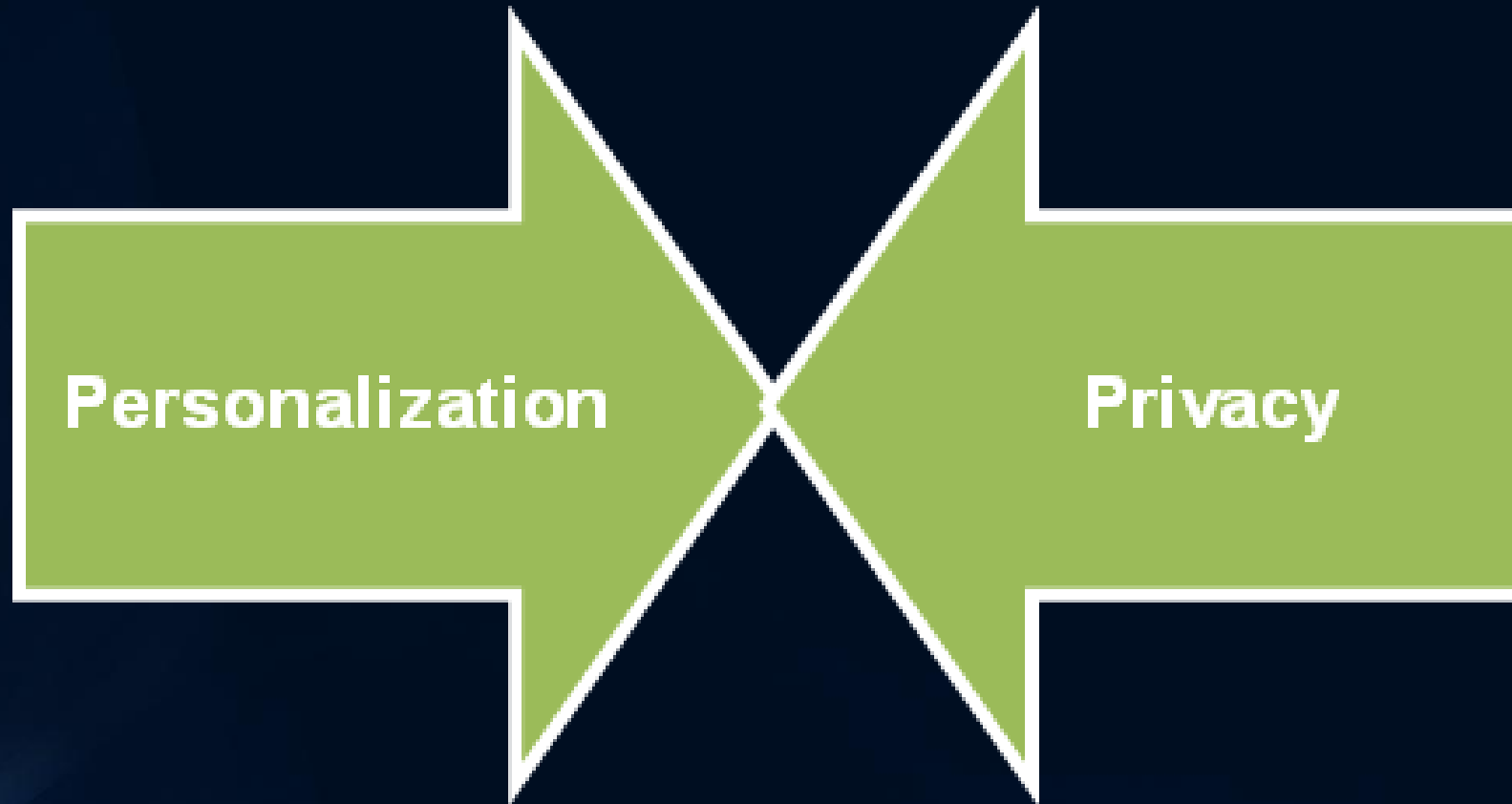
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
		PR	Protect
PR.AT	Awareness and Training		
PR.DS	Data Security		
PR.IP	Information Protection Processes and Procedures		
PR.MA	Maintenance		
PR.PT	Protective Technology		
DE.AE	Anomalies and Events		
DE.CM	Security Continuous Monitoring		
DE.DP	Detection Processes		
RS.RP	Response Planning		
RS	Respond	RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
		RC.RP	Recovery Planning
RC	Recover	RC.IM	Improvements
		RC.CO	Communications



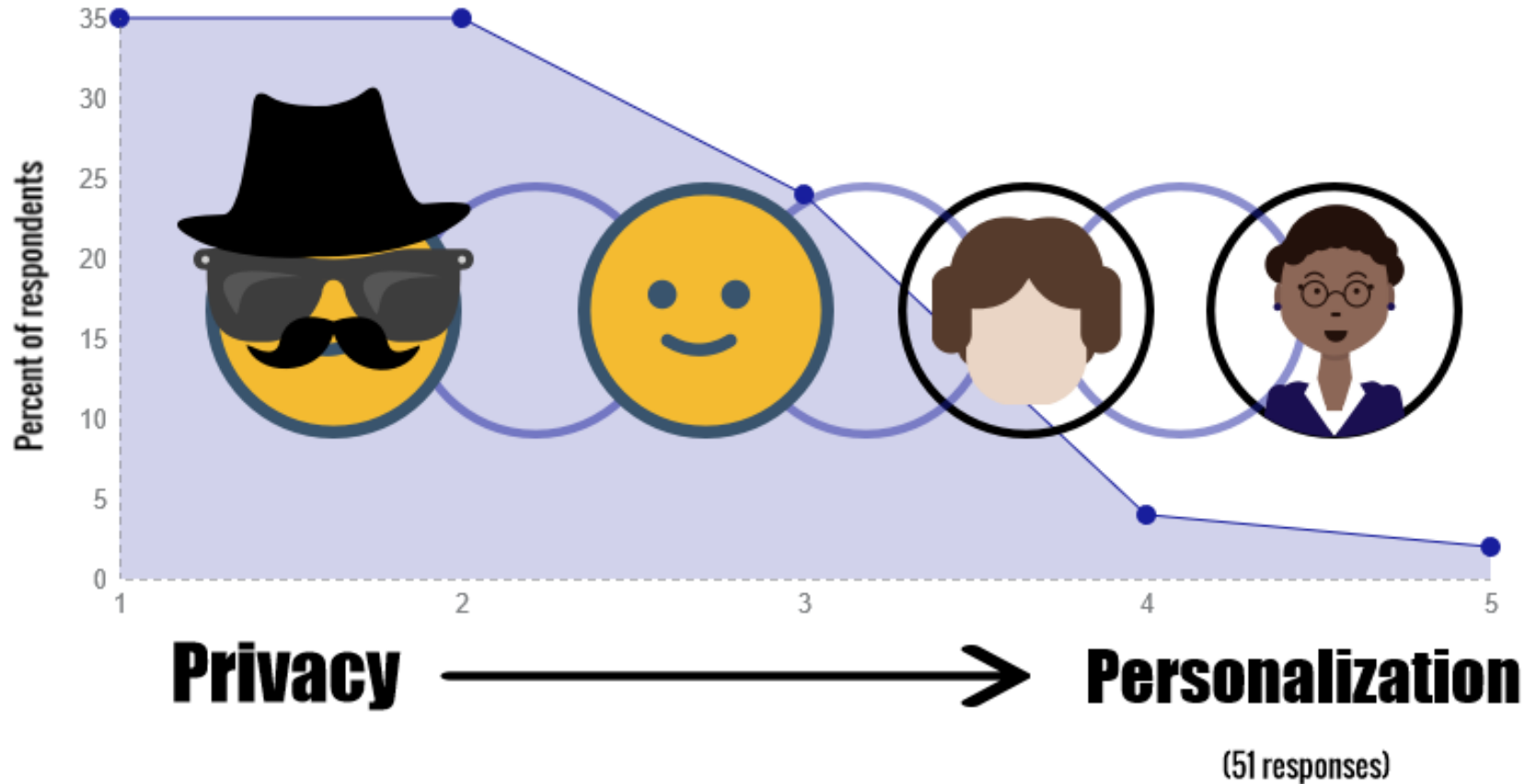
- Education** - knowledge or skill obtained or developed by a learning process
- Training** - the action provided to a user in the acquisition of knowledge, skills, and competencies in the security arena
- Awareness Training** - Managers must ensure that all users are provided awareness training, and that those identified as having significant responsibilities for information technology / cyber security are properly trained.
- Awareness** - the ability of the user to avoid behaviors that would compromise cybersecurity, practice good behaviors that will increase cybersecurity, and act wisely and cautiously, where judgment is needed, to increase cybersecurity.



Personalized Marketing vs. Customer Privacy



In terms of the services libraries provide, and given that two options are not always mutually exclusive, where would you fall on the spectrum of **privacy vs. personalization?**



Credit <https://news.minitex.umn.edu/news/2020-07/one-second-poll-results-privacy-vs-personalization>

Personalized Marketing: The New Era Of Personalization



Credit : <https://www.feedough.com/>

“Gain Consumer Confidence by Respecting Privacy With Your Big Data Marketing”

Credit : <https://www.socialmediatoday.com>

The Marketing & Privacy Myth: Are They Truly Incompatible?

Credit : <https://www.medium.com>

Pre-Internet Marketing vs. Digital Marketing

Pre-Internet Marketing	Digital Marketing
<ul style="list-style-type: none">• Name• Birthday• Phone number• Address <hr/>	<ul style="list-style-type: none">• Name• Birthday• Phone number• Address <hr/> <ul style="list-style-type: none">• Online Identifier Internet Protocol Address• Heatmap, screen recording with mouse movement• Type of device, device ID, location• Cookie (i.e., session cookie, persistent cookie, secure cookie, Google analytics cookie, third-party cookie)

Credit : <https://www.medium.com>

THE NEW CONSUMER EXPECTATIONS



Consumers want personalization...but not too much

67% want personalized content but
64% have been "creeped out" by personalization



Consumers want control over their marketing data

66% want control + ownership over their data
86% want to know when their data is passed to third parties



Consumers expect transparency and respect

96% want brands to be more transparent about the collection and use of their personal data

jebbit

Sources: Jebbit research, CMO, Business Wire, and Adlucent

Credit : <https://www.jebbit.com>

THE NEW MARKETING LANDSCAPE



67%

of consumers want
personalized experiences

92%

of consumers are worried
about their online data
privacy

jebbit

Sources: CMO and TrustArc

Credit : <https://www.jebbit.com>

**40% of
consumers**

OF FINANCIAL
INSTITUTIONS SAY
A PERSONALIZED
SERVICE WOULD
BOOST THEIR BANK
LOYALTY, BASED ON
ACCENTURE'S
RESEARCH.*

**85%
citizens**

EXPECT THAT
GOVERNMENT
DIGITAL SERVICES
SHOULD MATCH THE
QUALITY OF
COMMERCIAL
ONES.**

Credit : <https://blog.ladder.io/marketing-personalization/#z30r6ibuf3hhm3n46c0oj>

Consumer Attitudes to Irrelevant Website Content

% of online respondents

July 2013

74%	get frustrated with websites when content, offers, ads, promotions, etc. appear that have nothing to do with their interests
67%	claim that they would leave the site if asked for donations from a political party that they dislike the most
57%	say they'd leave a site if they were married and shown ads for a dating service
57%	are OK with providing personal information on a website as long as it's for their benefit and being used in responsible ways
77%	would trust businesses more if they explained how they're using personal information to improve their online experience

MC

MARKETINGCHARTS.COM

Source: Janrain/Harris Interactive

BAD DATA POWERS

BAD PERSONALIZATION

34%

What we found is that data being purchased and sold through a credible vendor was only 34% accurate.

58%

58% of consumers admit they have broken ties with a brand over bad personalization.

jebbit
Source: Jebbit

Credit : <https://www.jebbit.com>

MAPPING DATA FLOWS

Understanding how the largest technology companies collect, use, and share user information across the internet. We've transformed the "Big Four" terms of service and data policies – the thousands of lines of code that govern their use of your data – into a database powering an interactive visualization, an initial version of which we invite you to explore and critique. Select a company in the top menu and click on a line to see the original snippet of text from the company's terms of service or data policy.

To explore how these policies have changed over time take a look at [Google's previous terms of services](#) going back to 2001. And, given its enormous popularity during the current COVID-19 crisis, we have also created a [separate visualization just for Zoom](#).

SELECT COMPANY **All companies** Amazon Apple Facebook Google
 COLLECTION PURPOSE **All purposes** COLLECTION METHOD **All Methods** COMPARE COMPANIES **Select company** vs. **Select company**
 TYPES OF DATA **All types**
 CASE STUDIES **Say No Evil, But Keep Your Options Open** **The Illusion of Privacy Settings** **Are They Listening?!** **Absolutely, Definitely Imprecise** **RESET FILTERS**



CASE STUDIES

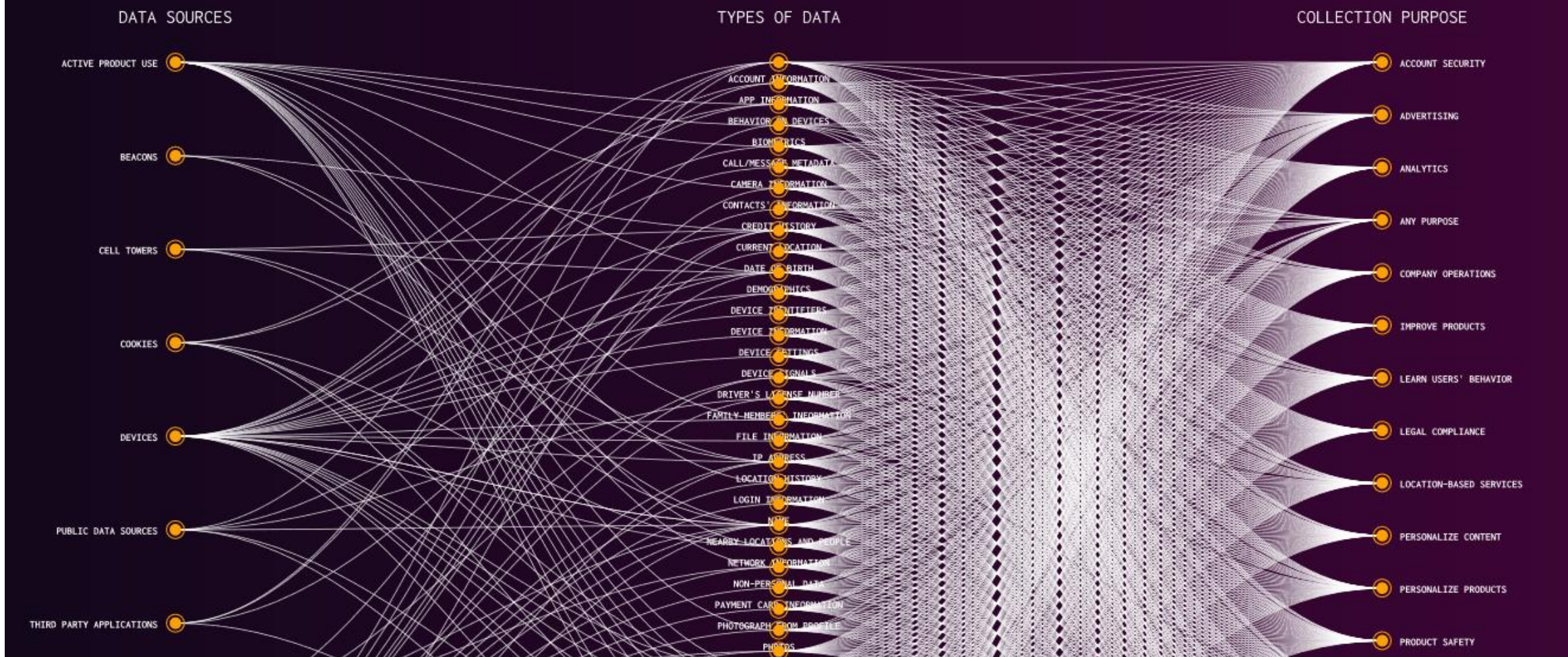
Say No Evil, But Keep Your Options Open

The Illusion of Privacy Settings

Are They Listening?!

