



**LAW
CHULA**

TDPG 3.0

Thailand Data Protection
Guidelines 3.0 - **Business Functions**

ติดตามการเปิดตัวโครงการ ที่นี่

>>> FB Law Chula เร็วๆ นี้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. 2562

ปิยะบุตร บุญอร่ามเรือง
คณะนิติศาสตร์
จุฬาลงกรณ์มหาวิทยาลัย

Faculty of Law, Chulalongkorn University

THAILAND DATA PROTECTION

GUIDELINES 2.0

แนวปฏิบัติเกี่ยวกับการคุ้มครอง
ข้อมูลส่วนบุคคล



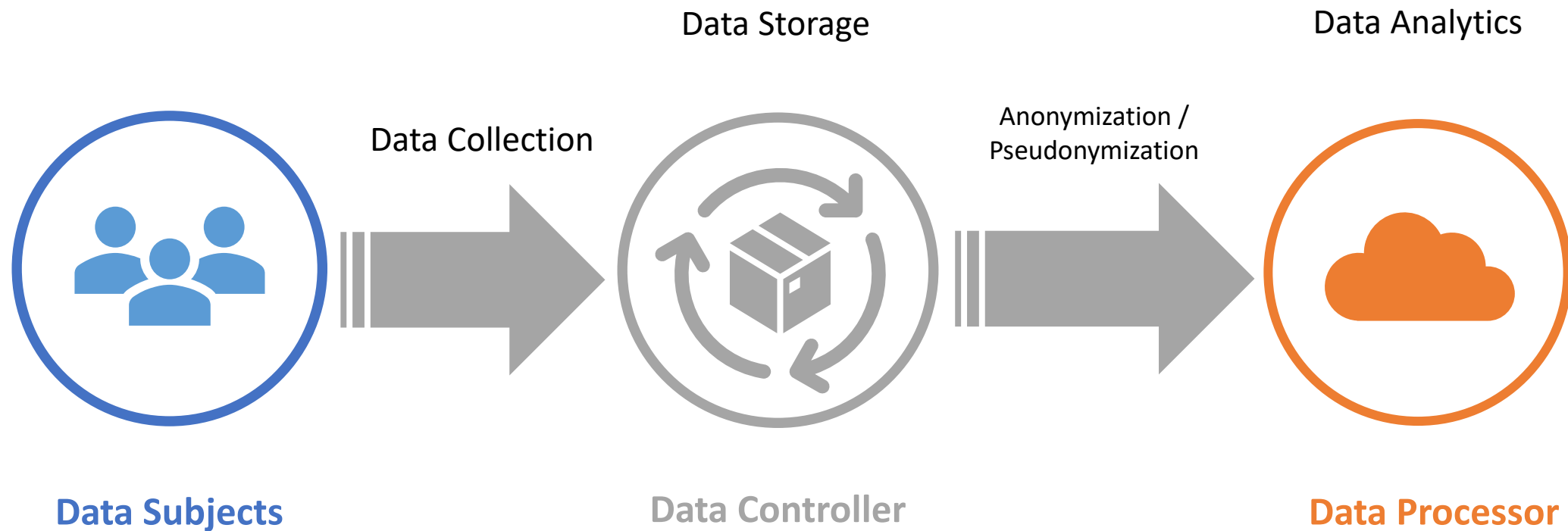
<http://www.law.chula.ac.th/event/7721/>

ISBN 978-616-407-458-3

เอกสารนี้ไม่ได้ให้การรับรองหรือรับประกันใดๆถึงความถูกต้องครบถ้วนของเนื้อหาของงานนี้ และขอปฏิเสธอย่างชัดแจ้งว่าไม่ได้ให้การรับรองหรือรับประกันใดๆทั้งสิ้นต่อเนื้อหาของงานนี้ โดยข้อแนะนำที่ปรากฏในงานนี้อาจไม่เหมาะสมต่อสถานการณ์บางลักษณะ เนื้อหาของงานนี้จึงไม่ใช่การให้คำปรึกษาทางกฎหมายหรือคำปรึกษาทางวิชาชีพใดๆทั้งสิ้น หากผู้ฟังหรือผู้อ่านจำเป็นต้องได้รับคำปรึกษาที่เกี่ยวข้อง ผู้อ่านจำเป็นต้องติดต่อขอคำปรึกษาจากผู้เชี่ยวชาญในด้านนั้นโดยตรง ผู้บรรยายจึงไม่มีความรับผิดชอบและไม่ต้องรับผิดชอบใดๆต่อความเสียหายที่อ้างว่าเกิดขึ้นจากการปฏิบัติตามเนื้อหาของงานนี้ และหากมีการอ้างอิงใดๆถึงงานนี้ไม่ว่าในรูปแบบใด ผู้บรรยายขอปฏิเสธอย่างชัดแจ้งไม่ให้การรับรองหรือการรับประกันการอ้างอิงนั้น การรับรองใดๆที่อาจมีขึ้นต้องออกเป็นหนังสือโดยผู้บรรยายเท่านั้น นอกจากนี้ผู้ฟังหรือผู้อ่านควรตระหนักไว้ด้วยว่าการคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องที่กำลังมีการพัฒนาและปรับปรุงอย่างรวดเร็วในปัจจุบัน เนื้อหาหลายประการในที่นี้อาจล้าสมัยหรือไม่เหมาะสมในหลายสถานการณ์เมื่อเวลาผ่านไป รายการอ้างอิงใดๆในงานนี้ก็อาจมีการเปลี่ยนแปลงหรือสูญหายไปได้เมื่อเวลาที่ท่านได้อ่านงานนี้

เอกสารนี้ได้รับความคุ้มครองตามกฎหมายลิขสิทธิ์และกฎหมายอื่นที่ใช้บังคับ ห้ามนำงานไปใช้อย่างอื่นนอกจากการใช้ที่ได้รับอนุญาตเป็นลายลักษณ์อักษรหรือตามกฎหมายลิขสิทธิ์ โดยเอกสารนี้ได้จัดให้ใช้ได้ตามข้อตกลงของสัญญาอนุญาตสาธารณะของ Creative Commons แบบแสดงที่มา 3.0 ประเทศไทย (CC BY 3.0 TH), <https://creativecommons.org/licenses/by/3.0/th/legalcode>

“ส่งเสริมและสนับสนุนให้เกิดการใช้ประโยชน์ข้อมูลส่วนบุคคลอย่างปลอดภัย
และสอดคล้องตามมาตรฐานสากล”



ภูมิทัศน์ดิจิทัลของไทยในระยะเวลา 20 ปี

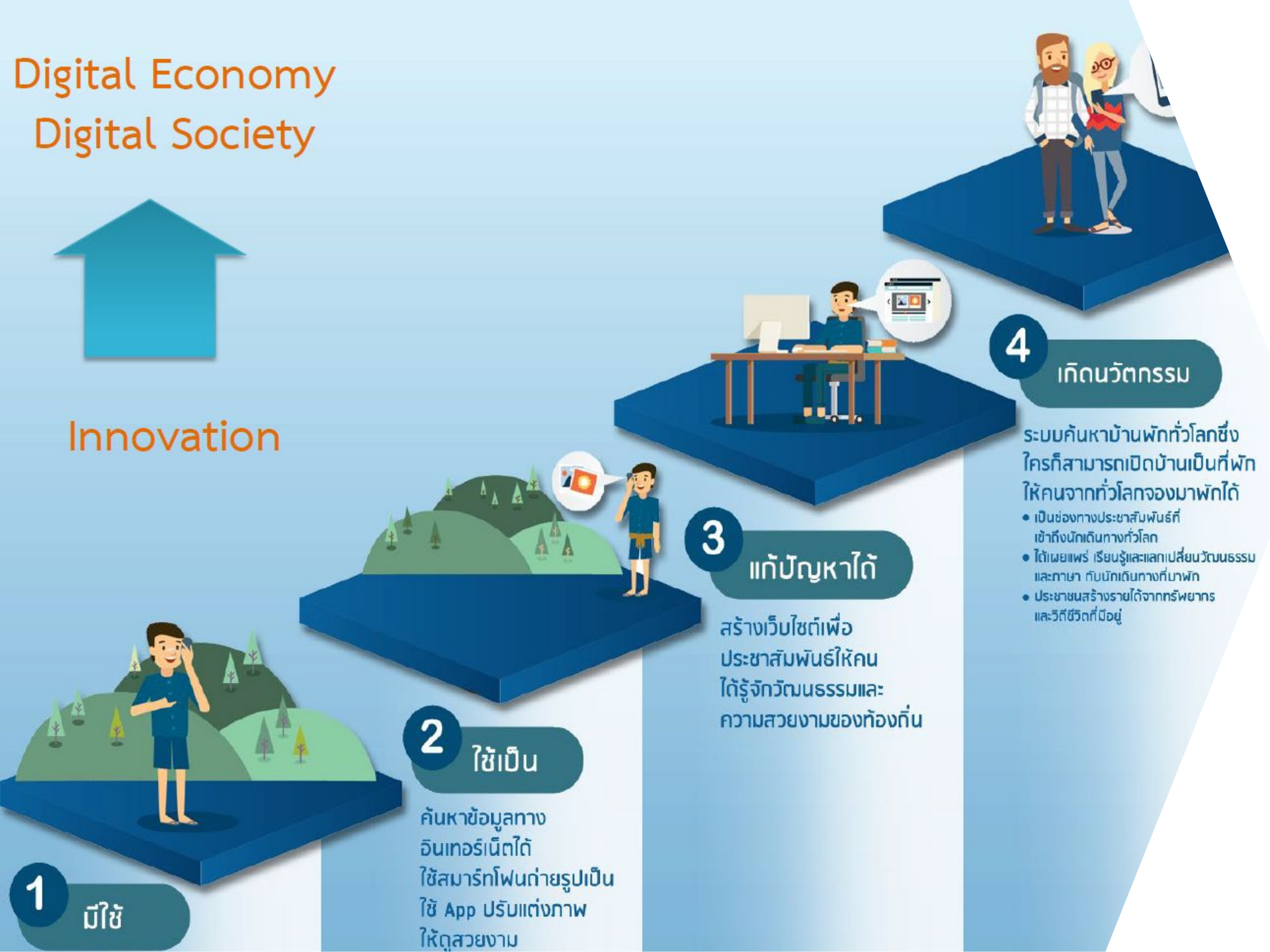


แผนพัฒนาดิจิทัลเพื่อ
เศรษฐกิจและสังคม
(5 เมษายน 2559)