Absolutely, Definitely Imprecise

RESET FILTERS

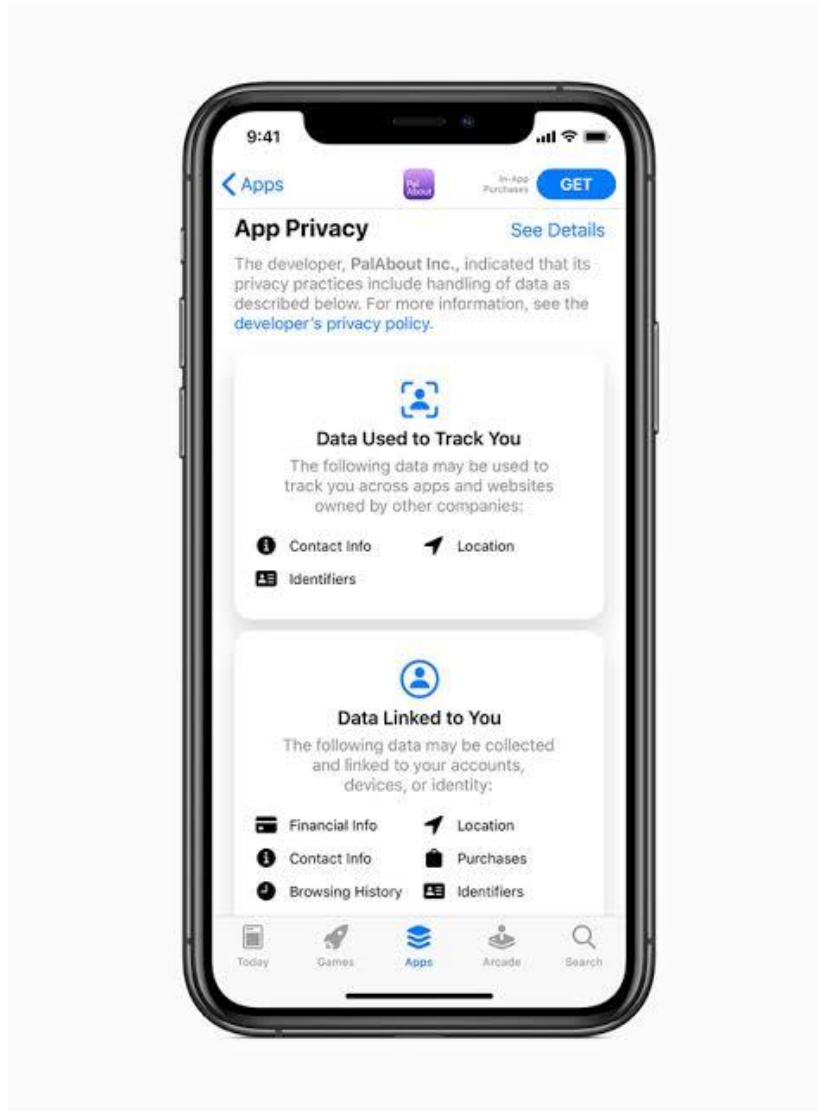


Apple : “Privacy Matters”



Credit : <https://www.apple.com>


iOS 14 : New “Privacy” Features



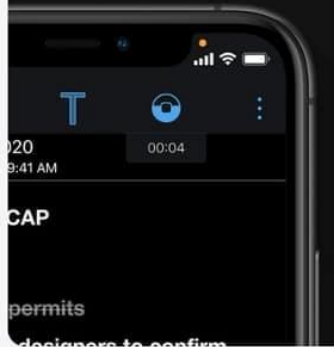
Privacy

Privacy is a fundamental human right and at the core of everything we do. That's why with iOS 14, we're giving you more control over the data you share and more transparency into how it's used.


Privacy information on the App Store
You can now get information on the App Store to help you understand the privacy practices of every app before you download it.¹⁴




Recording indicator
An indicator appears at the top of your screen whenever an app is using your microphone or camera. And in Control Center, you can see if an app has used them recently.



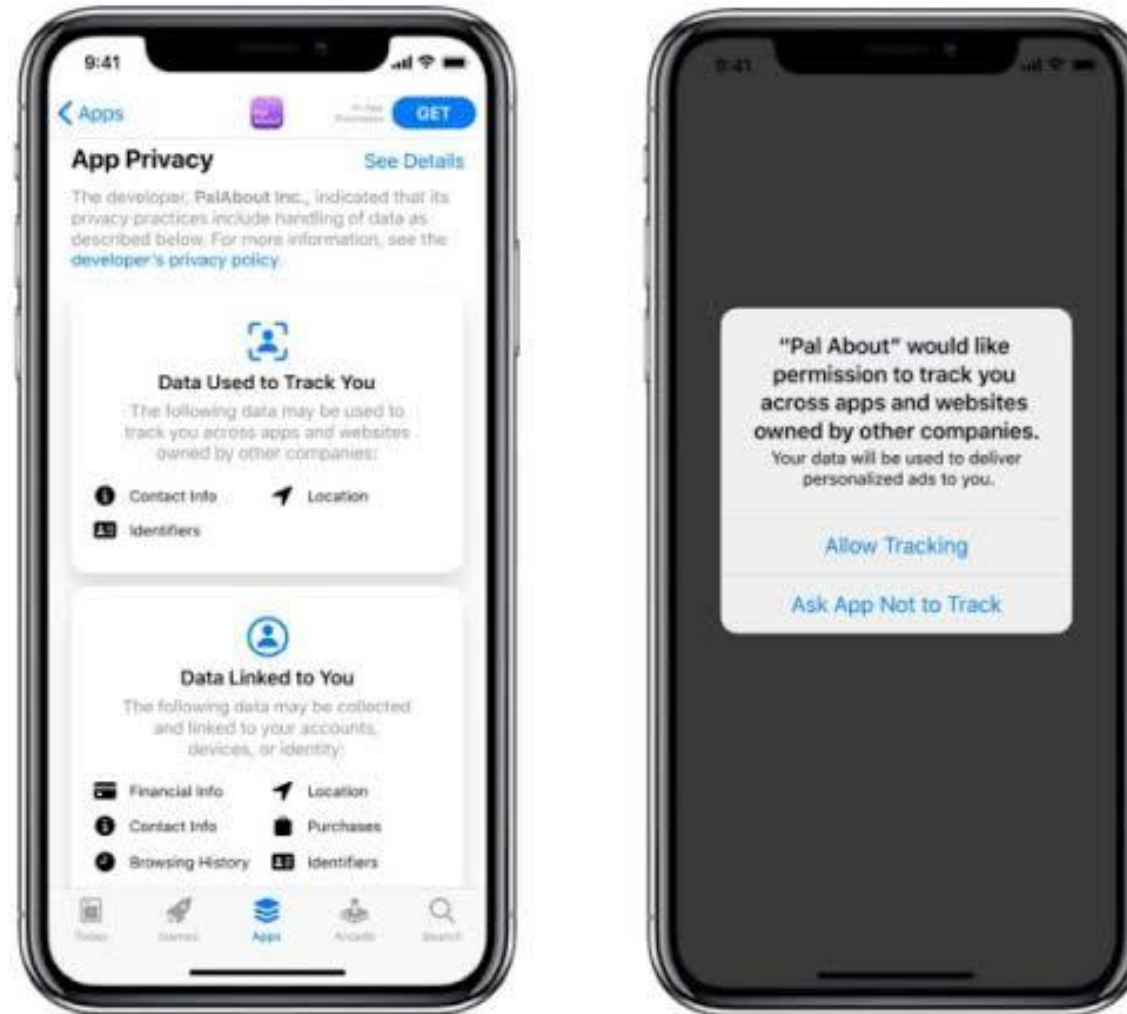
Upgrade to Sign in with Apple
Easily switch to Sign in with Apple when logging in to participating apps. You'll keep the account you already use, but have one less password to keep track of.



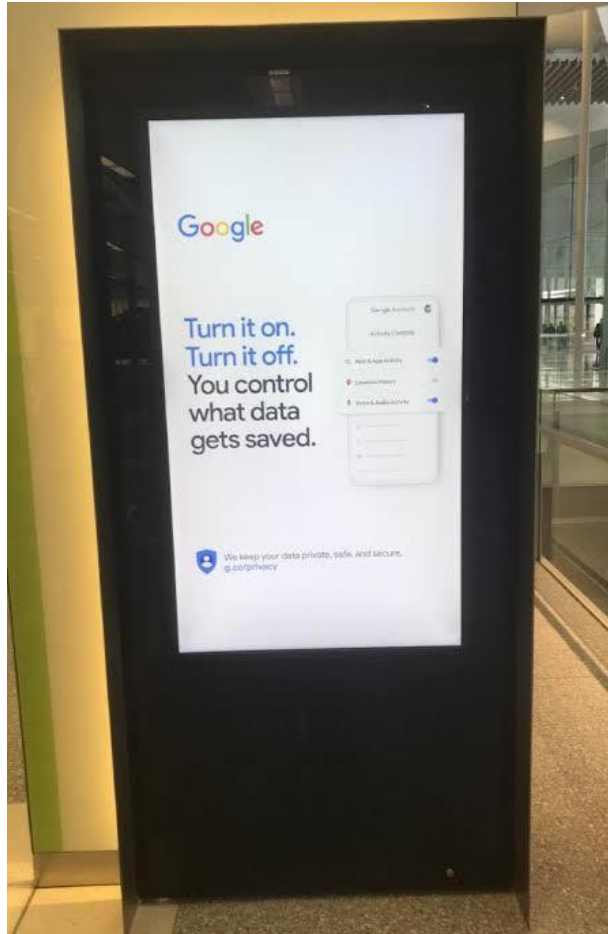
Approximate location
Share only your approximate location rather than your exact location — perfect for apps like local news or weather.



iOS 14 : New “Privacy” Features



How Google handles Privacy



Ad personalisation

Google makes your ads more useful on Google services (e.g. Search, YouTube), and on websites and apps that partner with Google to show ads. [Learn more](#)

Ad personalisation is ON

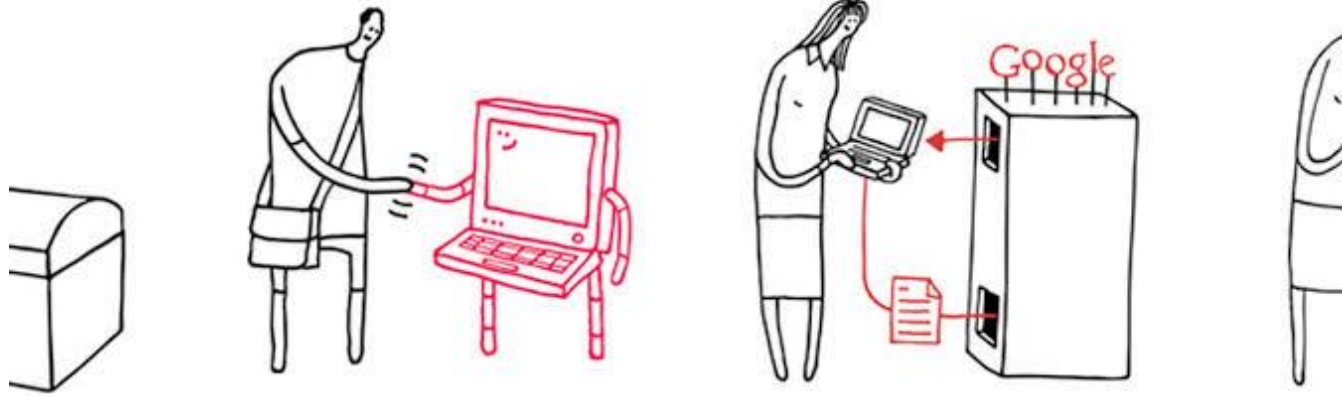
How Google handles Privacy

line

Your data on the web

Your data on Google

Mar



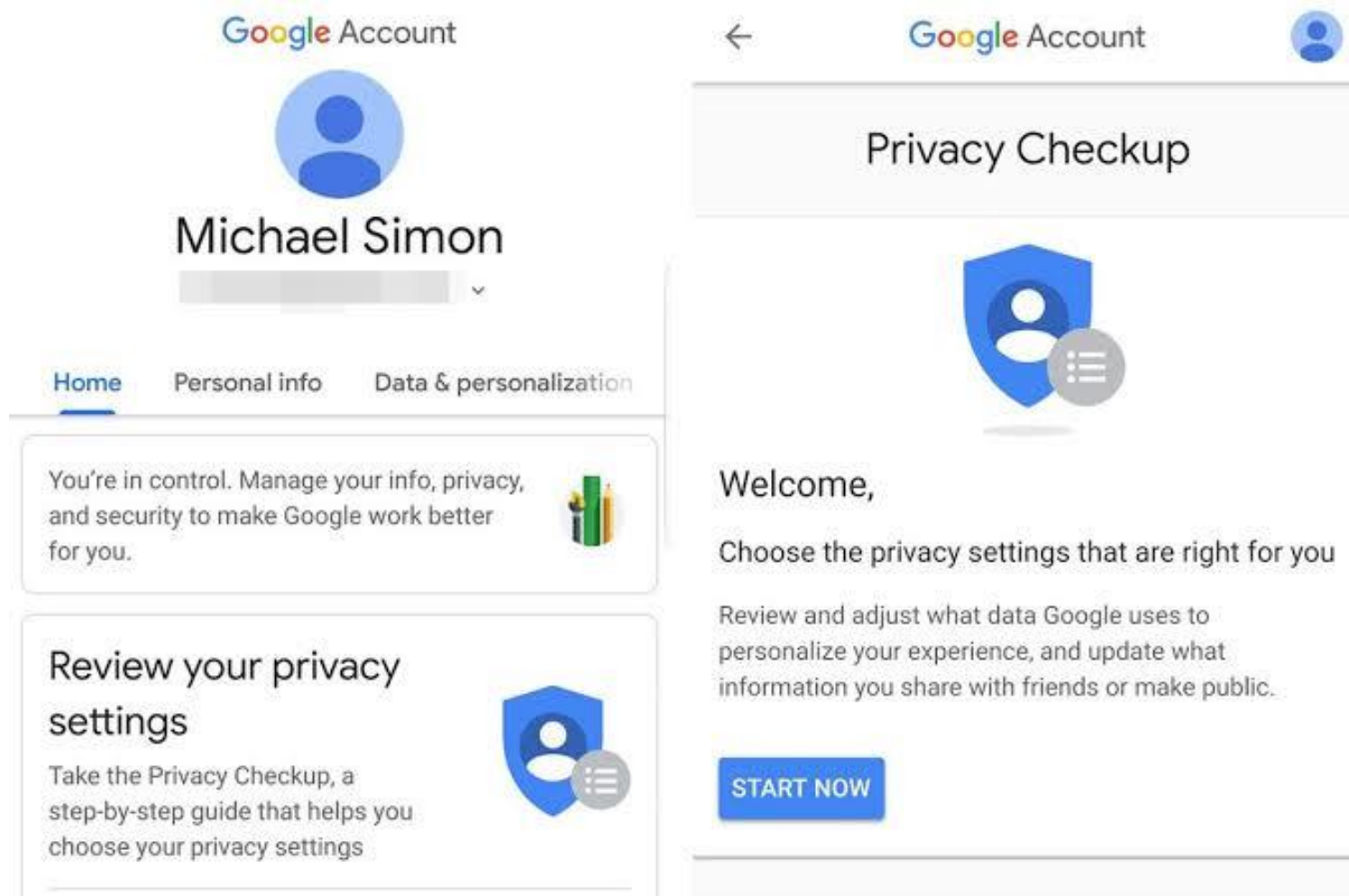
r staying
ie web

... and how it makes websites
more useful

... and how it makes Google
services more useful

... and
we

How Google handles Privacy



The image shows two screenshots of the Google Account interface. The left screenshot is the main account page for Michael Simon, and the right screenshot is the Privacy Checkup page.

Left Screenshot (Main Account Page):

- Header: Google Account
- Profile picture: Blue circle with a person icon
- Name: Michael Simon
- Navigation tabs: Home (selected), Personal info, Data & personalization
- Message: "You're in control. Manage your info, privacy, and security to make Google work better for you." with a pencil icon.
- Section: "Review your privacy settings" with a shield icon and a list icon. Text: "Take the Privacy Checkup, a step-by-step guide that helps you choose your privacy settings".

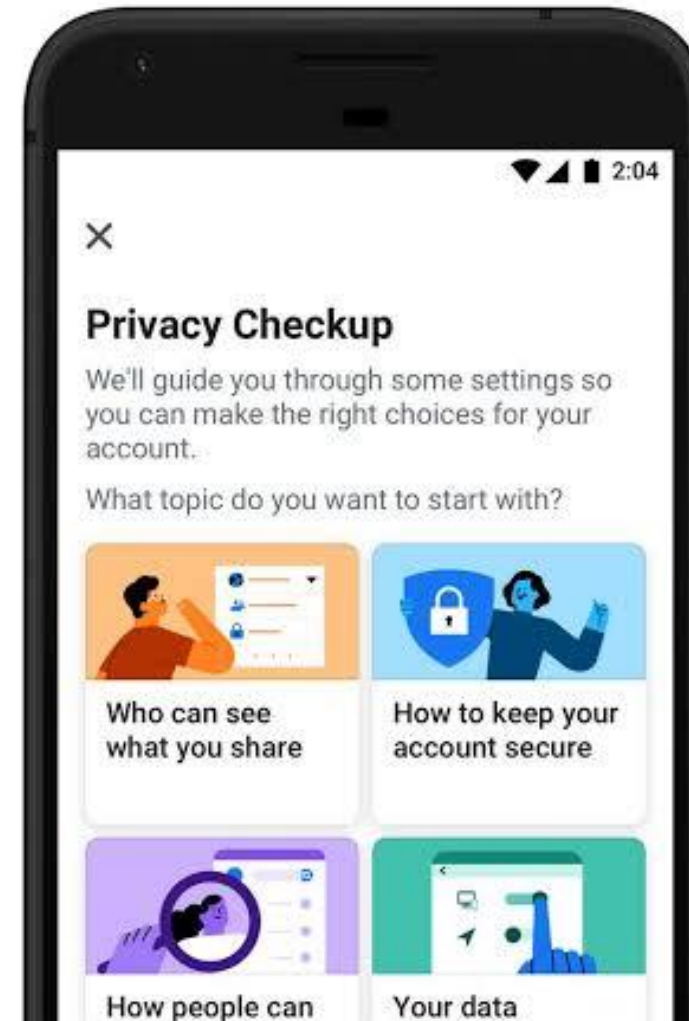
Right Screenshot (Privacy Checkup Page):

- Header: Google Account
- Section: "Privacy Checkup" with a shield icon and a list icon.
- Text: "Welcome, Choose the privacy settings that are right for you"
- Text: "Review and adjust what data Google uses to personalize your experience, and update what information you share with friends or make public."
- Button: "START NOW"

How Facebook handles Privacy



How Facebook handles Privacy



How Facebook's customer handles their privacy



TIPS FOR FACEBOOK PRIVACY

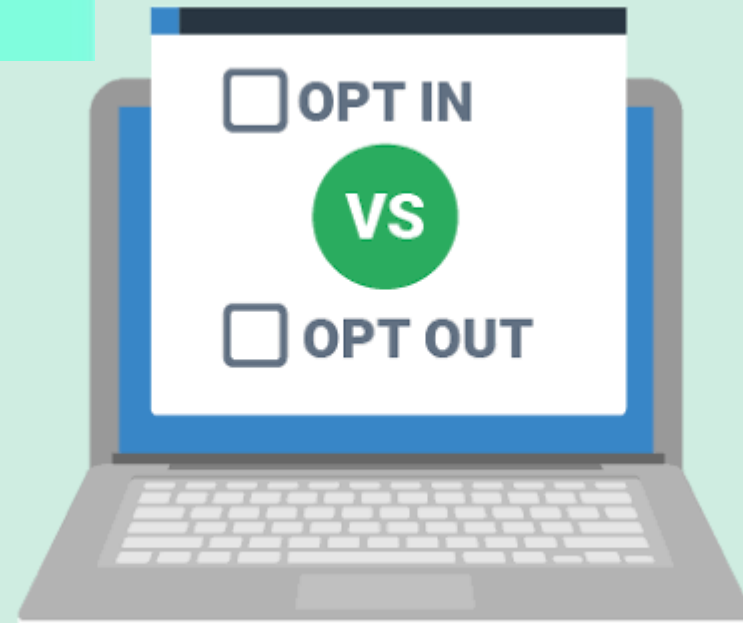
LE VPN
INTERNET BY YOUR OWN RULES

- Don't make random friends
- Don't share
- Don't like
- Don't use the apps
- Don't use Facebook as your log-in
- Use a burner profile
- Properly adjust your settings
- Don't post private pictures



SMS MARKETING

How to get
the “yes”
on opt-in



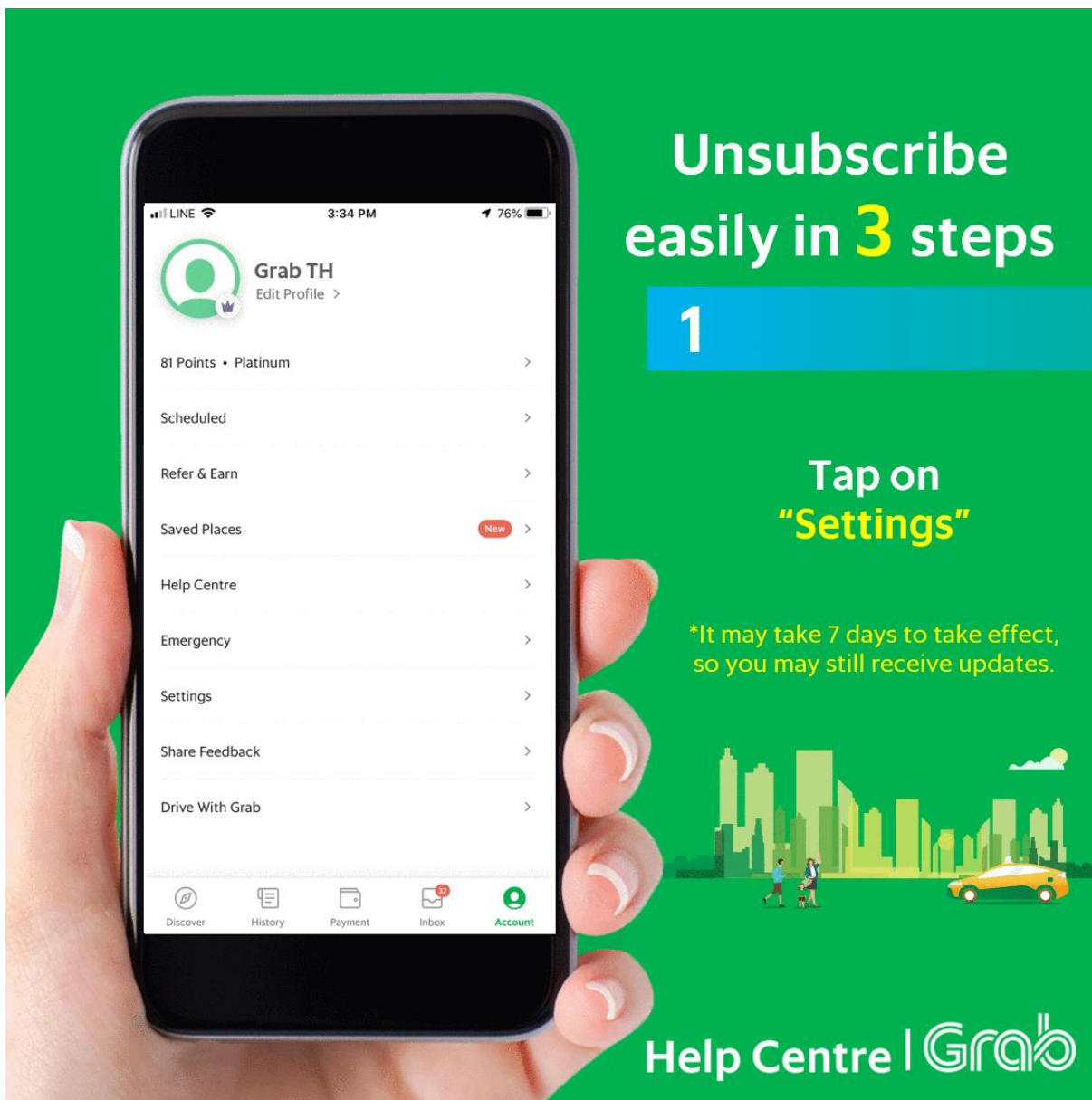
Unsubscribe easily in 3 steps

1

Tap on "Settings"

*It may take 7 days to take effect, so you may still receive updates.

Help Centre | Grab



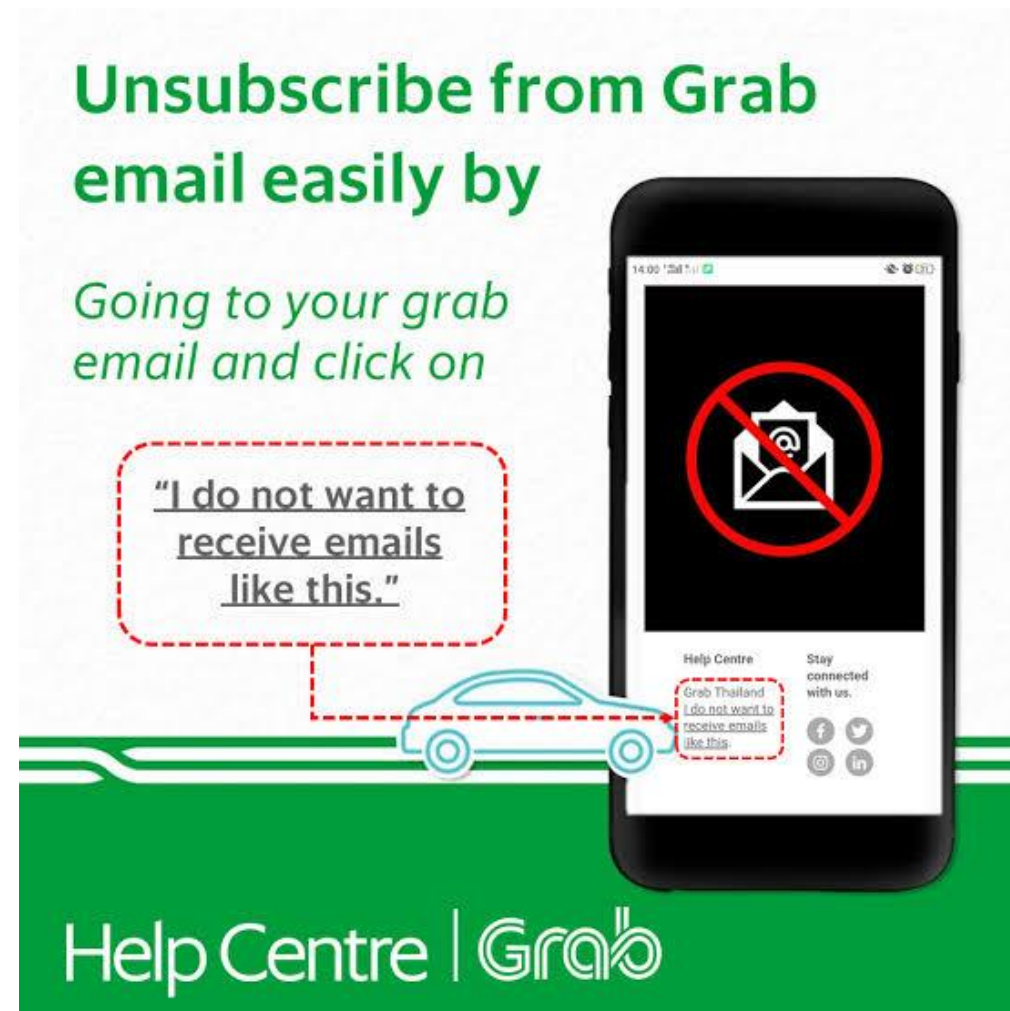
Unsubscribe from Grab email easily by

Going to your grab email and click on

"I do not want to receive emails like this."



Help Centre | Grab



From time to time, we may wish to contact you with marketing information and updates about our own products and services by email, post or telephone. If you do not want to hear from us in this way, you can opt-out by ticking the options below or contacting us at any time.

- I do not wish to hear from you by email in relation to marketing.**
- I do not wish to hear from you by post in relation to marketing.**
- I do not wish to hear from you by telephone in relation to marketing.**

For more details about how we will use your information and your rights in relation to your personal information please see our privacy notice at www.shawbrook.co.uk/privacy-notice. If you have made a joint application, then you must inform the joint applicant of the information contained in the Shawbrook Privacy Notice and have their prior agreement to disclose to us their information. By proceeding, you acknowledge having read our privacy notice.

Get my quote



GDPR Fines Tracker & Statistics



Total Number of GDPR Fines

339

Largest Fine

€50,000,000

Google Inc. on January 21 , 2019 -
France

Total Amount of GDPR Fines

€157,305,806

Smallest Fine

€90

Hospital on November 18 , 2019 -
Hungary

5 MOST RECENT GDPR FINES

*Only includes finalised cases

DATE	ORG	FINE

TOP 5 BIGGEST GDPR FINES

*Only includes final & binding fines

 Google Inc.	€50,000,000
---	-------------

TOP 5 BIGGEST GDPR FINES***Only includes final & binding fines**

	Google Inc.	€50,000,000
	TIM - Telecom Provider	€27,800,000
	Austrian Post	€18,000,000
	Deutsche Wohnen SE	€14,500,000
	1&1 Telecom GmbH	€9,550,000

<i>Knowns</i>	<i>Known Knowns</i> <i>Things we are aware of and understand.</i>	<i>Known Unknowns</i> <i>Things we are aware of but don't understand.</i>
	<i>Unknown Knowns</i> <i>Things we understand but are not aware of.</i>	<i>Unknown Unknowns</i> <i>Things we are neither aware of nor understand.</i>
	<i>Knowns</i>	<i>Unknowns</i>



**Digital
Transformation**

**Top Ten
Cyber Threats
and Trends for
2019**

Cybersecurity Act

Personal Data Protection Act

**Guidance
for CI & CII
“Banking
& Financial
Sector”**







ภาพรวมโครงสร้างลำดับของกฎหมายที่เกี่ยวข้อง

โครงสร้างลำดับกฎหมาย



<https://standard.eta.or.th/?p=7181>

หมายเหตุ: หน่วยงานกำกับดูแล

-  ▶ ครอ. คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
-  ▶ ธปท. ธนาคารแห่งประเทศไทย
-  ▶ ก.ล.ต. คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
-  ▶ คปภ. คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

 ค้นหาราชกิจจานุเบกษา

ประกาศในราชกิจจานุเบกษา

<http://www.rachakitcha.soc.go.th/RKJ/announce/newrkj.jsp>

<http://www.rachakitcha.soc.go.th/RKJ/announce/search.jsp>

<http://www.mrachakitcha.soc.go.th/index.php>

กฎหมาย พระราชบัญญัติ (Th / En)

Th <http://www.mdes.go.th/view/>

En <http://www.mdes.go.th/view/>

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Ministry of Digital Economy and Society

ระเบียบข้อบังคับ > กฎหมายที่เกี่ยวข้อง



<https://www.dga.or.th/th/download/982/>

สำนักงานพัฒนาธุรกิจดิจิทัล
(องค์การมหาชน)

  สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กฎหมาย

<https://www.eta.or.th/laws-sharing.html>

<https://standard.eta.or.th/?p=7181> ETDA Recommendation

กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ 

<http://www.etcommission.go.th/law.html>

มาตรฐานเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ 

<http://www.etcommission.go.th/standard.html>

 ประกาศและหนังสือเวียนธนาคารแห่งประเทศไทย

https://www.bot.or.th/App/FIPCS/Thai/PFIPCS_list.aspx

https://www.bot.or.th/Thai/FinancialInstitutions/InterestDocs/fiba_notification.pdf

https://www.bot.or.th/Thai/PaymentSystems/PSA_Oversight/Pages/RelatedLaws.aspx

 ประกาศ หนังสือเวียน วิธีปฏิบัติ ก.ล.ต.

https://capital.sec.or.th/webapp/nrs/nrs_table_of_contents.php

 ประกาศ ระเบียบ คปภ.