Digital Economy Digital Society



Innovation



1

มีใช้

2

ใช้เป็น

ค้นหาข้อมูลทาง
อินเทอร์เน็ตได้
ใช้สมาร์ทโฟนถ่ายรูปเป็น
ใช้ App ปรับแต่งภาพ
ให้ดูสวยงาม

3

แก้ปัญหาได้

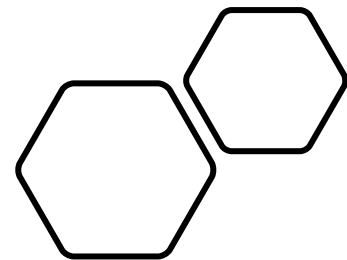
สร้างเว็บไซต์เพื่อ
ประชาสัมพันธ์ให้คน
ได้รู้จักวัฒนธรรมและ
ความสวยงามของท้องถิ่น

4

เกิดนวัตกรรม

ระบบค้นหาบ้านพักทั่วโลกซึ่ง
ใครก็สามารถเปิดบ้านเป็นที่พัก
ให้คนจากทั่วโลกจองมาพักได้

- เป็นช่องทางประชาสัมพันธ์ที่
เข้าถึงนักท่องเที่ยวทั่วโลก
- ได้เผยแพร่ เรียนรู้และแลกเปลี่ยนวัฒนธรรม
และภาษา กับนักท่องเที่ยวที่มาพัก
- ประชาชนสร้างรายได้จากทรัพยากร
และวิถีชีวิตที่มีอยู่



Thailand Digital Economy Policy



Infrastructure

Netpracharat
5G
Data Center
ASEAN Hub
Satellite



Security

Data Protection
Cybersecurity
e-Commerce



Service

Digital Government
NDID
Open Data



Promotion

Tech Startup
Business
Transformation
SMEs
Digital Content



Society

Digital Literacy
Inclusive Society



Workforce

ICT Professional
ICT Expat

Thailand near bottom of privacy protection table

New cybersecurity law could be used 'to silence critics', says Comparitech survey of 47 countries

PUBLISHED : 16 OCT 2019 AT 19:45

WRITER: [POST REPORTERS](#)

302



22





พรบ.ปรับปรุงกระทรวง
ทบวง กรม (ฉบับที่ 17) พ.ศ.
2559 (เพื่อจัดตั้งกระทรวง
ดิจิทัลเพื่อเศรษฐกิจและ
สังคม)



พรบ.การพัฒนาดิจิทัลเพื่อ
เศรษฐกิจและสังคม
พ.ศ.2560



พรบ.ว่าด้วยการกระทำ
ความผิดเกี่ยวกับ
คอมพิวเตอร์ พ.ศ.2560



พรบ.องค์กรจัดสรรคลื่น
ความถี่และกำกับการประกอบ
กิจการวิทยุกระจายเสียง วิทยุ
โทรทัศน์ และกิจการ
โทรคมนาคม (ฉบับที่ 2)
พ.ศ.2560



พรบ.องค์กรจัดสรรคลื่น
ความถี่และกำกับการประกอบ
กิจการวิทยุกระจายเสียง วิทยุ
โทรทัศน์ และกิจการ
โทรคมนาคม (ฉบับที่ 3)
พ.ศ.2562



พรบ.ว่าด้วยธุรกรรมทาง
อิเล็กทรอนิกส์
(ฉบับที่ 3) พ.ศ.2562



พรบ.ว่าด้วยธุรกรรมทาง
อิเล็กทรอนิกส์
(ฉบับที่ 4) พ.ศ.2562



พรบ.สำนักงานพัฒนา
ธุรกรรมทางอิเล็กทรอนิกส์
พ.ศ.2562



พรบ.ว่าด้วยการรักษาความ
มั่นคงปลอดภัยไซเบอร์
พ.ศ.2562



พรบ.คุ้มครองข้อมูลส่วน
บุคคล พ.ศ.2562



พรบ.การบริหารงานและการ
ให้บริการภาครัฐผ่านระบบ
ดิจิทัล พ.ศ.2562



พรบ.สภาดิจิทัลเพื่อเศรษฐกิจ
และสังคมแห่งประเทศไทย
พ.ศ.2562

กำเนิดสถาบันดิจิทัล

ภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ONDE : Office of National Digital Economy

DF : Digital Fund

DEPA : Digital Economy Promotion Agency

DSI : Digital Startup Institute

Ali : Artificial Intelligence Institute

GBDi : Government Big Data Institute

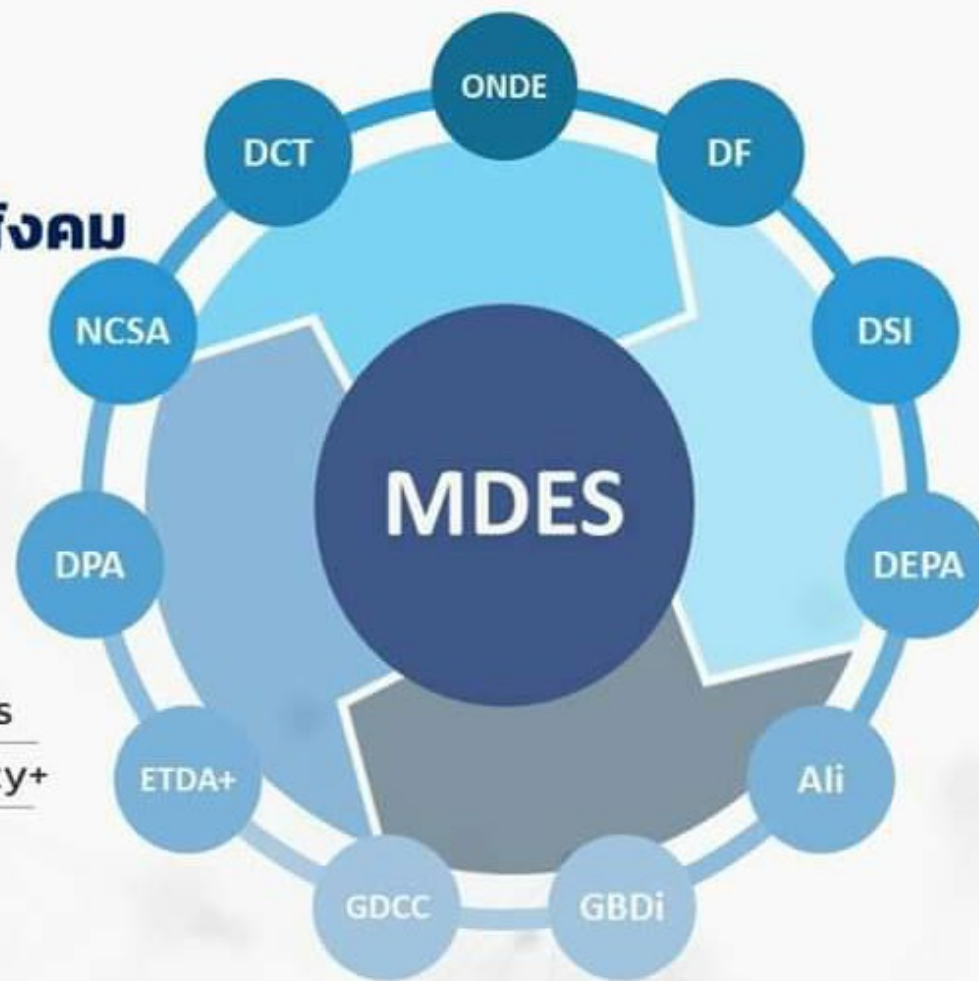
GDCC : Government Data Center and Cloud Services

ETDA+ : Electronic Transactions Development Agency+

DPA : Data Protection Agency

NCSA : National Cyber Security Agency

DCT : Digital Council of Thailand



พระราชบัญญัติคุ้มครอง
ข้อมูลส่วนบุคคล
พ.ศ.2562

มาตรา 81 ในกรณีที่ผู้กระทำความผิดตาม

พระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย



โทษอาญา
จำคุกไม่เกิน 1 ปี
ปรับไม่เกิน 1,000,000 บาท



โทษทางปกครอง
5,000,000 บาท



ความรับผิดทางแพ่ง
2 X ค่าสินไหมทดแทน

พระราชบัญญัติแก้ไขเพิ่มเติมบทบัญญัติแห่งกฎหมายที่เกี่ยวกับ
ความรับผิดในทางอาญาของผู้แทนนิติบุคคลพ.ศ. 2560 (76 ฉบับ)

ในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจาก

- การสั่งการหรือการกระทำของกรรมการ หรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือ
- ในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด
- ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