<http://oiceservice.oic.or.th/lawsearch.php>



กฎหมายสำคัญด้านเทคโนโลยีสารสนเทศ/ความมั่นคงปลอดภัยสารสนเทศ



กฎหมายสำคัญด้านเทคโนโลยีสารสนเทศ/ความมั่นคงปลอดภัยสารสนเทศ

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544		
พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551	พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 <small>ประกาศในราชกิจจานุเบกษา 14 เมษายน 2562</small>	พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 <small>ประกาศในราชกิจจานุเบกษา 22 พฤษภาคม 2562</small>
พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 <small>หน่วยงานของรัฐ (ส่วนราชการ รัฐวิสาหกิจ ฯลฯ)</small>	พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 <small>ผู้ประกอบการธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์</small>	พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 <ul style="list-style-type: none">ระดับองค์กรระดับกลางระดับพื้นฐาน <small>หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure: CI)</small>
พระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554		
พระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562		<small>ประกาศในราชกิจจานุเบกษา 14 เมษายน 2562</small>
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550		
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560		
พระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560		
พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560		
พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562		
พระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. 2561		
พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม (ฉบับที่ 2) พ.ศ. 2560		
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562		<small>ประกาศในราชกิจจานุเบกษา 27 พฤษภาคม 2562</small>
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562		<small>ประกาศในราชกิจจานุเบกษา 27 พฤษภาคม 2562</small>



ชุดกฎหมายดิจิทัล





Data Protection Law

Thailand Data Protection Law:

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

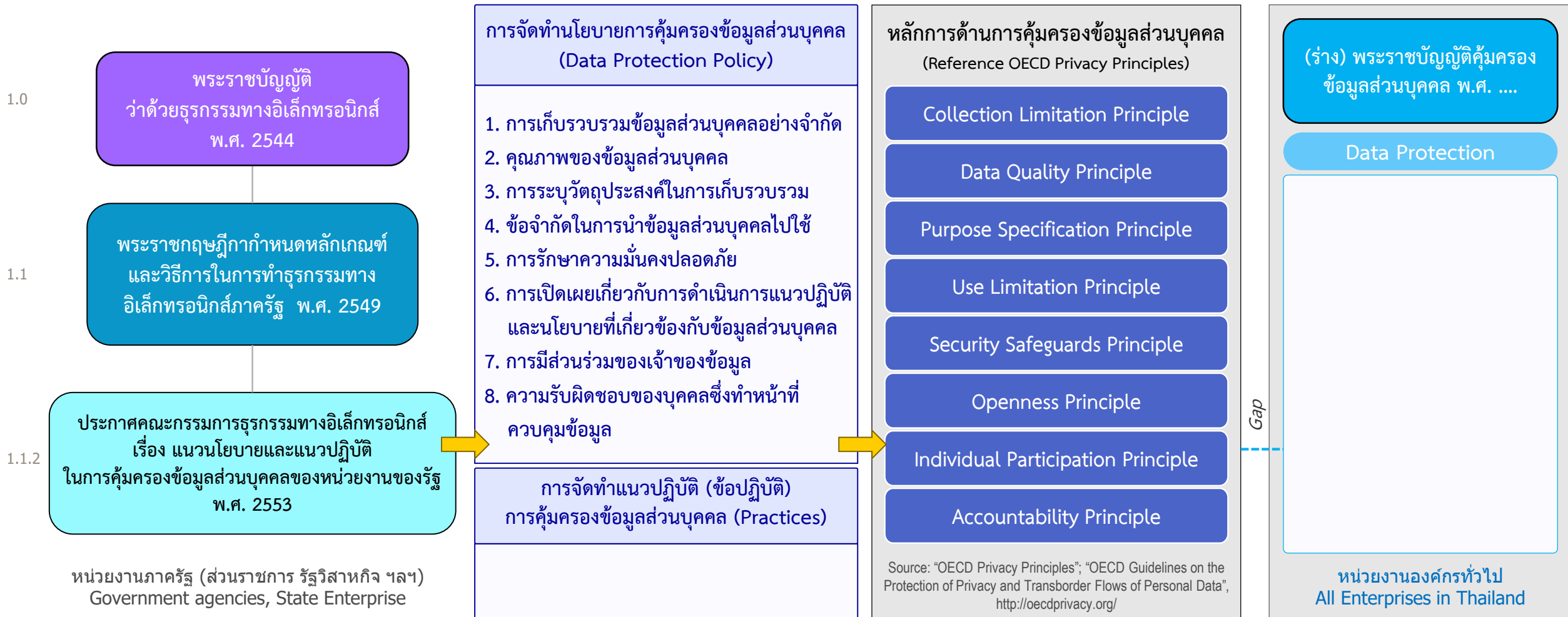
OECD privacy principles





กฎหมายสำคัญที่เกี่ยวข้องด้านการคุ้มครองข้อมูลส่วนบุคคล

Data Protection Laws



หลักการคุ้มครองข้อมูลส่วนบุคคล

Principles for Personal Information/Data Protection (Privacy)

 OECD The OECD Privacy Principles



ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
ข้อ 1 ให้จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร (อ้างอิงหลักการคุ้มครองข้อมูลส่วนบุคคล 8 ประการ)

1. Collection Limitation Principle

หลักการรวบรวมข้อมูลอย่างจำกัด :

- การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

2. Data Quality Principle

หลักการคุณภาพของข้อมูล :

- คุณภาพของข้อมูลส่วนบุคคล

3. Purpose Specification Principle

หลักการระบุวัตถุประสงค์ :

- การระบุวัตถุประสงค์ในการเก็บรวบรวม

4. Use Limitation Principle

หลักการใช้ข้อมูลอย่างจำกัด :

- ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

5. Security Safeguards Principle

หลักการรักษาความปลอดภัยของข้อมูล :

- การรักษาความมั่นคงปลอดภัย

6. Openness Principle

หลักการเปิดเผย :

- การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

7. Individual Participation Principle

หลักการมีส่วนร่วมของเจ้าของข้อมูล :

- การมีส่วนร่วมของเจ้าของข้อมูล







8. Accountability Principle

หลักการความรับผิดชอบ :

- ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

Lawful Basis for Processing Under GDPR

LAWFUL BASIS FOR PROCESSING UNDER GDPR

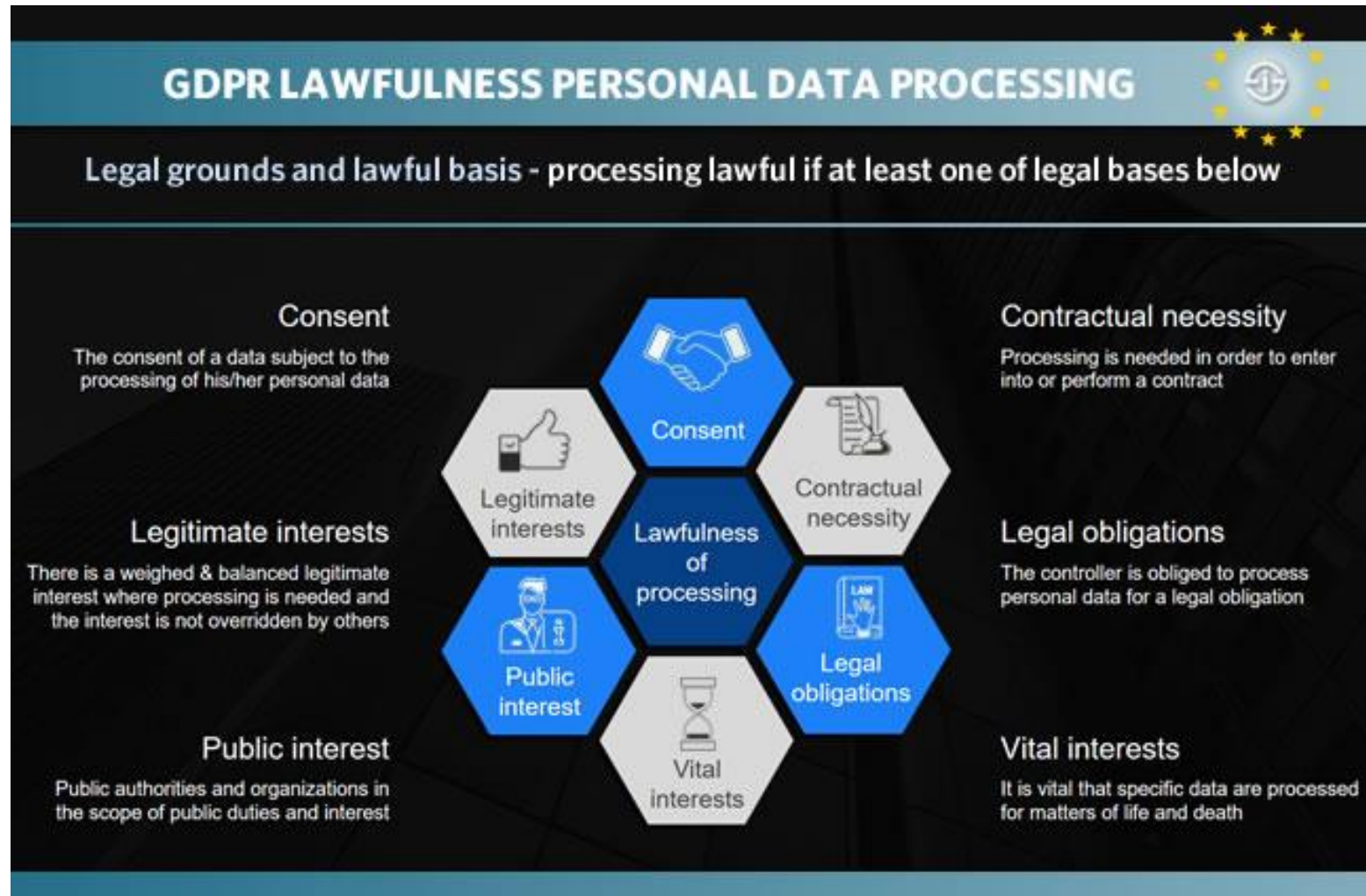
 <p>CONSENT</p> <p>The data subject has given consent to the processing of his or her personal data for one or more specific purposes</p>	 <p>VITAL INTERESTS</p> <p>Processing is necessary in order to protect the vital interests of the data subject or of another natural person</p>
 <p>CONTRACT</p> <p>Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract</p>	 <p>PUBLIC INTEREST</p> <p>Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller</p>
 <p>LEGAL OBLIGATION</p> <p>Processing is necessary for compliance with a legal obligation to which the controller is subject</p>	 <p>LEGITIMATE INTEREST</p> <p>Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child</p>

Helping small businesses work towards Data Protection Compliance and deliver on their Web Application goals

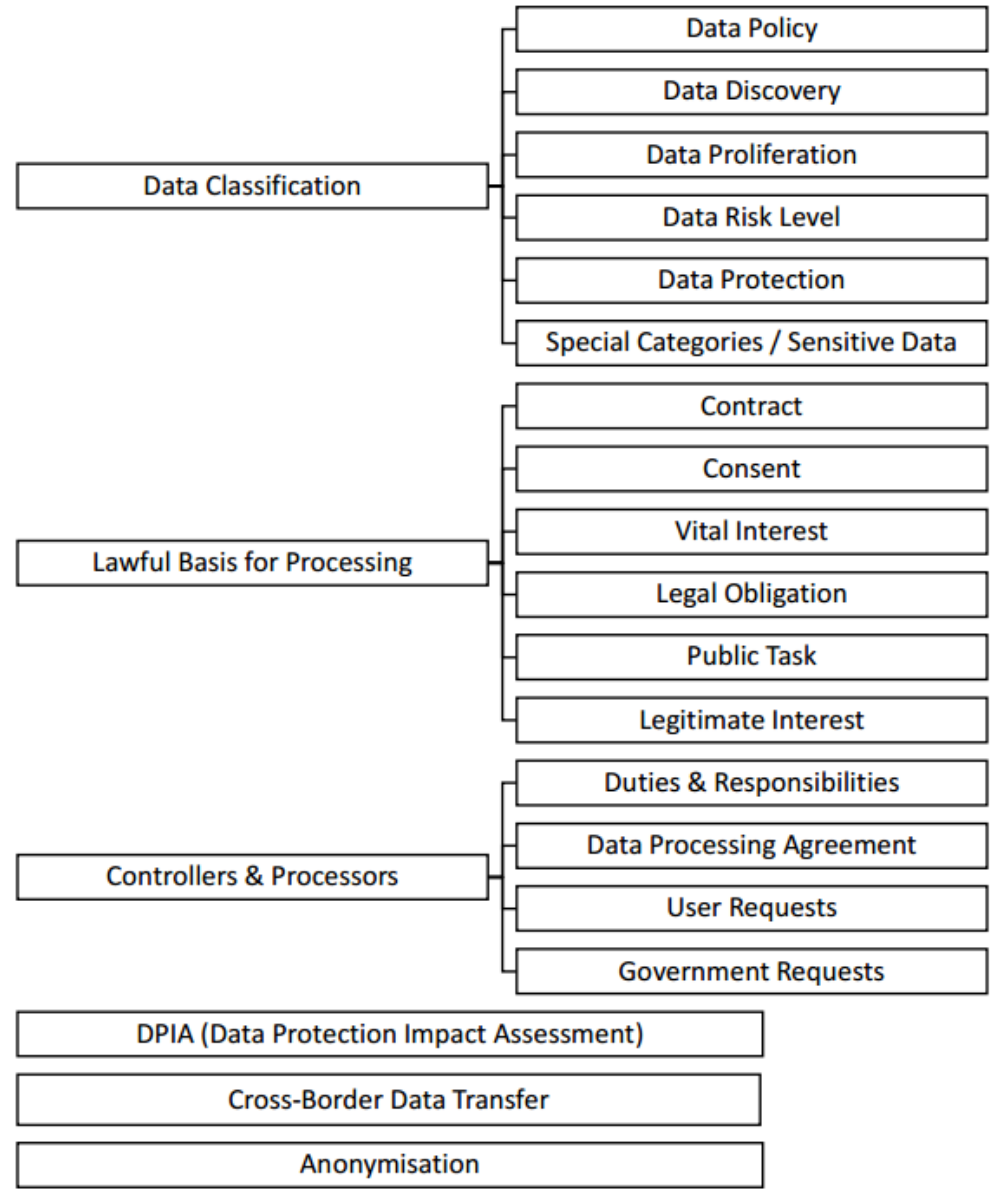
www.ServeIT.com

Source : <https://www.serveIT.com/>

Lawful Basis for Processing Under GDPR



Source : <https://www.i-scoop.eu/>



Source : Thailand Data Protection Guidelines 2.0

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

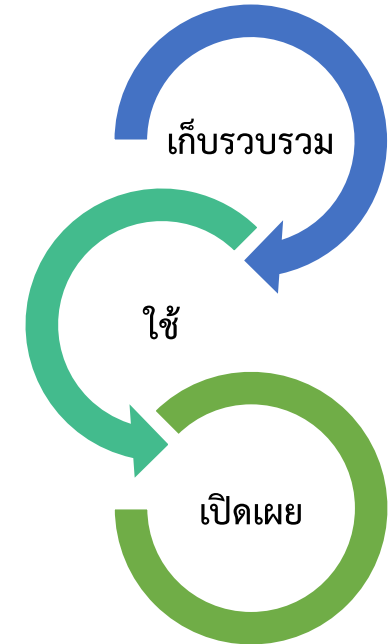
▶ เหตุผลและความจำเป็น

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการโดยทั่วไป

สอดคล้องตามหลักการสากล และ GDPR

การคุ้มครองข้อมูลส่วนบุคคล



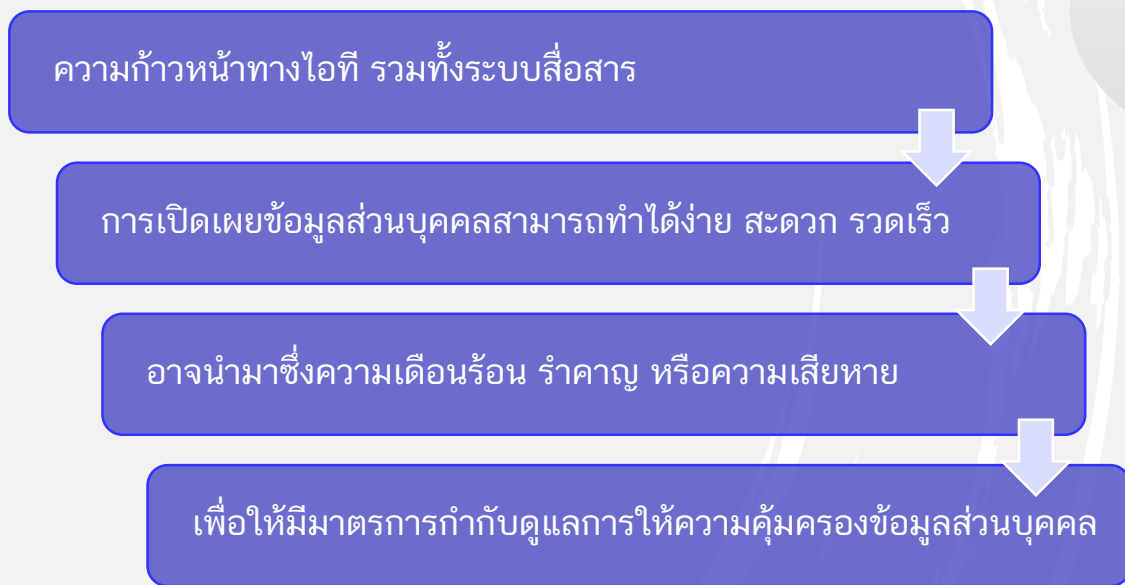
สิทธิของเจ้าของข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล

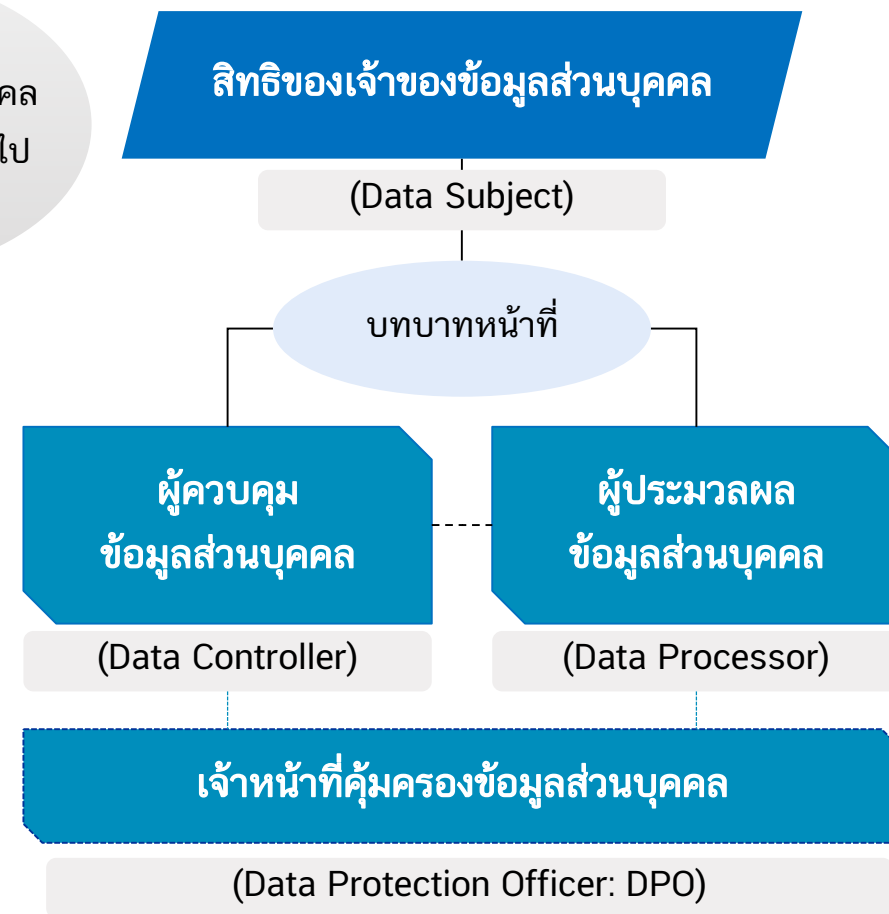
ผู้ควบคุมข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

▶ เหตุผลและความจำเป็น



คุ้มครองข้อมูลส่วนบุคคล
ที่เป็นหลักการโดยทั่วไป



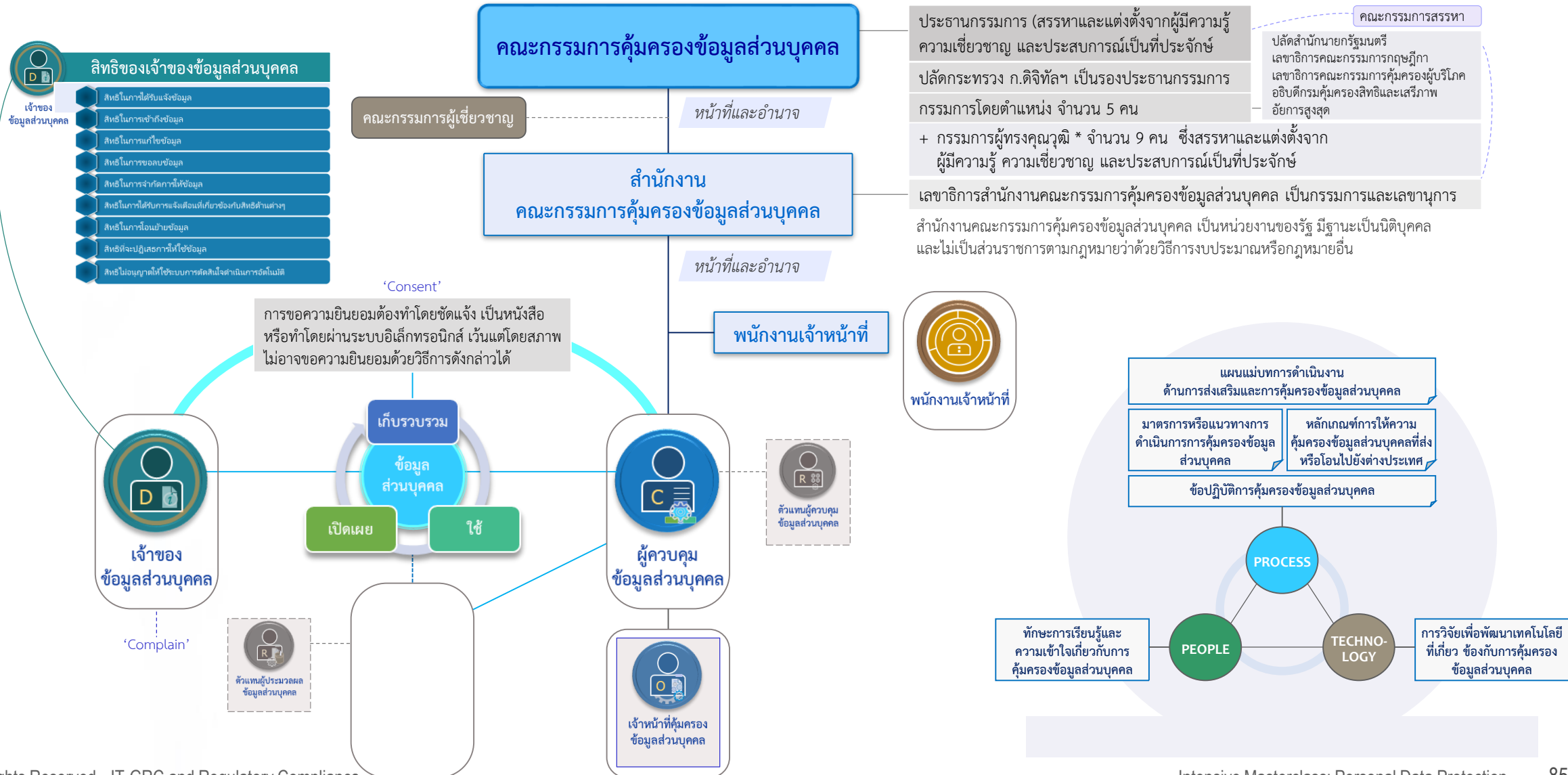
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

มาตรา ๑-๗	• การบังคับใช้ คำนิยาม	มาตรา ๑ - มาตรา ๗	
หมวด ๑	• คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	มาตรา ๘ - มาตรา ๑๘	
หมวด ๒	• การคุ้มครองข้อมูลส่วนบุคคล	มาตรา ๑๙ - มาตรา ๒๙	
หมวด ๓	• สิทธิของเจ้าของข้อมูลส่วนบุคคล	มาตรา ๓๐ - มาตรา ๔๒	
หมวด ๔	• สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	มาตรา ๔๓ - มาตรา ๗๐	
หมวด ๕	• การร้องเรียน	มาตรา ๗๑ - มาตรา ๗๖	
หมวด ๖	• ความรับผิดทางแพ่ง	มาตรา ๗๗ - มาตรา ๗๘	
หมวด ๗	• บทกำหนดโทษ	มาตรา ๗๙ - มาตรา ๙๐	
-	• บทเฉพาะกาล	มาตรา ๙๑ - มาตรา ๙๖	

ส่วนที่ ๑ บททั่วไป	มาตรา ๑๙ - มาตรา ๒๑
ส่วนที่ ๒ การเก็บรวบรวมข้อมูลส่วนบุคคล	มาตรา ๒๒ - มาตรา ๒๖
ส่วนที่ ๓ การใช้หรือเปิดเผยข้อมูลส่วนบุคคล	มาตรา ๒๗ - มาตรา ๒๙
สิทธิของเจ้าของข้อมูลส่วนบุคคล	มาตรา ๓๐ - มาตรา ๓๖
หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล	มาตรา ๓๗ - มาตรา ๓๙
หน้าที่ของผู้ประมวลข้อมูลส่วนบุคคล	มาตรา ๔๐
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	มาตรา ๔๑ - มาตรา ๔๒

ส่วนที่ ๑ โทษอาญา	มาตรา ๗๙ - มาตรา ๘๑
ส่วนที่ ๒ โทษทางปกครอง	มาตรา ๘๒ - มาตรา ๙๐

ภาพรวมการคุ้มครองข้อมูลส่วนบุคคลในระดับชาติ



พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล vs. GDPR

สิทธิของเจ้าของข้อมูลส่วนบุคคล



The EU General Data Protection Regulation (GDPR)

- Right to be informed Article 13 Article 14
- Right of access by the data subject Article 15
- Right to be rectification Article 16
- Right to erasure ('Right to be forgotten') Article 17
- Right to restrict processing Article 18
- Notification obligation regarding rectification or erasure of personal data or restriction of processing Article 19
- Right to data portability Article 20
- Right to object Article 21
- Right of automated decision making and profiling Article 22



ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.
(ฉบับฯสภานิติบัญญัติแห่งชาติ เห็นสมควรประกาศใช้เป็นกฎหมายแล้ว 28 กุมภาพันธ์ 2562)

- สิทธิในการได้รับแจ้งข้อมูล
- สิทธิในการเข้าถึงข้อมูล
- สิทธิในการแก้ไขข้อมูล
- สิทธิในการขอลบข้อมูล
- สิทธิในการจำกัดการให้ข้อมูล
- สิทธิในการได้รับการแจ้งเตือนที่เกี่ยวข้องกับสิทธิด้านต่าง ๆ
- สิทธิในการโอนย้ายข้อมูล
- สิทธิที่จะปฏิเสธการให้ใช้ข้อมูล
- สิทธิไม่อนุญาตให้ใช้ระบบการตัดสินใจดำเนินการอัตโนมัติ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



Intensive Masterclass: PART I

1

สาระสำคัญ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

ภาพรวมสาระสำคัญ ผลการบังคับใช้ของกฎหมาย

ความสำคัญและภาพรวมบทบาทหน้าที่ของหน่วยงานองค์กรที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2

หลักการคุ้มครองข้อมูลส่วนบุคคล ภัยคุกคามและความเสี่ยง

ภาพรวมภัยคุกคามและความเสี่ยง Privacy Risk หลักการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูล การพิจารณาข้อมูลองค์กรและการระบุข้อมูลส่วนบุคคล ภาพรวมแนวทางดำเนินการ

3

บทบาทหน้าที่และแนวทางดำเนินการของหน่วยงาน/องค์กร

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) และหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

4

แนวทางการประเมินองค์กรและการเตรียมความพร้อม

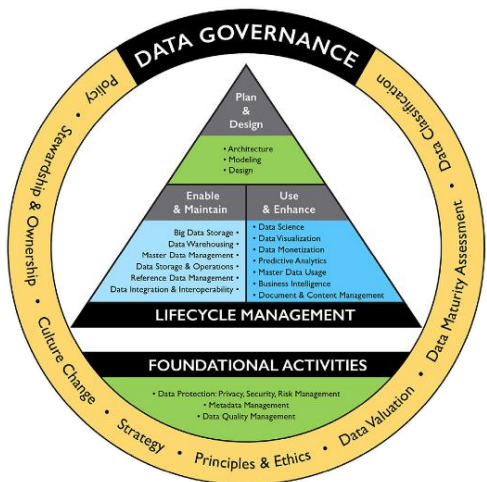
ตัวอย่างการประเมิน Gap Assessment ตามข้อกำหนดกฎหมาย

ภาพรวมมาตรฐานการบริหารจัดการข้อมูลส่วนบุคคล และแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Course Agenda

Intensive Masterclass: PART II



5

แนวทางดำเนินการสอดคล้องตามกฎหมาย GDPR

ภาพรวมความสอดคล้องของกฎหมายกับข้อกำหนด GDPR แนวทางดำเนินการตามกฎหมายกับข้อกำหนด GDPR บทบาทหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และการจัดจ้าง Outsourcing DPO

6

กรอบมาตรฐานฯ การประเมินผลกระทบและความเสี่ยง

กรอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (Privacy Framework) แนวทางการประเมินผลกระทบและความเสี่ยง แนวทางการจัดทำมาตรการและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