1) การขายทอดตลาดและค้าของเก่า	27) การอนุรักษ์พลังงาน	53) การประกอบกิจการโทรคมนาคม
2) ประมวลรัษฎากร	28) รักษาคุณภาพสิ่งแวดล้อมแห่งชาติ	54) ธุรกิจทางอิเล็กทรอนิกส์
3) เรือไทย	29) วัตถุอันตราย	55) การพาณิชย์สงเคราะห์
4) การเดินอากาศ	30) โรงงาน	56) สัญญาซื้อขายล่วงหน้า
5) ความผิดเกี่ยวกับห้างหุ้นส่วน บริษัทจำกัด สมาคม และมูลนิธิ	31) ประกันชีวิต	57) สถาบันอุดมศึกษาเอกชน
6) สถานบริการ	32) ประกันวินาศภัย	58) สิ่งบ่งชี้ทางภูมิศาสตร์
7) ภาษีป้าย	33) สภาผู้ส่งสินค้าทางเรือ	59) วิชาชีพบัญชี
8) องค์การสงเคราะห์ทหารผ่านศึก	34) ลิขสิทธิ์	60) การผลิตผลิตภัณฑ์ที่ดี
9) ภาษีเงินได้ปิโตรเลียม	35) กองทุนบำเหน็จบำนาญข้าราชการ	61) การขนส่งต่อเนื่องหลายรูปแบบ
10) ปู่ย	36) บริษัทบริหารสินทรัพย์	62) โรงงานผลิตอาวุธของเอกชน
11) คนเข้าเมือง	37) ราคาสินค้าและบริการ	63) การประกอบกิจการพลังงาน
12) สิทธิบัตร	38) ป้องกันและปราบปรามการฟอกเงิน	64) โรงเรียนเอกชน
13) การรับเด็กเป็นบุตรบุญธรรม	39) มาตราชั่งตวงวัด	65) กรัสด์เพื่อธุรกิจในตลาดทุน
14) อาคารชุด	40) กลุ่มครองพันธุ์พืช	66) องค์การกระจายเสียงและแพร่ภาพสาธารณะแห่งประเทศไทย
15) กลุ่มครองผู้บริโภคร	41) ภูมิปัญญาการแพทย์แผนไทย	67) ธุรกิจสถาบันการเงิน
16) ควบคุมอาคาร	42) วิศวกร	68) กลุ่มครองซากดึกดำบรรพ์
17) งดเซยค่าภาษีอากรสินค้าส่งออกที่ผลิตในราชอาณาจักร	43) ควบคุมน้ำมันเชื้อเพลิง	69) สถาบันคุ้มครองเงินฝาก
18) ควบคุมสินค้าตามชายแดน	44) สถาปนิก	70) การดูแลผลประโยชน์ของคู่สัญญา
19) อ้อยและน้ำตาลทราย	45) การขุดดินและถมดิน	71) มาตรฐานสินค้าเกษตร
20) การกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน	46) การบัญชี	72) การมาตรฐานแห่งชาติ
21) จัดหางานและคุ้มครองคนหางาน	47) กลุ่มครองแบบผังภูมิของวงจรรวม	73) ภาพยนตร์และวีดิทัศน์
22) กองทุนสำรองเลี้ยงชีพ	48) การจัดสรรที่ดิน	74) เครื่องมือแพทย์
23) ประกันสังคม	49) การจัดการหุ้นส่วนและหุ้นของรัฐมุนตรี	75) กลุ่มครองผู้รับงานไปทำที่บ้าน
24) การเล่นแชร์	50) การค่าน้ำมันเชื้อเพลิง	76) กองทุนการออมแห่งชาติ
25) ทะเบียนราษฎร	51) การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย	
26) สงวนและคุ้มครองสัตว์ป่า	52) กองทุนสนับสนุนการสร้างเสริมสุขภาพ	

รัฐธรรมนูญแห่ง
ราชอาณาจักรไทย
พ.ศ.2560

มาตรา 32 บุคคลย่อมมีสิทธิในความ
เป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

การกระทำอันเป็นการละเมิดหรือกระทบ
ต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูล
ส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใดๆ จะ
กระทำได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติ
แห่งกฎหมายที่ตราขึ้นเพียงพอที่จำเป็นเพื่อ
ประโยชน์สาธารณะ

ประมวลกฎหมายแพ่ง และพาณิชย์

มาตรา 420 ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่น โดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่า ผู้นั้นทำละเมิด จำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น

มาตรา 421 การใช้สิทธิซึ่งมีแต่จะให้เกิดเสียหายแก่บุคคลอื่นนั้น ท่านว่าเป็นการอันมิชอบด้วยกฎหมาย

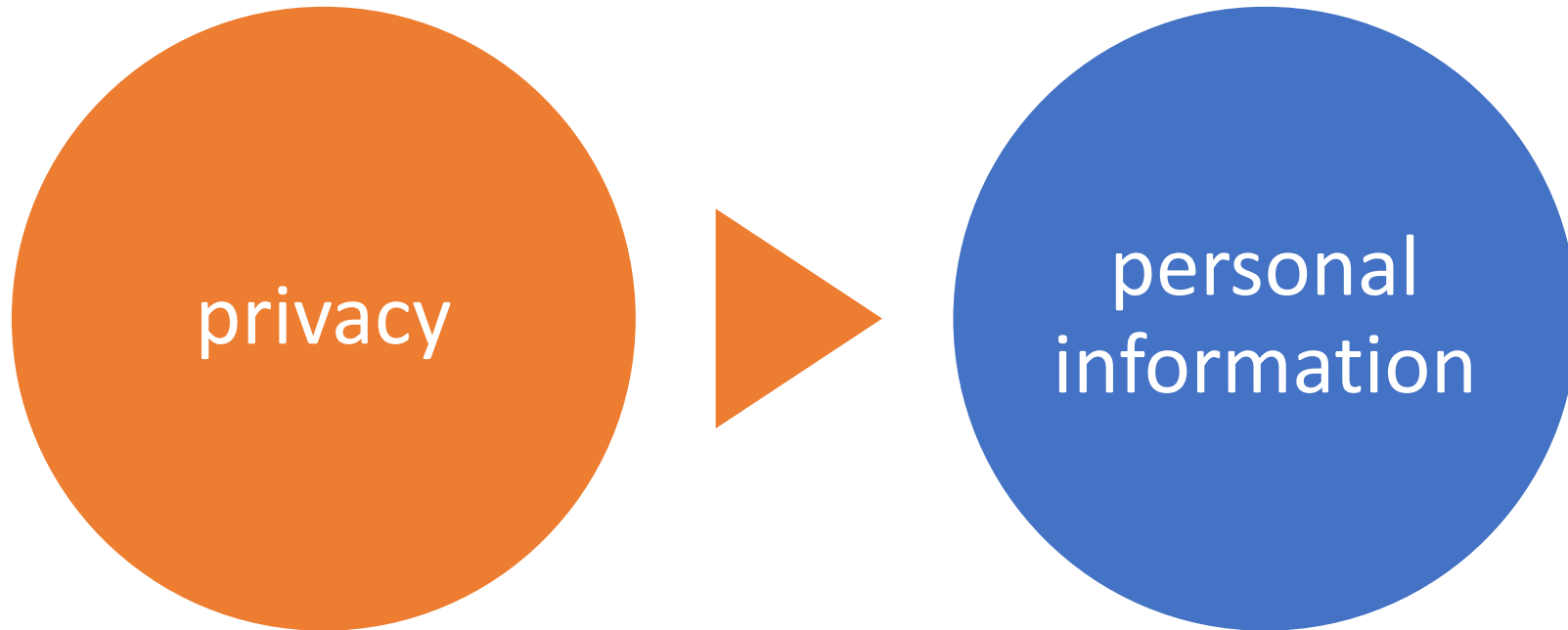
คำพิพากษาศาลฎีกาที่ 4893/2558

ข้อเท็จจริงฟังได้ว่า การกระทำของจำเลยทั้งสองเป็นการละเมิดสิทธิในความเป็นส่วนตัวของโจทก์ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 มิใช่เป็นการกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนต่อความจริง ตามมาตรา 423 โจทก์จึงไม่อาจเรียกให้จำเลยทั้งสองรับผิดชอบในความเสียหายแก่ชื่อเสียงหรือเกียรติคุณและความเสียหายแก่ทางทำมาหาได้หรือทางเจริญของตนโดยประการอื่นอันเป็นค่าสินไหมทดแทนอันเนื่องมาจากการกระทำละเมิดตามมาตรา 423 ได้ โจทก์คงเรียกได้เฉพาะค่าเสียหายจากการละเมิดสิทธิในความเป็นส่วนตัวเท่านั้น



This Photo by Unknown Author is licensed under [CC BY-SA](#)

Privacy as Control over Personal Information



Singapore

Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted

A total of 1.5 million SingHealth patients' non-medical personal data were stolen, while 160,000 of those had their dispensed medicines' records taken too, according to MCI and MOH.



Marriott now says 5 million unencrypted passport numbers were stolen in Starwood hotel data breach

Zack Whittaker
@zackwhittaker / 3 weeks ago



Sport | **Football**

More ▾

🏠 > Sport > Football

Exclusive: West Ham could face investigation after sharing personal data of up to 200 season ticket holders in email error



Technology

Facebook fined £500,000 for Cambridge Analytica scandal

🕒 25 October 2018



Facebook-Cambridge Analytica data breach



GETTY IMAGES

Facebook's chief executive has repeatedly declined to answer questions from UK MPs about the scandal

Facebook has been fined £500,000 by the UK's data protection watchdog for its role in the Cambridge Analytica data scandal.

News Opinion Sport Culture Lifestyle



British Airways

British Airways: 185,000 more passengers may have had details stolen

LATEST: Macron not responsive enough to Yellow Jackets: poll



Swedish Minister for Home Affairs Anders Ygeman gives an interview after resigning his position | Ari Luostarinen/AFP via Getty Images

Swedish ministers resign amid data security breach scandal Citizens' sensitive personal information may have been leaked.