7

แนวทางดำเนินการกำกับดูแลและบริหารจัดการข้อมูล

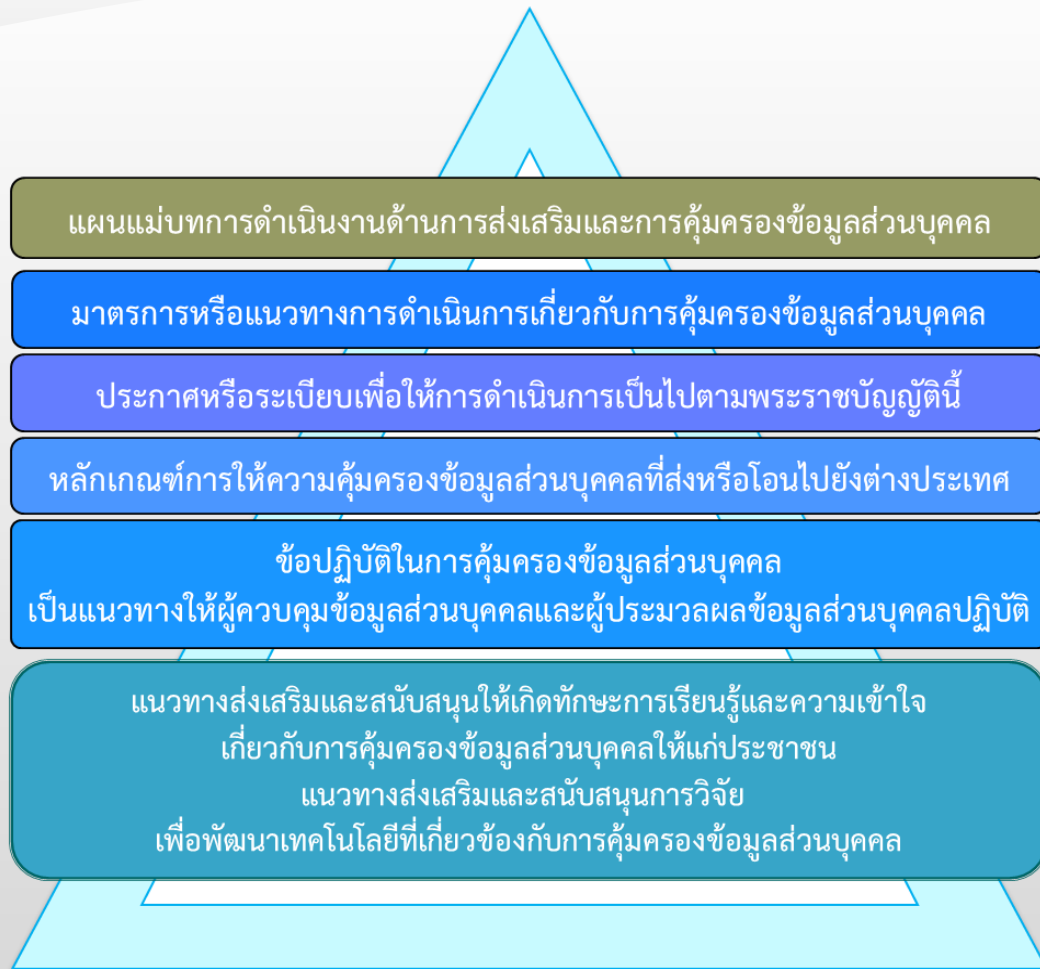
ภาพรวมการจัดการข้อมูลด้านกระบวนการและด้านเทคนิค แนวทางการกำกับดูแลข้อมูล (Data Governance) แนวทางการบริหารจัดการข้อมูล (Data Management) แนวทางการจัดชั้นข้อมูล (Data Classification)

8

แนวทางการจัดการข้อมูล

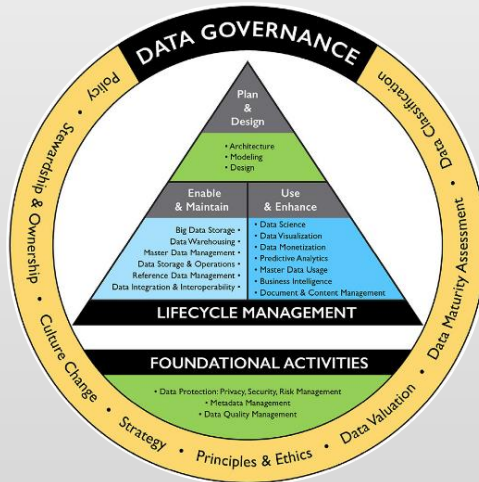
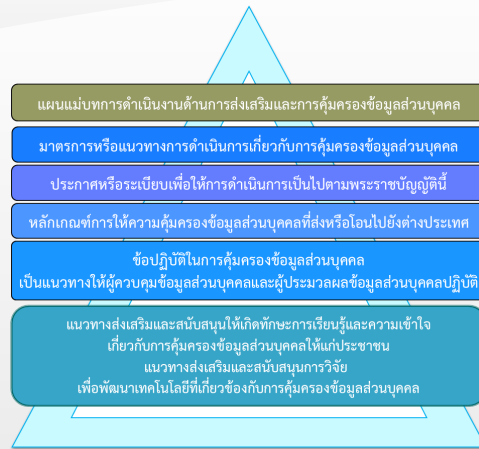
แนวทางการจัดการข้อมูลด้านเทคนิค (Data Quality Management, Metadata, ฯลฯ) และกระบวนการทางเทคนิค

สรุปภาพรวมแนวทางดำเนินการคุ้มครองข้อมูลส่วนบุคคล



- ▶ แนวทางการกำกับดูแลในการคุ้มครองข้อมูลส่วนบุคคล
- ▶ โครงสร้างการกำกับดูแล นโยบายการคุ้มครองข้อมูลส่วนบุคคล และกรอบการดำเนินงาน Data Protection (Privacy Framework)
- ▶ กำหนด “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” (Data Protection Officer: DPO) / “ตัวแทน”
- ▶ กำหนด “ผู้ประมวลผลข้อมูลส่วนบุคคล / “ตัวแทน”
- ▶ กำหนด Business Owner, Data Owner, Data Protection Officer
- ▶ พิจารณาข้อมูลต่าง ๆ ขององค์กร เพื่อกำหนด “ข้อมูลส่วนบุคคล” ที่ต้องดำเนินการตามกฎหมายหรือกฎเกณฑ์ที่ประกาศบังคับใช้

สรุปภาพรวมแนวทางดำเนินการคุ้มครองข้อมูลส่วนบุคคล



- ▶ กรอบการกำกับดูแลและบริหารจัดการข้อมูลระดับองค์กร (Data Governance, Data Management, Data Protection)
- ▶ กรอบการบริหารความเสี่ยง การประเมินความเสี่ยง การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy/Data Protection Impact Assessment, Risk Assessment)
- ▶ กำหนด Business Owner, Data Owner, Data Protection Officer
- ▶ วิธีปฏิบัติ ขั้นตอนปฏิบัติ คู่มือการปฏิบัติงานในการคุ้มครองข้อมูลส่วนบุคคล
- ▶ การสร้างความตระหนัก การเสริมสร้างความรู้ให้กับผู้ปฏิบัติงาน
- ▶ กรอบการประสานกับหน่วยงานกำกับดูแล หน่วยงานภาครัฐ และหน่วยงานความร่วมมืออื่นๆ

สรุปภาพรวมแนวทางดำเนินการคุ้มครองข้อมูลส่วนบุคคล



เจ้าของข้อมูลส่วนบุคคล
(Data Subject / PII principal)
(Natural person)

“ข้อมูลส่วนบุคคล” : ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

สิทธิของเจ้าของข้อมูลส่วนบุคคล

- ➡ สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล
- ➡ สิทธิขอรับข้อมูลส่วนบุคคล ส่งหรือโอนข้อมูลส่วนบุคคล
- ➡ สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้
- ➡ สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
- ➡ สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้



ผู้ควบคุมข้อมูลส่วนบุคคล
(PII/Data Controller)

“ผู้ควบคุมข้อมูลส่วนบุคคล” : บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

หน้าที่

- ➡ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
- ➡ ดำเนินการเพื่อป้องกันมิให้ *บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล* ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- ➡ จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล
- ➡ แจ้งเหตุการณ์รั่วไหลข้อมูลส่วนบุคคล โดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้
- ➡ แต่งตั้งตัวแทน จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามเงื่อนไขของข้อกฎหมาย



ผู้ประมวลผลข้อมูลส่วนบุคคล
(PII/Data Processor)

“ผู้ประมวลผลข้อมูลส่วนบุคคล” : บุคคลหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

หน้าที่

- ➡ ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น
- ➡ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
- ➡ จัดทำและเก็บรักษาบันทึกการรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่ประกาศกำหนด
- ➡ แต่งตั้งตัวแทน จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามเงื่อนไขของข้อกฎหมาย



เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
(Data Protection Officer: DPO)

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” ของผู้ควบคุมข้อมูลส่วนบุคคล หรือของผู้ประมวลผลข้อมูลส่วนบุคคล

- มีคุณสมบัติ ความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการกำหนด
- อาจเป็นพนักงานของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือเป็นผู้รับจ้างให้บริการตามสัญญากับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

หน้าที่

- ➡ ให้คำแนะนำเกี่ยวกับการปฏิบัติตาม พ.ร.บ.นี้
- ➡ ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ➡ ประสานงานและให้ความร่วมมือกับสำนักงาน
- ➡ รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้

Personal Data Protection Compliance

Principles, Rights, Responsibilities, Gap, Guidelines

Regulatory Compliance: Personal Data / Personally Identifiable Information (PII) / Privacy

PART I

'Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(Source: General Data Protection Regulation: GDPR, 2016)

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
(ที่มา: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)



สาระสำคัญของ
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
(Personal Data Protection Act)



หลักการคุ้มครองข้อมูลส่วนบุคคล
สิทธิของเจ้าของข้อมูลส่วนบุคคล
ภัยคุกคามและความเสี่ยง




บทบาทหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)



แนวทางการประเมินองค์กร (Gap)
และการเตรียมความพร้อม (Guidelines)
มาตรฐานการบริหารจัดการข้อมูลส่วนบุคคล

หลักการคุ้มครองข้อมูลส่วนบุคคล


Principles for Personal Information/Data Protection (Privacy)



ISO/IEC 27701
Extension to ISO/IEC 27001 and ISO/IEC 27002 for **Privacy Information Management** — Requirements and Guidelines (Aug,2019)



The EU General Data Protection Regulation (GDPR)



Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data



ประกาศคณะกรรมการธุรกรรม
ทางอิเล็กทรอนิกส์
เรื่อง นโยบายและแนวปฏิบัติ
ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ
พ.ศ. 2553




ISO/IEC 29100
Privacy framework



European Union Agency for Network and Information Security (ENISA)



The NIST Privacy Framework (Draft 2019)



พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ประกาศในราชกิจจานุเบกษา 27 พฤษภาคม 2562
มีผลบังคับใช้ตั้งแต่ 28 พฤษภาคม 2562

What is DPO



- Data Protection Officer is a professional defined into the General Data Protection Regulation (GDPR) of the EU.
- Since the introduction of the GDPR it was known as Chief Privacy Officer, that is a professional figure mainly diffused in the anglo-saxon culture companies.
- DPO shall have competences and skills in terms of IT Security, Process Analysis, Legal and Risk Management.
- The role of DPO consists in observing, evaluating and organizing the activities and processes of data processing.

When is a DPO required



- The GDPR requires the designation of a DPO in three specific cases:
 1. where the processing is carried out by a public authority or body (irrespective of what data is being processed);
 2. where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; and
 3. where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

DPO certification general Process



Certification must be provided by a different organisation than the training one

Certification

Training courses and examinations could be provided by external partner (ex. Local AssoDPO) or by Local BV Office

Examination

80h Training course

To be checked by the examination body

Basic requirements (academic background + experience)

Example of DPO certificate

CERTIFICATE

The training course
for
Data Protection Officer
provided by
Bureau Veritas Slovenija
is entered in the training course register
(ref. PG01, SCH73 current revisions)



CEPAS

Reg. n° 147 Issue date 27/11/2017 Annual Expiry Date 26/11/2018

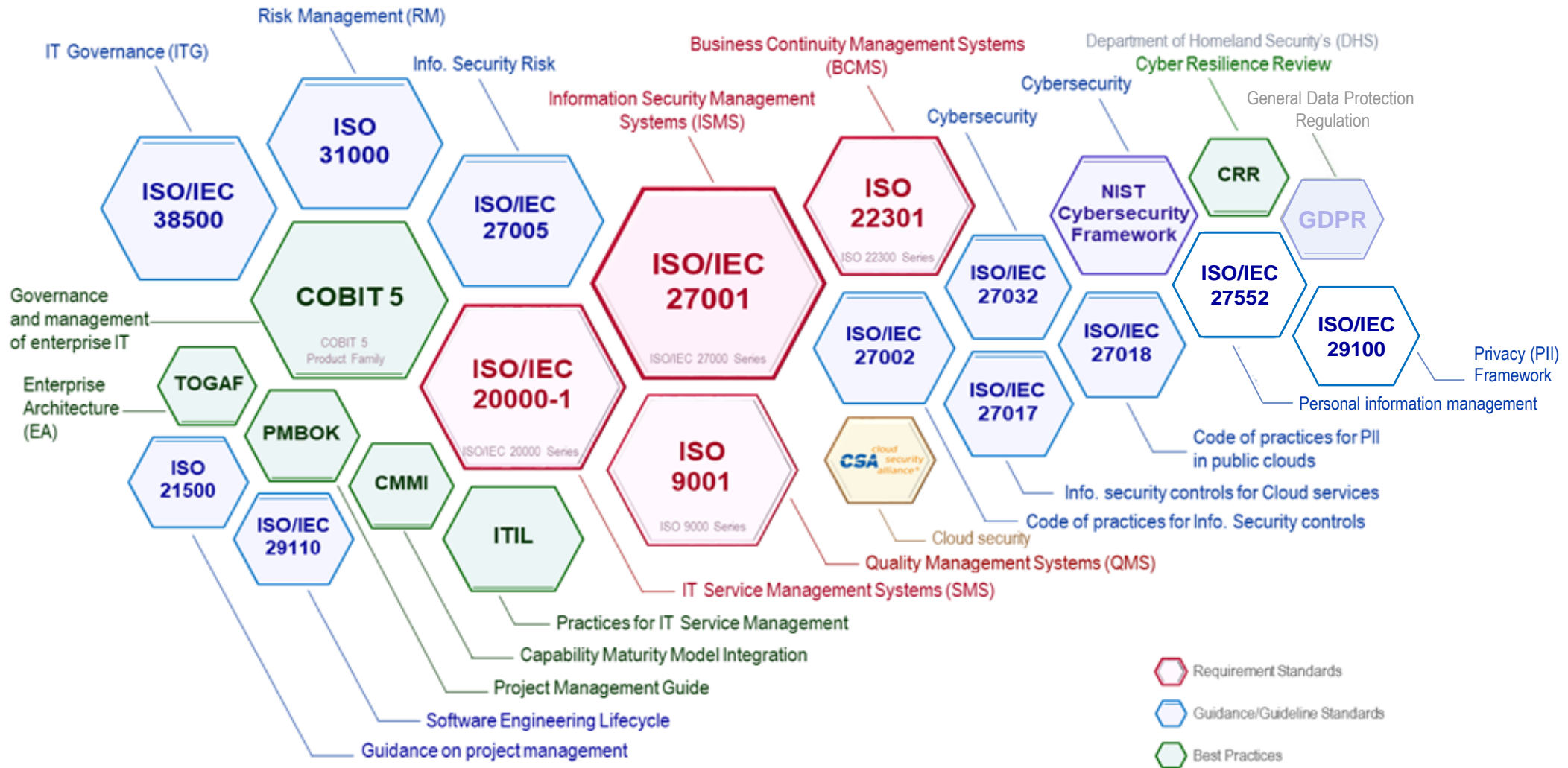
Operational & Technical Manager
Rosa Anna Favorito
Rosa Anna Favorito

This certificate is valid only if the training course is currently entered in the CEPAS register (www.cepas.it)
This certificate has been issued electronically, remains property of CEPAS srl and is bound by the conditions of contract.