By MARK SCOTT AND CONNOR MURPHY | 7/27/17, 6:21 PM CET | Updated 1/28/18, 10:21 PM CET



**Lawfulness of
Processing**



Data Security



**Lawfulness, Fairness
And Transparency**



Purpose Limitation



Data Minimization



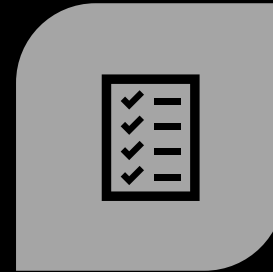
Accuracy



Storage Limitation



**Integrity and
Confidentiality**



Accountability

Records of Processing Activities



Descriptions



Collection



Storage



Usage



Transfer



Disposal



Access
Control



Encryption



Availability



Backup



Recovery



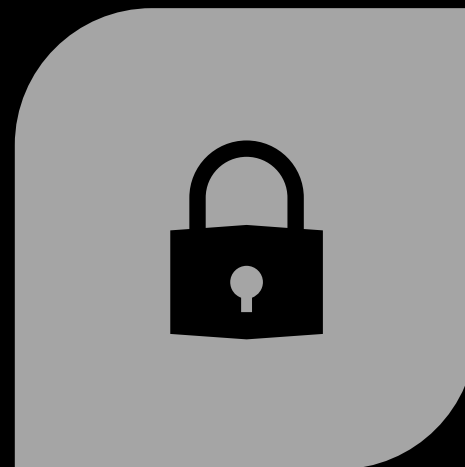
Data
Subjects'
Rights



เปิดเผย / ปกปิด

พรบ.ข้อมูลข่าวสารฯ

พรบ.สาธารณสุข



ความปลอดภัย

พรบ.คุ้มครองข้อมูลส่วนบุคคล

Level 6: Information Management & Security

- Strategy, Process, Policy, Identity, Authentication
- Standards: PCI DSS, ISO27001, SSAE16, ISAE3402

Level 5: Data Regulation

- Data Protection, Competition Law (Data parity), Cybercrime
- Sector-specific regulations: Financial services, Airlines, Healthcare, Insurance

Level 4: Contracting for data

- Actual data
- Liability '*in personam*'

Level 3: IP rights in relation to data

- Copyright, Database right, Confidentiality, Patents, Trademarks

Level 2: Information Architecture

- Data structure, Design, Schemas, Format
- Data model, Data flows through data entities, Attributes and Interrelationships

Level 1: Platform Infrastructure

- Software: OS, Middleware Business Intelligence & Analytics Applications
- Equipment: Processing Storage, Connectivity

Legal Framework for Big Data



EU General Data
Protection Regulation
25 May 2018

Section 19	Conditions for consent	Section 36	Right to Rectification - Record of Refusal
Section 20	Conditions for child's consent	Section 37(1)	Duties of the Controller - Appropriate Security
Section 21	Purpose Limitation	Section 37(2)	Duties of the Controller - Prevention of Unauthorized Access
Section 22	Data Minimization	Section 37(3)	Duties of the Controller - Data Retention
Section 23	Right to be informed	Section 37(4)	Duties of the Controller - Data Breach Notification
Section 24	Lawfulness of processing - Collection	Section 37(5)	Duties of the Controller - Designation of a Representative
Section 25	Indirect Collection	Section 38	Duties of the Controller - Exemption of Designation
Section 26	Processing of special categories	Section 39	Duties of the Controller - Record of Processing Activities
Section 27	Lawfulness of processing - Use and Disclosure	Section 40.1(1)	Duties of the Processor - Processing under Instructions
Section 28	Cross-border Data Transfer - Adequacy Decision	Section 40.1(2)	Duties of the Processor - Appropriate Security
Section 29	Cross-border Data Transfer - Appropriate Safeguards	Section 40.1(3)	Duties of the Processor - Record of Processing Activities
Section 30	Right of Access	Section 40.2	Duties of the Processor - Processing without Instructions
Section 31	Right to Data Portability	Section 40.3	Duties of the Processor - Data Processing Agreement
Section 32	Right to Object	Section 40.4	Duties of the Processor - Exemption of Record of Processing Activities
Section 33	Right to Erasure	Section 41	Data Protection Officer - Designation
Section 34	Right to Restrict Processing	Section 42	Data Protection Officer - Duties
Section 35	Right to Rectification		

Customer Touchpoints



Customers



Mobile Apps



Web browsing



Communications



Meeting & Visit



Agreements



Move-in



Retention

LETTER FROM SATYA NADELLA



Team,

Each one of us shapes our culture through our words and actions. We strive to build a diverse and inclusive culture that embraces learning and fosters trust—a culture where every employee can do their best work.

Making good decisions and ethical choices in our work builds trust in each other and with our customers and partners. You should never compromise your personal integrity or the company's reputation and trust in exchange for any short-term gain.

We are more likely to make ethical choices when integrity, honesty, and compliance guide our decision-making. We should always be transparent about our motives, learn from our mistakes, and ask for help when faced with a difficult situation. I expect leaders and managers to foster a culture where employees feel free to ask questions and raise concerns when something doesn't seem right.

Our Standards of Business Conduct emphasizes the role that each of us plays in building trust, and the approach you should take in making decisions. When we apply these principles in our daily work, we can move forward with confidence in our ability to make good decisions that build trust and empower our customers and partners to achieve more.

Thank you very much.

Satya Nadella



INTENTS

STANDARDS OF BUSINESS CONDUCT	
LETTER FROM SATYA NADELLA	1
OUR CULTURE AND VALUES	6
HOW TO USE THE STANDARDS TO MAKE GOOD DECISIONS	8
SPEAKING UP	13
TRUST WITH OUR CUSTOMERS	19
Honor Privacy	20
Don't Make Improper Payments	22
Compete Fairly	23
TRUST WITH GOVERNMENTS AND COMMUNITIES	25
Respect Laws Around the World	26
Design Accessible Products and Services	29
Respect and Promote Human Rights	30
TRUST WITH EACH OTHER	32
Foster Diversity and Inclusion	34
Contribute to a Safe and Productive Workplace	36
TRUST WITH OUR INVESTORS AND THE PUBLIC	40
Don't Trade on Inside Information	42
Keep Accurate Records and Contracts	43
Communicate Accurately to the Public	44
Safeguard Microsoft's Resources	46
Protect Confidential Information & Intellectual Property	47
TRUST WITH OUR REPRESENTATIVES	48
Use Trustworthy Representatives	50
Treat Gifts, Hospitality, & Travel Responsibly	53
Choose Suppliers with Integrity	54
UPHOLDING THESE STANDARDS	56



The SUPREME COURT

[> Home](#) [> The Supreme Court](#) [Privacy policy](#)

[Decided
cases](#)

[Court
procedures](#)

[Visiting The
Court](#)

[About The
Supreme Court](#)

[Latest
news](#)

[Current
cases](#)

[> Terms and conditions](#)

[> Site map](#)

[> Privacy notice](#)

[> RSS feeds](#)

[> Twitter policy](#)

[> Lost property policy](#)

Privacy notice

Introduction

The Supreme Court respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data when we are performing our necessary functions, when you contact us, or when you visit our website (regardless of where you visit it from) and tell you about your privacy rights and how the law protects you.

Purpose of this privacy notice

This privacy notice aims to give you information on how The Supreme Court collects and processes your personal data through your interactions with us. This includes visitors to this website as well as Court users, job applicants and visitors to us in person.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended

we have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the DPO using the details set out below.

Contact details

Data Protection Officer:

Paul Sandles

Email address:

dataprotection@supremecourt.uk

Postal address:

Data Protection Officer
The Supreme Court of the United Kingdom
Parliament Square
London
SW1P 3DB

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (<https://ico.org.uk>). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth, gender, as well as images recorded on CCTV.
- **Contact Data** includes billing address, delivery address, email address and telephone numbers.
- **Financial and Transaction Data** includes bank account and payment card details as well as details about payments to and from you.
- **Technical and Usage Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website. It includes information about how you use our website.
- **Communications Data** includes your communications preferences in receiving updates from us.

Our services are not designed for, or intentionally targeted at, children 13 years of age or younger. We do not intentionally collect or maintain data about anyone under the age of 13.

How is your personal data collected?

We use different methods to collect data from and about you including through:

Direct interactions. You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- complete Court forms or supply other documents in relation to Court proceedings;
- request communication updates to be sent to you;
- enter a competition or survey; or
- give us some feedback or contact us for another specific purpose.

Automated technologies or interactions. As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, and other similar technologies.

Visitors to the building should also note that CCTV footage is used throughout the building, including within the court rooms.

Third parties or publicly available sources. We may receive personal data about you from various third parties and public sources.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To produce an accurate record for the purposes of Court proceedings	(a) Identity (b) Contact (c) Financial and Transaction	(a) Performance of a public task (b) Necessary for our legitimate interests (to recover debts due to us)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our service, provision of administration and IT services, network security and to prevent fraud) (b) Necessary to comply with a legal obligation
Use of CCTV throughout the building and in its immediate vicinity as well as broadcast filming in Court	(a) Identity	(a) Performance of a public task (to preserve records of court proceedings) (b) Necessary for our legitimate interests (to ensure public safety)
To use data analytics to improve our website and our services	(a) Technical and Usage	Necessary for our legitimate interests (to keep our website updated and relevant, and to develop our services)
Distribution of information regarding Court activities via email	(a) Communications	(a) Performance of a public task (b) Necessary for our legitimate interests (for the purposes of ensuring timely and accurate reporting of Court proceedings)
To enable us to process job applications for vacancies within the Court's administrative staff	(a) Identity (b) Contact	(a) Performance of a public task (b) Necessary to comply with a legal obligation

Compliance

[HOW WE USE YOUR DATA](#)[SUBMIT AN INFORMATION REQUEST](#)[POLICIES & STATEMENTS](#)[STAFF GUIDANCE ON DATA PROTECTION](#)[ABOUT](#)[Home](#) > [Policies & statements](#) > [Data protection policy](#)

Data protection policy

This policy was approved by Council on 14 May 2018, to take effect on 25 May 2018

Read the University policy on data protection below or view it as a PDF by clicking this link:

[University Policy on Data Protection.pdf](#)

[1. Purpose and scope](#)[2. Background](#)[3. Principles](#)[4. Aims and commitments](#)[5. Roles and responsibilities](#)[6. Breaches of data privacy legislation](#)[7. Compliance](#)[8. Further information](#)[9. Review and development](#)[10. Related policies](#)

Email: [data](#)

Tel: (01865



Council

Executive Responsibility
General Purposed
Committee



Data Protection Officer (DPO)

Internal Compliance
Information Compliance
Team



Heads of Department (or equivalent)

Department Compliance



Other processing for a University purpose

Individual Responsibility



คำสั่งจุฬาลงกรณ์มหาวิทยาลัย
ที่ ๔๕๖๑๕/๒๕๖๓
เรื่อง แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

เพื่อเป็นการเตรียมความพร้อมในการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และ
ดำเนินการตามข้อบังคับจุฬาลงกรณ์มหาวิทยาลัย ว่าด้วย การคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓

อาศัยอำนาจตามความในมาตรา ๒๗ และมาตรา ๓๒ แห่งพระราชบัญญัติจุฬาลงกรณ์มหาวิทยาลัย พ.ศ. ๒๕๕๑
จึงเห็นสมควรแต่งตั้ง ศาสตราจารย์ ดร.บุญไชย สถิตมั่นในธรรม ข้าราชการพลเรือนในสถาบันอุดมศึกษา สังกัดคณะวิศวกรรมศาสตร์
จุฬาลงกรณ์มหาวิทยาลัย เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัย โดยให้มีอำนาจหน้าที่ดังนี้

(๑) ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้งผู้ปฏิบัติงานในมหาวิทยาลัย
ลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครอง
ข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๒) ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้งผู้ปฏิบัติงาน
ในมหาวิทยาลัย ลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เกี่ยวกับการเก็บ รวบรวม ใช้ หรือ
เปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๓) ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีปัญหา
เกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้ง
ผู้ปฏิบัติงานในมหาวิทยาลัย ลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในการปฏิบัติตาม
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๔) เตรียมความพร้อมเพื่อรองรับการดำเนินการตามข้อบังคับจุฬาลงกรณ์มหาวิทยาลัย ว่าด้วย การคุ้มครองข้อมูล
ส่วนบุคคล พ.ศ. ๒๕๖๓

(๕) เสนอแนะเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลต่ออธิการบดี รวมทั้งเสนอแต่งตั้งคณะกรรมการหรือ
คณะทำงานตามขอบเขตอำนาจหน้าที่

(๖) ปฏิบัติหน้าที่หรือภารกิจอื่นที่ไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

ทั้งนี้ ให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่
คุ้มครองข้อมูลส่วนบุคคลโดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอรวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการ
ปฏิบัติหน้าที่ข้างต้น

สั่ง ณ วันที่ ๒๔ กรกฎาคม พ.ศ. ๒๕๖๓

(ศาสตราจารย์ ดร.บัณฑิต เอื้ออาภรณ์)
อธิการบดี



Chula
Chulalongkorn University

Data Protection Laws set out the obligations HCA UK has to you for the processing of your Personal Data. When we use or disclose your personal data we will comply with these Laws.

Your Personal Data is data which by itself or with other data available to HCA International Limited (HCA UK) can be used to identify you as an individual. HCA UK is the Data Controller. This Privacy Notice sets out how HCA will use your personal data. You can contact our Data Protection Officer (DPO) at 242 Marylebone Rd, Marylebone, London NW1 6JL, or at DPO@hcahealthcare.co.uk if you have any questions.

[Home](#) ▸ [Privacy Notice](#)

PRIVACY NOTICE

In this page:

[Information about you and how we use it](#)
[Using and sharing information about you and your care](#)
[Legal aspects](#)
[Your information rights](#)
[Accessing your health record \(a subject access request\)](#)
[OUH IM&T Services - PACS/RIS Team](#)
[Oxford University Hospitals NHS Foundation Trust Membership Scheme](#)
[General enquiries](#)
[Data Protection Officer](#)

Information about you and how we use it

When you come into hospital, information about you, your illness and its treatment is recorded - on paper and/or on computers - to help us care for you. This information is part of your health record and will be kept in case we need to see you again.

Our clinical teams looking after you may share your personal health information with each other. These teams include doctors, nurses, therapists, support staff and students. All NHS staff are bound by law and a strict code of confidentiality, and are monitored by the Trust's **Caldicott Guardian**, a senior clinician who is responsible for making sure your confidential information is respected. Your information is very important to us, and we have strict controls in place to protect it.

PRIVACY NOTICE

[How we use your information - legal aspects](#)

[Who we share your information with](#)

[Foundation Trust Membership](#)

[Staff Privacy Notice](#)

[← Home](#)

**Help us
improve this
website**

[Take our short survey.](#)

Roles of DPO

GDPR, Article 39

PDPA, Section 41



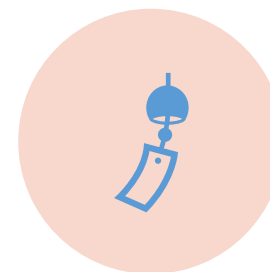
Cooperation With Data Protection
Supervisory Authority And Other
Stakeholders



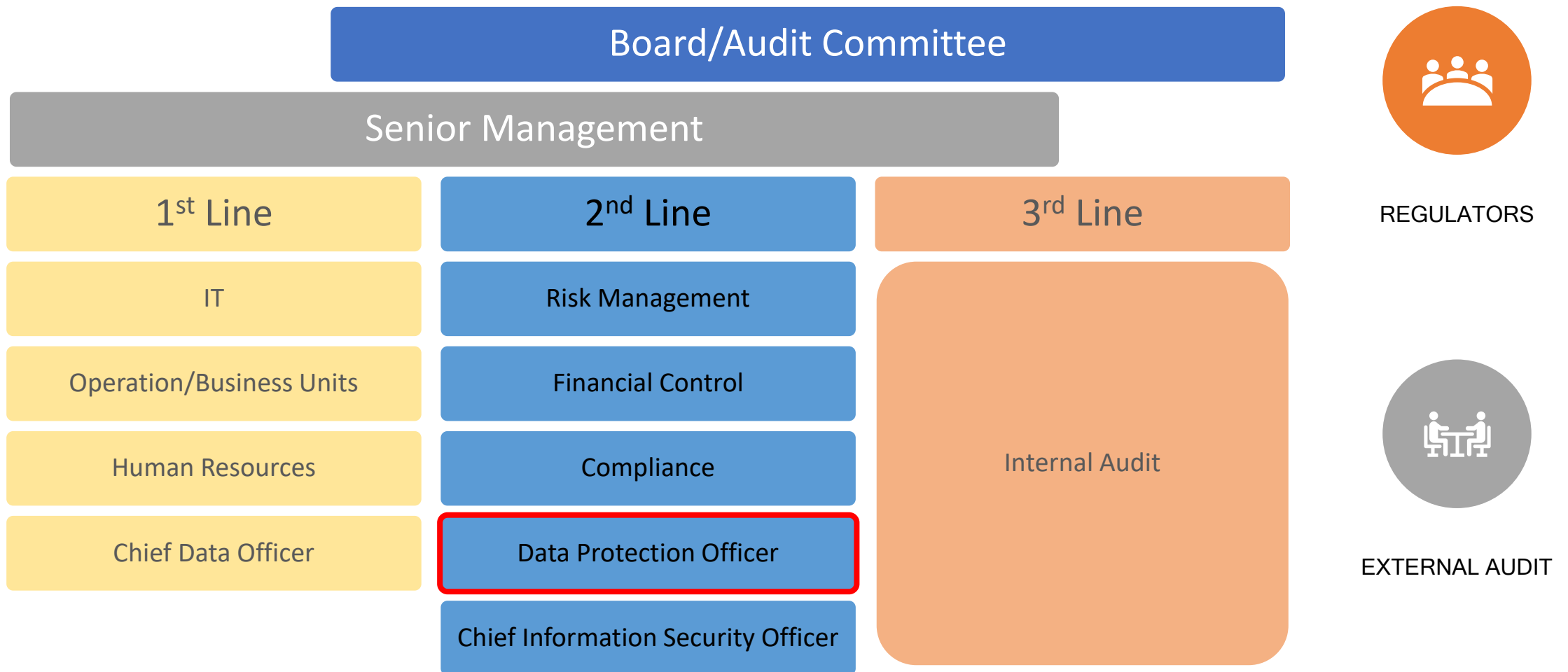
Advisory Activities



Monitoring Compliance With The
Data Protection Framework And
Internal Regulations



รักษาความลับ



DPO as 2nd Line of Defence Model

หน้าที่ในการแจ้งการ
ประมวลผลข้อมูลส่วนบุคคล
(Privacy Policy and
Notices)



Purposes and Lawful Bases



Conditions of Services



Types of Data and Retention Periods



Transfer of Data



Contact Details



Data Subject Rights

หน้าที่ในการเก็บบันทึกการ
ประมวลผลข้อมูลส่วนบุคคล
(Record of Processing Activities)