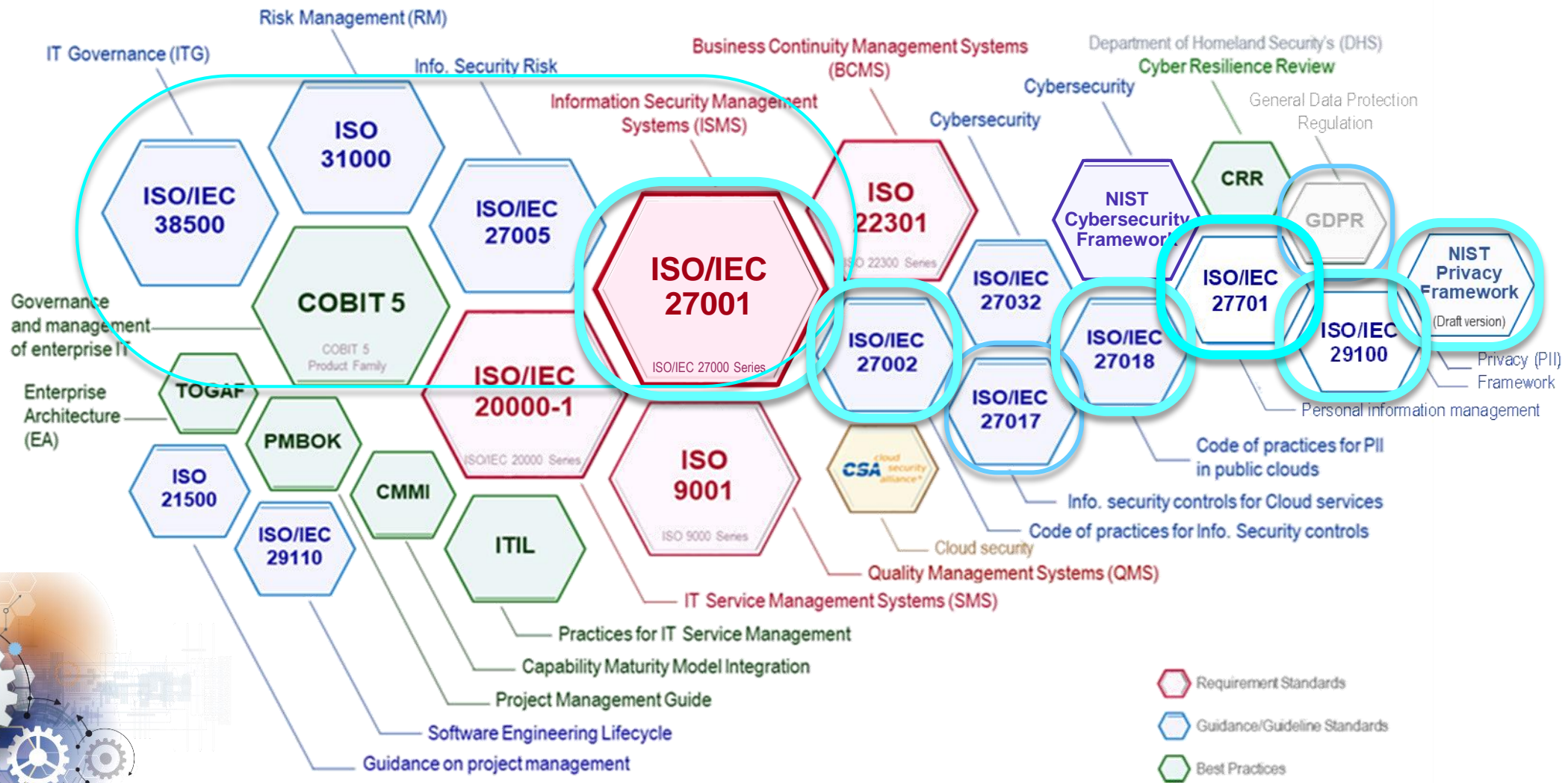
CEPAS srl – Via Mario Bianchini, 13-15 - 00142 Roma – tel. 065915373 - E-mail: comunicazioni@cepas.bureauveritas.com - Web: www.cepas.it

Key Risk-based Standards and Best Practices

for IT-GRC, Privacy, Cybersecurity and Information Security Management



Reference Risk-based Standards & Best Practices



Standards related to Privacy and Data Protection

- NIST Privacy framework (preliminary draft) :
A Tool for Improving Privacy through Enterprise Risk Management

- ISO/IEC 29100 – Privacy framework
- ISO/IEC 29101 – Privacy architecture framework

- ISO/IEC 29134 – Guidelines for privacy impact assessment
- ISO/IEC 29151 / ITU-T X.1058 – Code of practice for PII protection
- ISO/IEC 29190 – Privacy capability assessment model
- ISO/IEC 29146 – A framework for access management
- ISO/IEC 27018 – Code of practice for protection of PII in public Clouds acting as PII processors

- ISO/IEC TR 38505-1 – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data

- General Data Protection Regulation (EU GDPR)

- ISO/IEC 27701 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines

- ISO/IEC 27001 - Information Security Management Systems — Requirements

- ISO/IEC 27002 - Code of practice for information security controls

- ISO/IEC TR 38505-2 – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management

- ISO/IEC 38500 – Governance of IT for the organization

- ISO/IEC TS 38501 – Governance of IT – Implementation guide

- ISO/IEC TR 38502 – Governance of IT – Framework and model

- ISO/IEC TR 38504 – Governance of IT – Guidance for principles – based standards in the governance of IT

Overview of the NIST Privacy Framework

Data Action

A system/product/service data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.

Data Processing

The collective set of data actions.

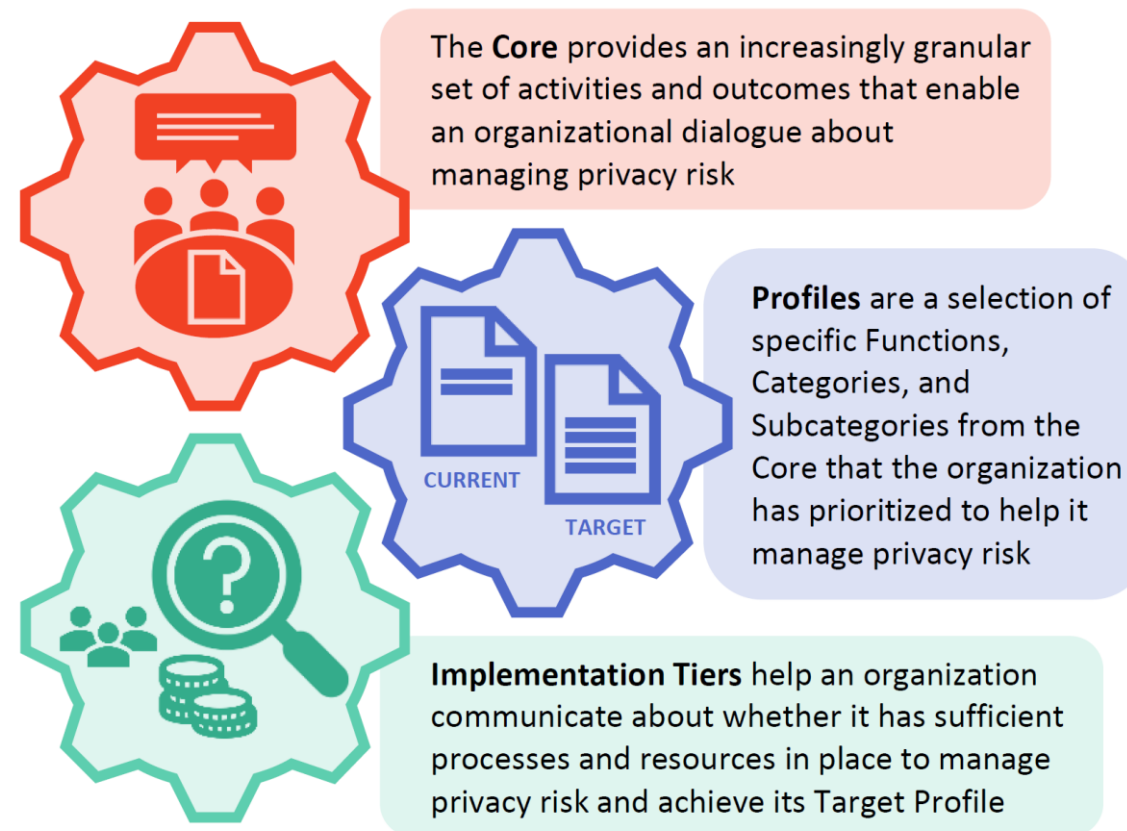


Figure 1: Core, Profiles, and Implementation Tiers

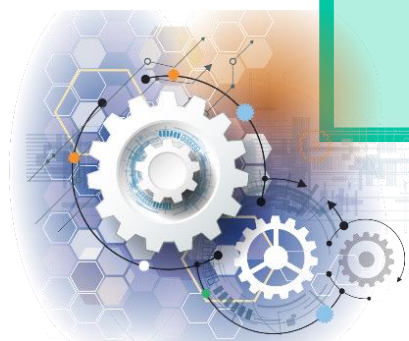
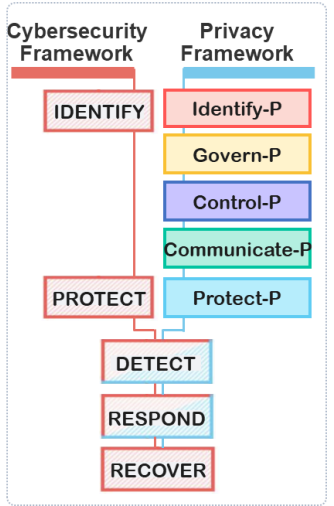


Table 1: Privacy Framework Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PP-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Management Policies, Processes, and Procedures
		CT.DM-P	Data Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PP-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.DP-P	Data Protection Policies, Processes, and Procedures
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology

Function Unique Identifier	Function	Category Unique Identifier	Category
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications



ISO/IEC 29100:2011 Privacy Framework

The Privacy Principles

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

Privacy Framework

Privacy Risk Assessment

Privacy Impact Assessment

อธิบาย/ดูรายละเอียดเพิ่มเติมในการบรรยาย Day 2 (Part II)
หัวข้อ 6 กรอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

Intensive Masterclass: **PART II**

5 | แนวทางดำเนินการสอดคล้องตามกฎเกณฑ์ GDPR

ภาพรวมความสอดคล้องของกฎหมายกับข้อกำหนด GDPR แนวทางดำเนินการตามกฎหมายกับข้อกำหนด GDPR การจัดทำรายงาน/บุคคลภายนอก (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)

6

6 | กรอบมาตรฐานฯ การประเมินผลกระทบและความเสี่ยง

กรอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (Privacy Framework) แนวทางการประเมินผลกระทบและความเสี่ยง แนวทางการจัดทำมาตรการและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

7

7 | แนวทางดำเนินการกำกับดูแลและบริหารจัดการข้อมูล

ภาพรวมการจัดการข้อมูลด้านกระบวนการและด้านเทคนิค แนวทางการกำกับดูแลข้อมูล (Data Governance) แนวทางการบริหารจัดการข้อมูล (Data Management) แนวทางการจัดชั้นข้อมูล (Data Classification)

8

8 | แนวทางการจัดการข้อมูล

แนวทางการจัดการข้อมูลด้านเทคนิค (Data Quality Management, Metadata, ฯลฯ) และกระบวนการทางเทคนิค

ISO/IEC 29101:2013 Privacy Architecture Framework

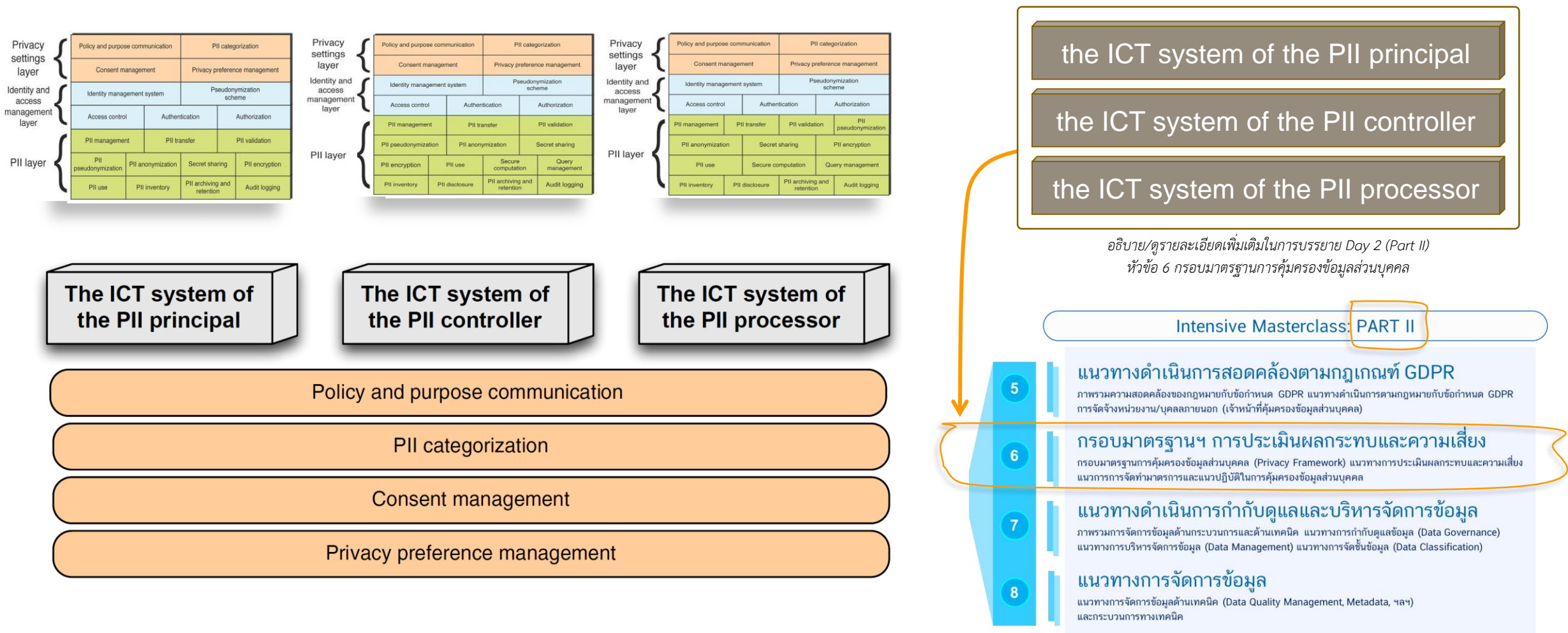
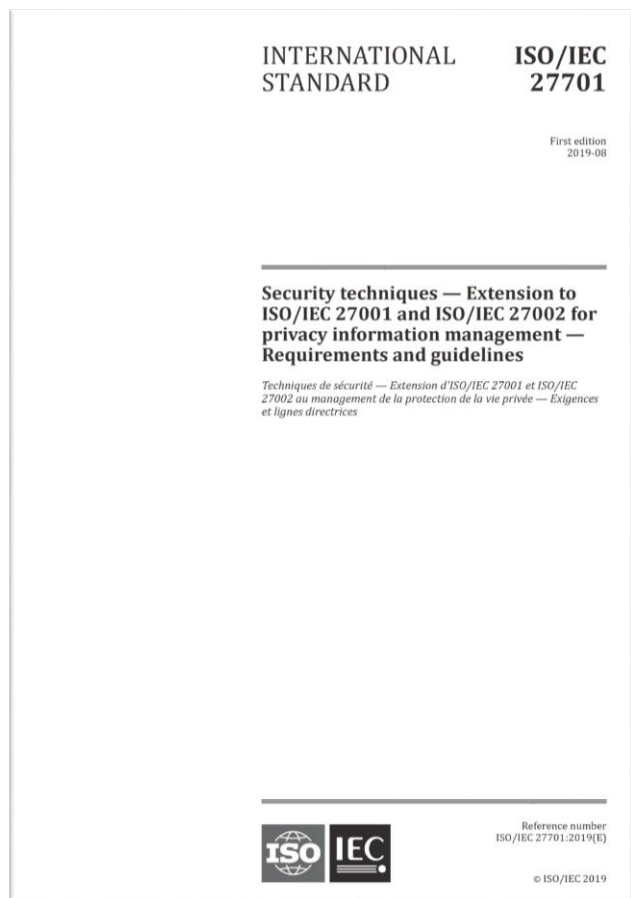


Figure 6 — The deployment of components in the privacy settings layer

ISO/IEC 27701:2019 Privacy Information Management

Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines



PIMS-specific requirements related to ISO/IEC 27001

General and 7 Requirements Clauses

PIMS-specific guidance related to ISO/IEC 27002

General and 14 Domains, 114 Controls

Additional ISO/IEC 27002 guidance for PII controllers

Conditions for collection and processing

Obligations to PII principals

Additional ISO/IEC 27002 guidance for PII processors

Privacy by design and privacy by default

PII sharing, transfer, and disclosure

Annex A (normative) PIMS-specific reference control objectives and controls (PII Controllers)

Annex B (normative) PIMS-specific reference control objectives and controls (PII Processors)

Annex C (informative) Mapping to ISO/IEC 29100

Annex D (informative) Mapping to the General Data Protection Regulation

Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151

Annex F (informative) How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

INTERNATIONAL
STANDARD

ISO/IEC
27701

First edition
2019-08

**Security techniques — Extension to
ISO/IEC 27001 and ISO/IEC 27002 for
privacy information management —
Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC
27002 au management de la protection de la vie privée — Exigences
et lignes directrices*

Annex A (normative)

PIMS-specific reference control objectives and controls (PII Controllers)

This annex is for use by organizations acting as PII controllers, with or without the use of PII processors. It extends ISO/IEC 27001:2013, Annex A.