Types of Data



Purposes



Controller Details



Retention Periods



Right and Process to Access



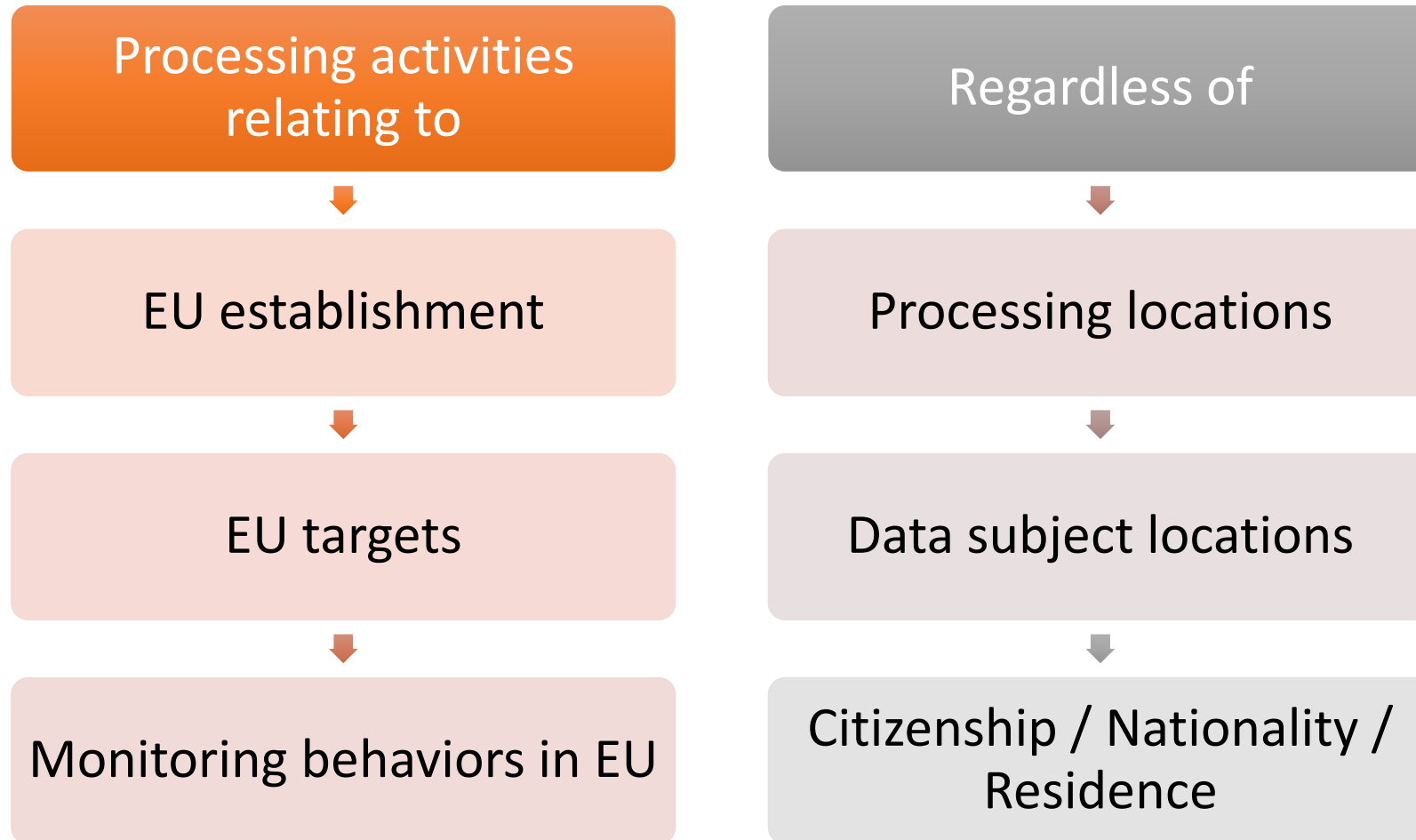
Lawful Bases



Reasons to Reject



Security Measures



GDPR's extraterritorial scope (Art.3)

The Long Arm of the GDPR



Territorial Scope (Art.3)



Data Transfers (Art.44)



**Adequacy Decisions
(Art.45)**



**Appropriate Safeguards
(Art.46)**

Legal instrument between
public authorities

Binding Corporate Rules (Art.47)

Standard data protection
clauses

An approved code of conduct

An approved certification
mechanism

European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows

The key elements of the adequacy decision

- **A set of rules (Supplementary Rules) that will bridge several differences between the two data protection systems.** These additional safeguards will strengthen, for example, the protection of sensitive data, the exercise of individual rights and the conditions under which EU data can be further transferred from Japan to another third country. These Supplementary Rules will be binding on Japanese companies importing data from the EU and enforceable by the Japanese independent data protection authority (PPC) and courts.
- The Japanese government also gave assurances to the Commission regarding safeguards concerning the access of Japanese public authorities **for criminal law enforcement and national security purposes**, ensuring that any such use of personal data would be limited to what is necessary and proportionate and subject to independent oversight and effective redress mechanisms.
- **A complaint-handling mechanism** to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities. This new mechanism will be administered and supervised by the Japanese independent data protection authority.

Article 29 Working Party - Adequacy Referential

Concepts: Personal Data, Processing, Data Controller, Data Processor, Recipient, Sensitive Data

Grounds for lawful and fair processing for legitimate purposes

The purpose limitation principle

The data quality and proportionality principle

Data retention principle

The security and confidentiality principle

The transparency principle (right to be informed)

The right of access, rectification, erasure and objection

Restrictions on onward transfers

Special categories of data

Direct marketing

Automated decision making and profiling

Competent Independent Supervisory Authority

The data protection system must ensure a good level of compliance

Accountability

The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms

It is all about standards!



GDPR (2018)



ISO/IEC 27701:2019



NIST PRIVACY
FRAMEWORK 1.0
(2020)



CIPP/A

PRC Cybersecurity Law (2017)

Guidelines on Multi-Level Protection Scheme for Information Systems
(MLPS 2.0 Standards 2019)

GB/T 22239 – 2019 Information Security Technology – Baseline for Multi-level Protection Scheme

GB/T 25070 – 2019 Information Security Technology – Technical Requirements of Security Design for Multi-level Protection Scheme

GB/T 28448 – 2019 Information Security Technology – Evaluation Requirements for Multi-level Protection Scheme.

Decision on Strengthening Online Information Protection, effective from (Decision on December 28, 2012)

National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services (2013 Guideline)

National Standard of Information Security Technology – Personal Information Security Specification, (PIS Specification 2018)

Personal Information Outbound Transfer Security Assessment Measures (Draft for Comment), June 2019

Guideline for Internet Personal Information Security Protection (2018)



ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม พ.ศ.2549



ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553



เอกสารแนบ 6 ประกาศธนาคารแห่งประเทศไทยที่ สกส.1/2561 เรื่องการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม (market conduct) โดยมีสาระสำคัญเน้นเรื่องการไม่เปิดเผยข้อมูลลูกค้าและการขอความยินยอม



พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

Situation



Thailand is to start from scratch.



Cross-Border Data
Transfer Issues

US – EU Privacy Shield

Guidelines 1/2018 on certification, adopted on 25 May 2018

APEC-CBPRs (Cross-Border Privacy Rules System)

EU Adequacy Decision



DPA is adopting GDPR standards.



Data protection are to be certified and
standardized.

ISO/IEC 27001

ISO/IEC 29100

Etc.

บทเสริมการคุ้มครอง ข้อมูลส่วนบุคคล

มาตรา 3 ในกรณีที่มีกฎหมายว่าด้วยการใด
บัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด
กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตาม
บทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(1) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือ
เปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับสิทธิของ
เจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง
ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการ
เพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการ
นั้นหรือไม่ก็ตาม

...

การดำเนินการที่ได้รับยกเว้น (มาตรา 4)



เพื่อประโยชน์ส่วนตนหรือเพื่อ
กิจกรรมในครอบครัวของบุคคลนั้น
เท่านั้น



หน้าที่ในการรักษาความมั่นคงของ
รัฐซึ่งรวมถึงความมั่นคงทางการ
คลังของรัฐ หรือการรักษาความ
ปลอดภัยของประชาชน รวมทั้ง
หน้าที่เกี่ยวกับการป้องกันและ
ปราบปรามการฟอกเงิน นิติ
วิทยาศาสตร์ หรือการรักษาความ
มั่นคงปลอดภัยไซเบอร์



เพื่อกิจการสื่อมวลชน งาน
ศิลปกรรม หรืองานวรรณกรรมอัน
เป็นไปตามจริยธรรมแห่งการ
ประกอบวิชาชีพหรือเป็นประโยชน์
สาธารณะเท่านั้น



การพิจารณาตามหน้าที่และอำนาจ
ของสภาผู้แทนราษฎร วุฒิสภา
รัฐสภา หรือคณะกรรมการ



การพิจารณาพิพากษาคดีของศาล
และการดำเนินงานของเจ้าหน้าที่ใน
กระบวนการพิจารณาคดี การ
บังคับคดี และการวางทรัพย์
รวมทั้งการดำเนินงานตาม
กระบวนการยุติธรรมทางอาญา



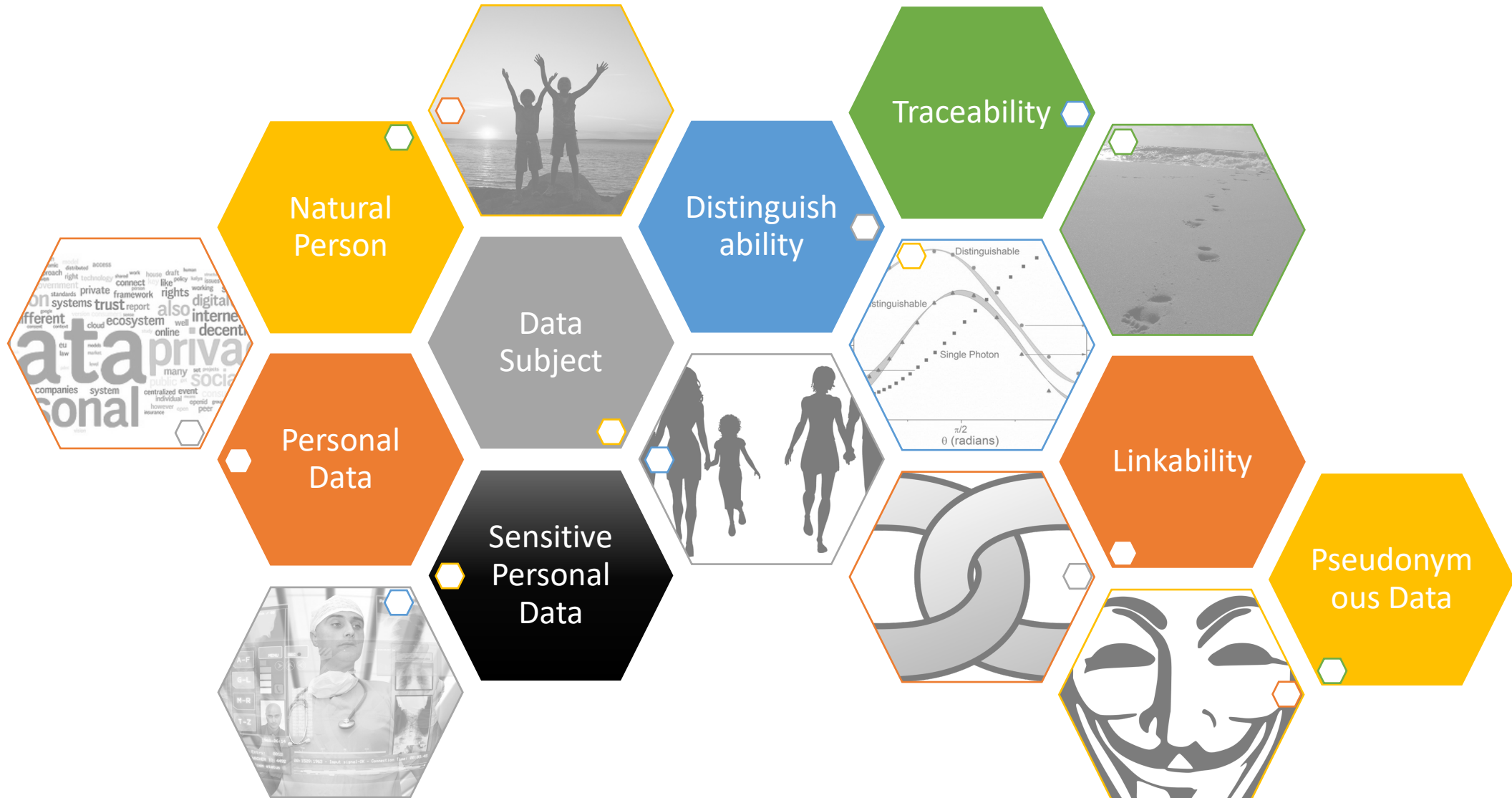
การดำเนินการกับข้อมูลของบริษัท
ข้อมูลเครดิตและสมาชิกตาม
กฎหมายว่าด้วยการประกอบธุรกิจ
ข้อมูลเครดิต

มาตรา 4 วรรค 3



ผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง
...ต้องจัดให้มีการรักษาความมั่นคง
ปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไป
ตามมาตรฐานด้วย

Scope of Personal Data



พระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ.2562

มาตรา 6

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

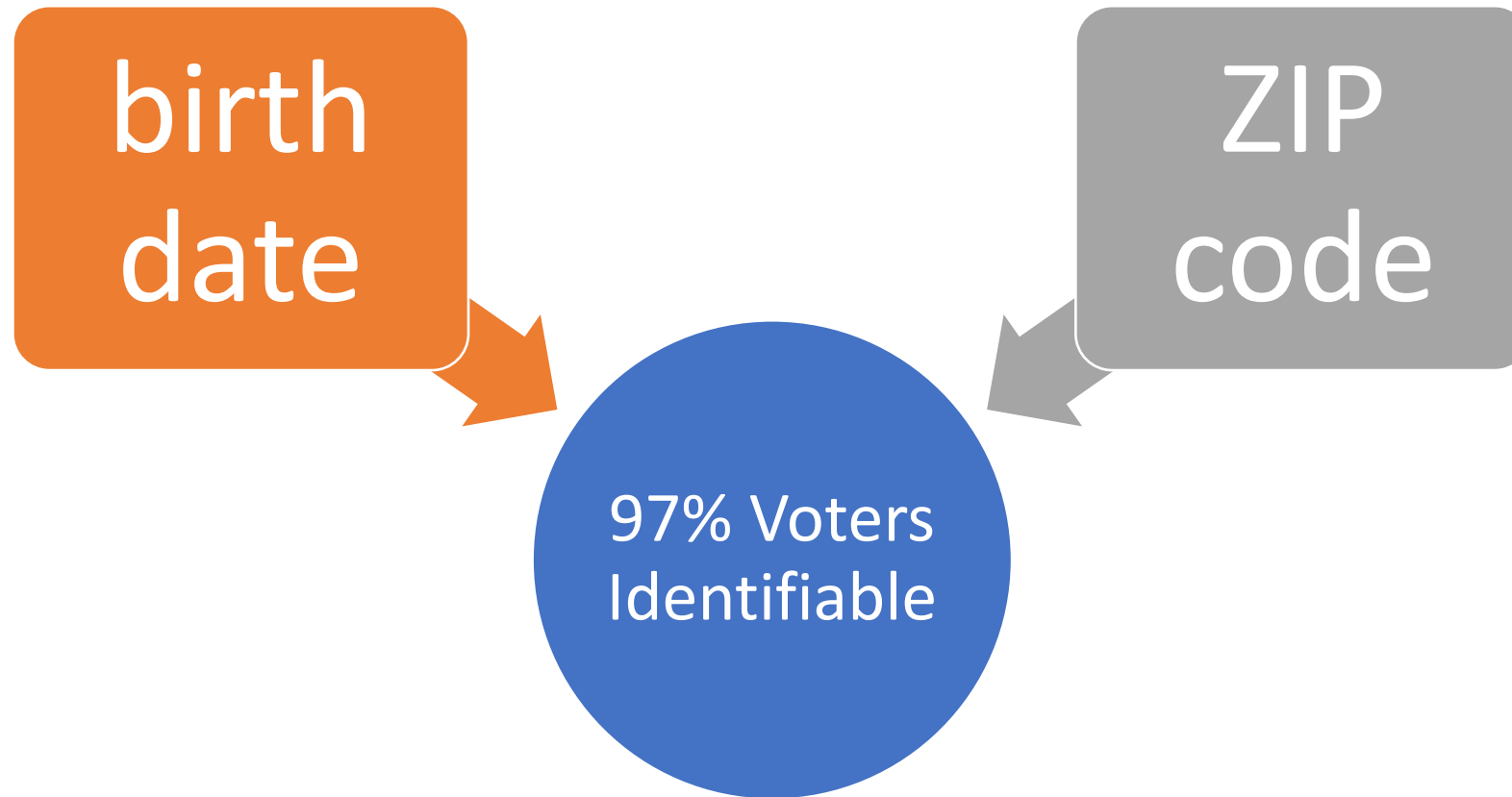
“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“บุคคล” หมายความว่า บุคคลธรรมดา

...

'personal data' means any information relating to an identified or identifiable natural person ('data subject')



Latanya Sweeney, *Computational disclosure control : a primer on data privacy protection*, 2001,
<http://dspace.mit.edu/handle/1721.1/8589>

Data Risk Level



Low

Limited adverse effect



Moderate

Serious adverse effect



High

Severe or catastrophic adverse effect

Data Classification



DATA POLICY



DATA
DISCOVERY



DATA
PROLIFERATION



DATA RISK
LEVEL



DATA
PROTECTION

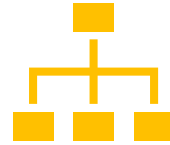
Data Discovery



Assets



Processing
Activities



Entities



Vendors

Actors and Roles



DATA SUBJECTS



DATA
CONTROLLERS



DATA
PROCESSORS



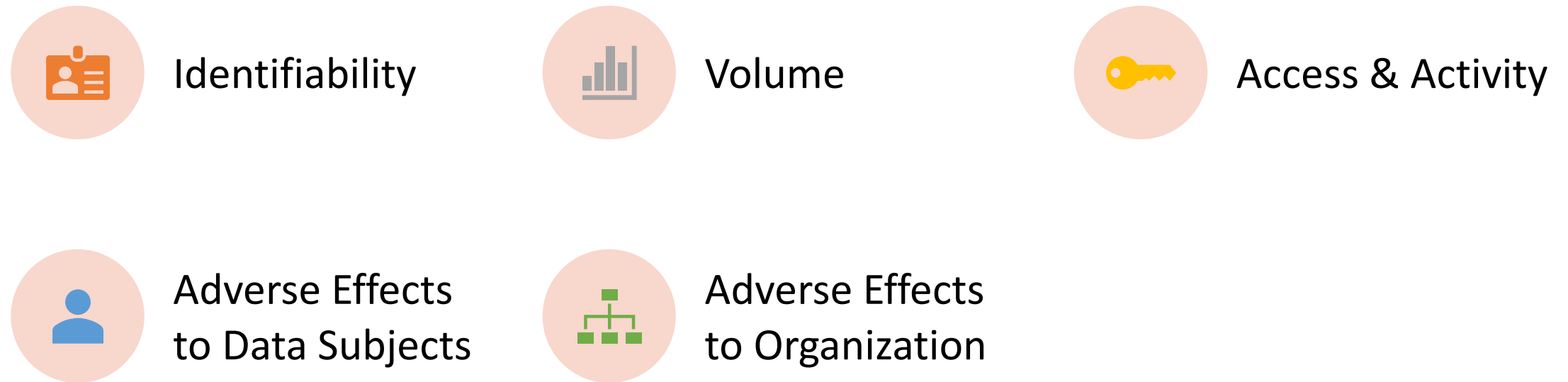
THIRD PARTIES

	Data Subject	Controller	Processor	Third Parties
A.	Provider	Recipient		
B.		Provider	Recipient	
C.	Provider		Recipient	
D.	Recipient	Provider		
E.	Recipient		Provider	
F.		Recipient	Provider	
G.		Provider		Recipient
H.			Provider	Recipient