The additional or modified control objectives and controls listed in [Table A.1](#) are directly derived from and aligned with those defined in this document and are to be used in context with ISO/IEC 27001:2013, 6.1.3 as refined by [5.4.1.3](#).

Not all the control objectives and controls listed in this annex need to be included in the PIMS implementation. A justification for excluding any control objectives shall be included in the Statement of Applicability (see [5.4.1.3](#)). Justification for exclusion can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the applicable legislation and/or regulation.

NOTE Clause numbers in this annex relate to the subclause numbers in [Clause 7](#).

Table A.1 — Control objectives and controls

A.7.2 Conditions for collection and processing		
Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.		
A.7.2.1	Identify and document purpose	<i>Control</i> The organization shall identify and document the specific purposes for which the PII will be processed.
A.7.2.2	Identify lawful basis	<i>Control</i> The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.
A.7.2.3	Determine when and how consent is to be obtained	<i>Control</i> The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals
A.7.2.4	Obtain and record consent	<i>Control</i> The organization shall obtain and record consent from PII principals according to the documented processes.

Cybersecurity and Privacy Risk Relationship

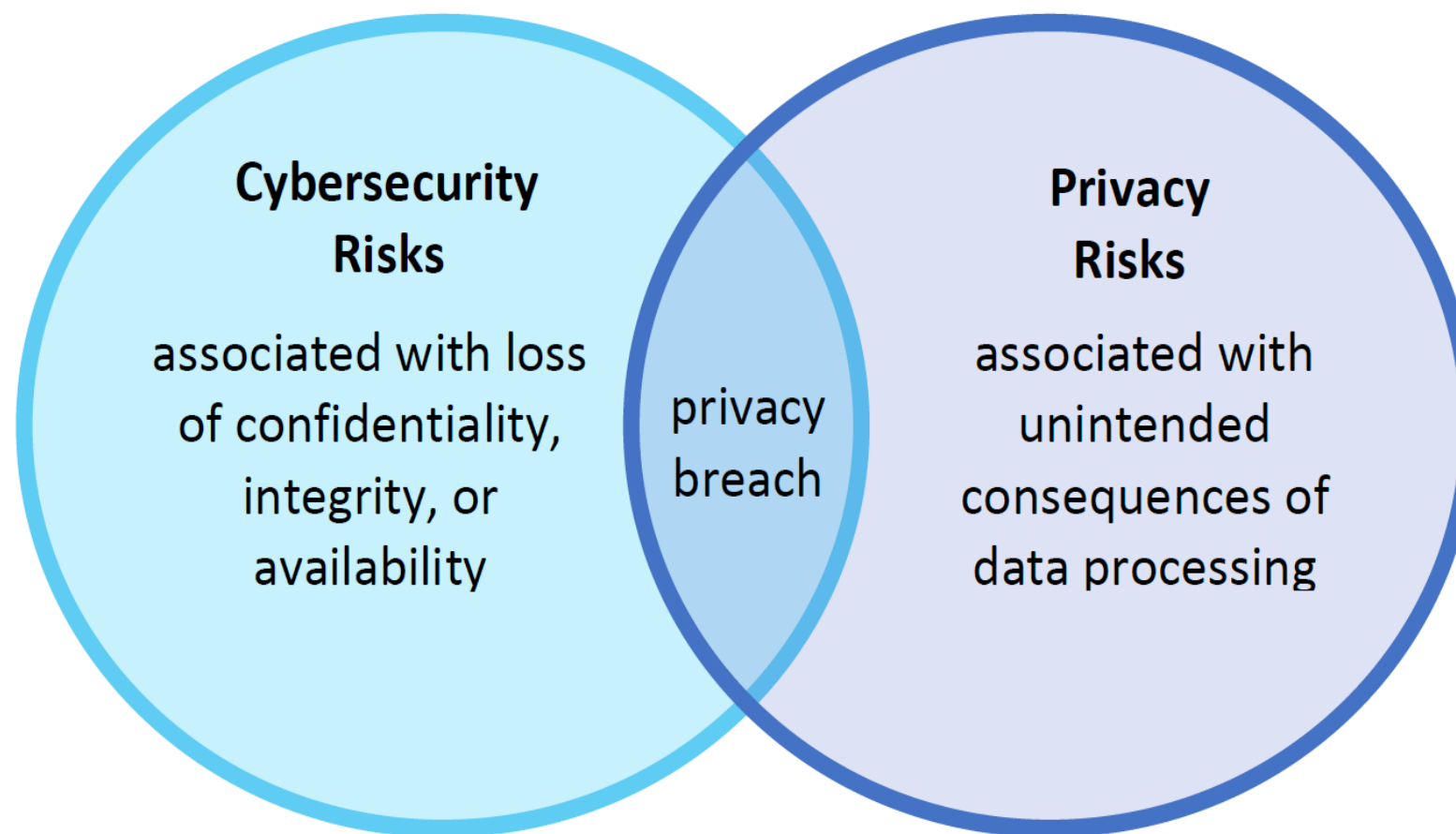


Figure 2: Cybersecurity and Privacy Risk Relationship

Cybersecurity and Privacy Risk Relationship

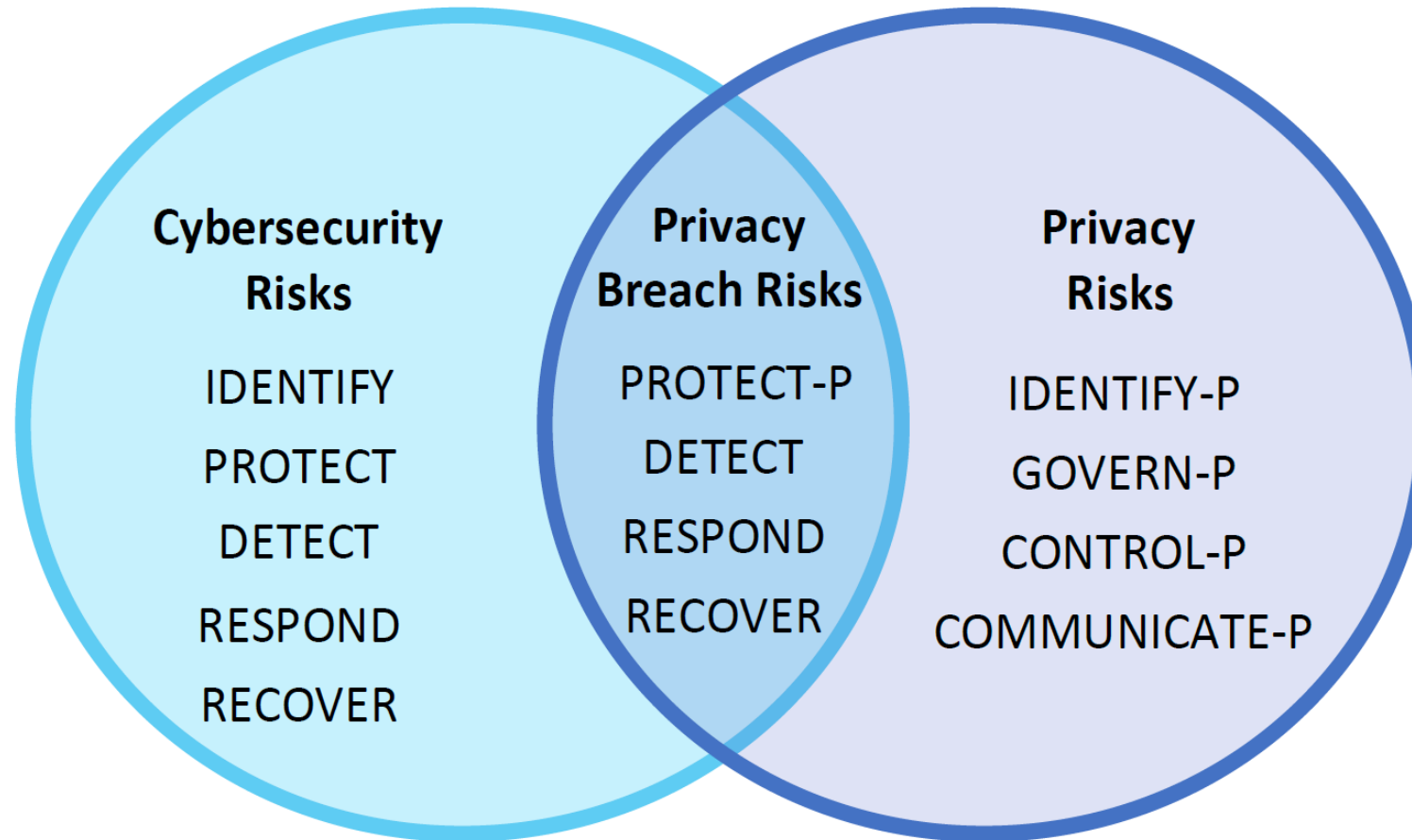
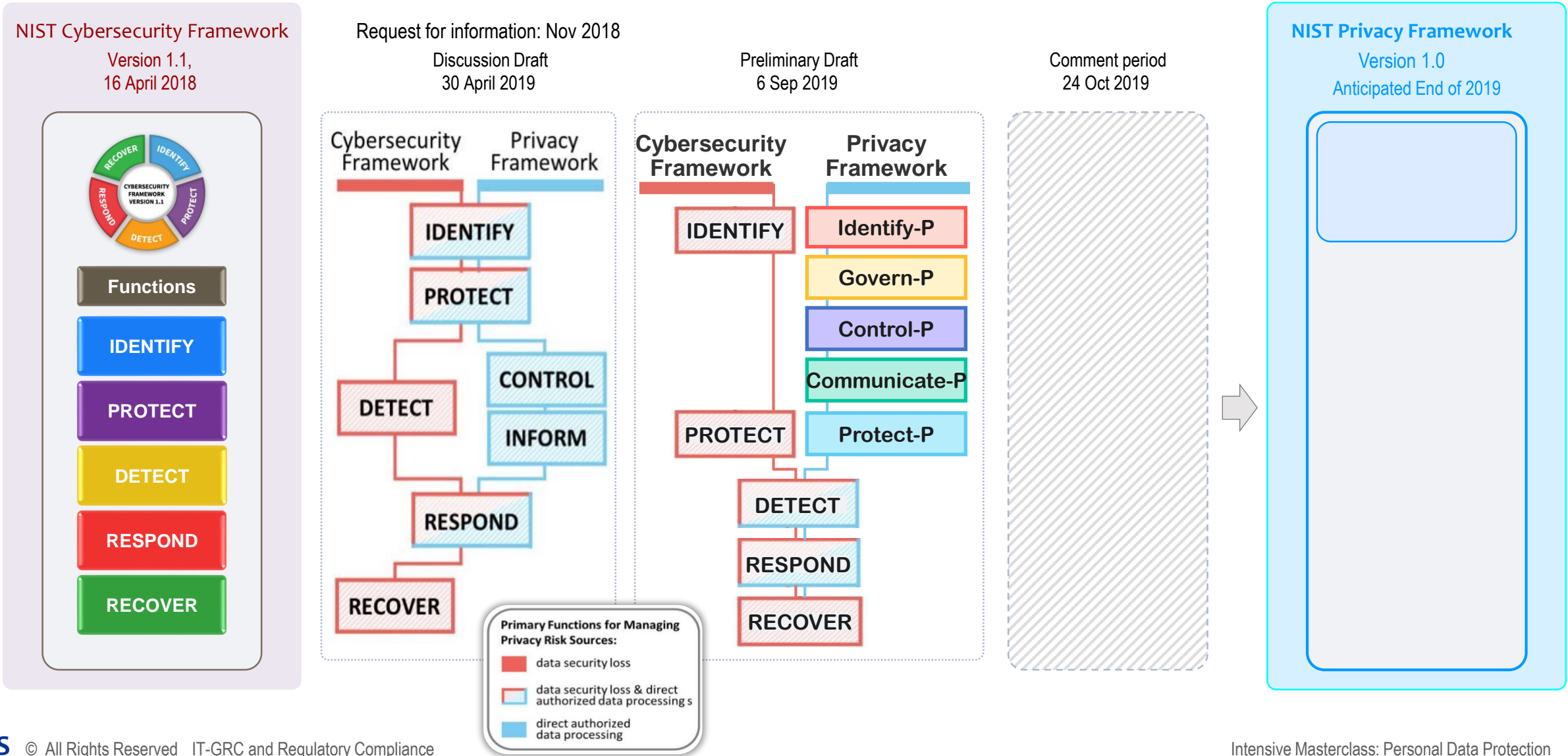


Figure 8: Using Functions to Manage Privacy Risk

NIST Cybersecurity Framework and Privacy Framework



Data Protection Implementation

Impact & Risk Assessment, Data Governance & Management

General Data Protection Regulation, Personal Data Protection Framework, Process and Technique

PART II

'Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(Source: General Data Protection Regulation: GDPR, 2016)

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (ที่มา: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)



แนวทางดำเนินการ
สอดคล้องตามกฎหมาย GDPR



กรอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล
การประเมินผลกระทบ การประเมินความเสี่ยง



แนวทางดำเนินการกำกับดูแล
และบริหารจัดการข้อมูล



แนวทางการจัดการข้อมูล
และกระบวนการทางเทคนิค

Key Takeaway

Credit :

**There is no “one size fits all”
in privacy and security**

Credit : <https://staysafeonline.org/>

**We are only as secure as the
weakest link**

Credit : <https://staysafeonline.org/>

**You can have security without
privacy, but you can't have
privacy without security**

Credit : <https://staysafeonline.org/>

**The bottom line is no person
or business is without risk –
and we are often unaware of
the magnitude of our
exposure.**

Credit : <https://staysafeonline.org/>

We all have an obligation to ourselves to protect our information. When we entrust our data to a company, it becomes a shared partnership to protect that data.

Credit : <https://staysafeonline.org/>

**Security and transparency are
privacy's key driver of
success.**

Credit : <https://staysafeonline.org/>



Thailand Information Security Association (TISA)
www.TISA.or.th



Cyber Defense Initiative Conference
www.cdiconference.com



ACIS Professional Center Co., Ltd.
www.acisonline.net



www.youtube.com/thehackertv



www.youtube.com/thecyber911



Prinya.ho@acisonline.net



www.twitter.com/prinyaACIS (@prinyaacis)



www.facebook.com/acisonline
www.facebook.com/prinyah

Facebook search : prinya hom-anek

ขอบคุณครับ

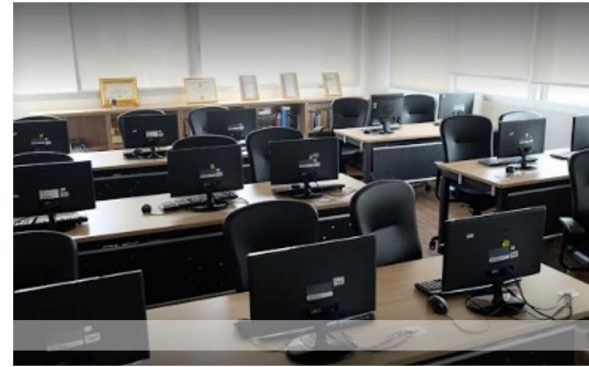


ACIS Professional Center Co., Ltd.
YOUR SATISFACTION IS OUR PRIDE

140/1 Kian Gwan Building 2, 18th Floor, Wireless Road, Lumpini,
Pathumwan, Bangkok 10330, Thailand
Tel: +66 2 253 4736, Fax: +66 2 253 4737 www.acisonline.net



ACIS Professional Center Co., Ltd.



"Security Intelligence"



ACIS Professional Center Co., Ltd.
YOUR SATISFACTION IS OUR PRIDE

140/1 Kian Gwan Building 2, 18th Floor, Wireless Road, Lumpini, Pathumwan, Bangkok 10330, Thailand
Tel: +66 2 253 4736, Fax: +66 2 253 4737 www.acisonline.net