Actors, Roles and Interactions



Data Risk Level



Lawful Basis for Processing (GDPR, Art.6)

ฐานการประมวลผลข้อมูลส่วนบุคคล
(มาตรา 24)



Contract



Consent



Vital Interest

(To protect health and life of data subjects and third persons)



Legal Obligations



Public Task

(Usually cases of public authorities)



Legitimate Interest

(Must be balanced between controller's interest and data subject fundamental rights)

Contract & Consent



Contract

Necessary for contract

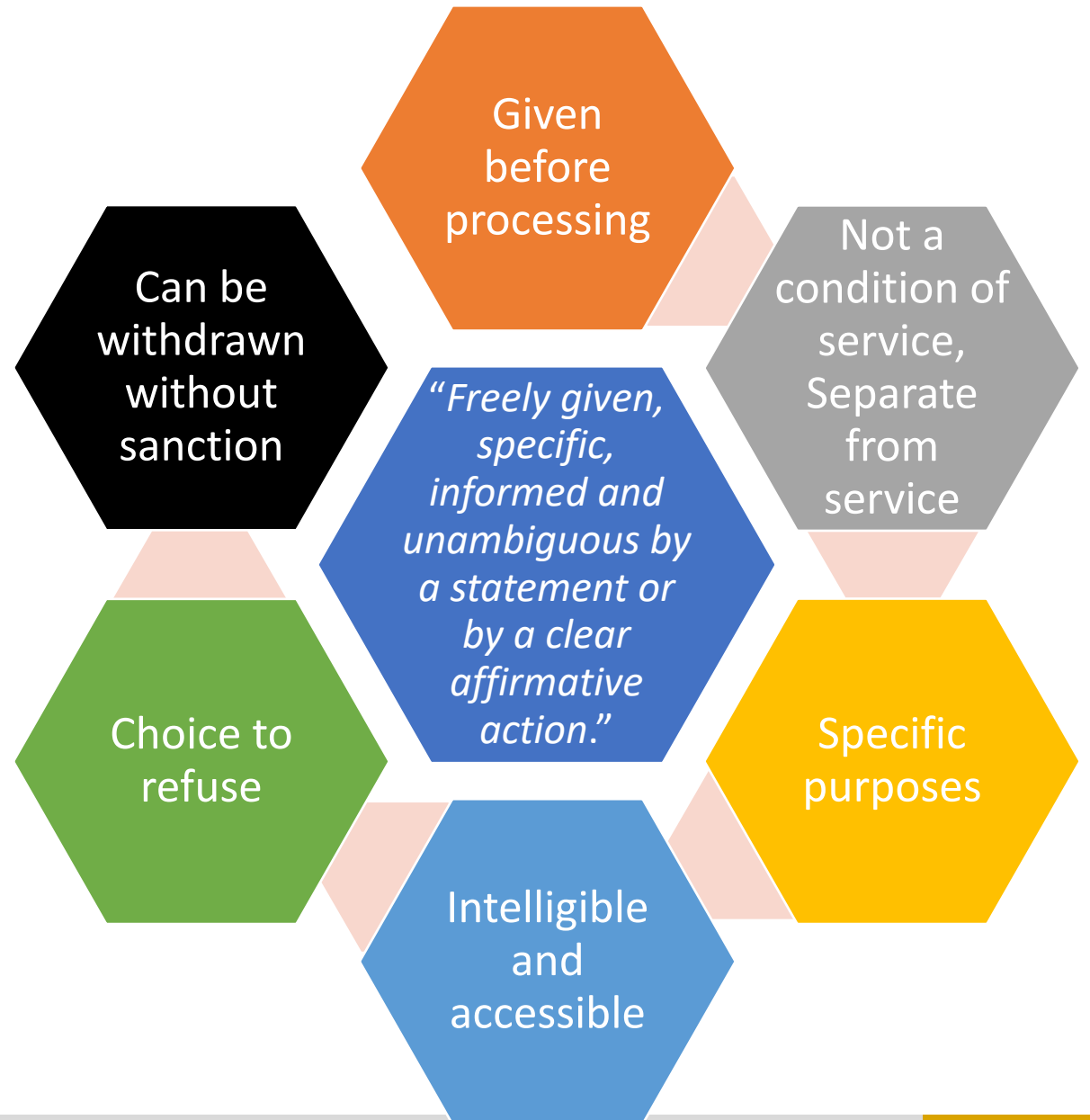



Consent

Choice of data subject

GDPR Conditions for Consent (Art.4)

เงื่อนไขของความยินยอม
(มาตรา 19)





ฐานการประมวลผลโดยชอบ
ด้วยกฎหมาย (มาตรา 24)

(Lawful Basis for
Processing)

Consent (วรรค 1)

Research (1)

Vital Interest (2)

Contract (3)

Public Task (4)

Legitimate Interest (5)

Legal Obligations (6)

ฐานการประมวลผลโดยชอบ ด้วยกฎหมาย (มาตรา 24) (Lawful Basis for Processing)

“ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(๔) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจอรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๕) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(๖) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล”

ฐานการประมวลผลโดยชอบด้วยกฎหมายสำหรับข้อมูลอ่อนไหว (มาตรา 26) (Sensitive Personal Data)



Explicit Consent (วรรค 1)



Vital Interest (1)



Social Protection & Non-profit (2)



Manifestly made public (3)



Legal Claims (4)



Preventive or Occupational Medicine (5)(ก)



Public Health (5)(ข)



Health or Social Care Systems (5)(ค)



Archiving, Scientific or Historical Research (5)(ง)



Substantial Public Interest (5)(จ)

Consent Forms



CONTRACT



CONSENT



SENSITIVE DATA

การขอความยินยอม (Consent)

มาตรา 19 ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

...

การขอความยินยอม (Consent)

...

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบตามที่กำหนดไว้ในหมวดนี้

...

Consent Forms

Standard consent forms and forms for adults who are unable to consent for themselves are available for download.

[Consent Form 1 – Patient agreement to investigation, treatment or procedure](#)

[Consent Form 2 – Parental agreement to investigation, treatment or procedure for a child or young person](#)

[Consent Form 3 – Patient Parental agreement to investigation, treatment or procedure where consciousness not impaired](#)

[Clinical Photography/Video Consent Form](#)

Consent for use and sharing of information

Consent to treatment implies consent to make and keep appropriate records. It also implies consent to share the relevant personal confidential data with any regulated health or social care professional who has a legitimate relationship with the patient for the purposes of direct care. ...

A legitimate relationship exists when any of the following criteria are met:

- The patient or client presents themselves to the professional for the purpose of their care.
- The patient or client agrees to a referral from one registered and regulated health or social care professional to another
- The patient or client is invited by a professional to take part in a screening or immunisation programme for which they are eligible and accept
- The patient or client presents to a health or social care professional in an emergency situation where consent is not possible
- The relationship is part of a legal duty, e.g. contact tracing in public health
- The patient is told of a proposed communication and does not object

The implied consent to share relevant information does not mean the whole record unless the whole record is relevant in a particular case.

18 HIPAA PHI (Protected Health Information)

- Names
- Dates, except years
- Telephone numbers
- Geographic data
- FAX numbers
- Social Security numbers
- Email addresses
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Web URLs
- Device identifiers and serial numbers
- Internet protocol addresses
- Full face photos and comparable images
- Biometric identifiers (i.e. retinal scan, fingerprints)
- Any unique identifying number or code

Public Tasks



Legitimate Interest Assessment (LIA)



Identify a legitimate interest

purpose
necessary to meet the purposes
Legal basis



Necessity test

Important?
No other way?



Balancing test

Expectation of others
Value-added?
Negative impact?



Microsoft Privacy Statement

Last Updated: March 2019 [What's new?](#)

[Expand All](#)

[Print](#)

Your privacy is important to us. This privacy statement explains the personal data Microsoft processes, how Microsoft processes it, and for what purposes.

Microsoft offers a wide range of products, including server products used to help operate enterprises worldwide, devices you use in your home, software that students use at school, and services developers use to create and host what's next. References to Microsoft products in this statement include Microsoft services, websites, apps, software, servers, and devices.

Please read the product-specific details in this privacy statement, which provide additional relevant information. This statement applies to the interactions Microsoft has with you and the Microsoft products listed below, as well as other Microsoft products that display this statement.

Personal data we collect

How we use personal data

Reasons we share personal data

How to access and control your personal data

Cookies and similar technologies

Products provided by your organization—notice to end users

Microsoft account

Other important privacy information [v](#)

Product-specific details:

Enterprise and developer products [v](#)

Productivity and communications products [v](#)

Search and artificial intelligence [v](#)

Windows [v](#)

Entertainment and related services [v](#)

Microsoft Health services [v](#)

Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products. You provide some of this data directly, and we get some of it by collecting data about your interactions, use, and experiences with our products. The data we collect depends on the context of your interactions with Microsoft and the choices you make, including your privacy settings and the products and features you use. We also obtain data about you from third parties.

If you represent an organization, such as a business or school, that utilizes Enterprise and Developer Products from Microsoft, please see the [Enterprise and developer products](#) section of this privacy statement to learn how we process your data.

You have choices when it comes to the technology you use and the data you share. When we ask you to provide personal data, you can decline. Many of our products require some personal data to provide you with a service. If you choose not to provide data necessary to provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this relates to an existing product you're using, we may have to suspend or cancel it. We will notify you if this is the case at the time. Where providing the data is optional, and you choose not to share personal data, features like personalization that use such data will not work for you.

[Learn more](#)

[Top of page](#) [↑](#)



Create an account

If you already sign in to a Windows PC, tablet, or phone, Xbox Live, Outlook.com, or OneDrive, use that email address to [sign in](#). Otherwise, create a new Outlook.com email address.

First name

Last name

User name

 @outlook.com 

Password

8-character minimum; case sensitive

Reenter password

Country/region

Birthdate

Month 

Day 

Year 

Gender

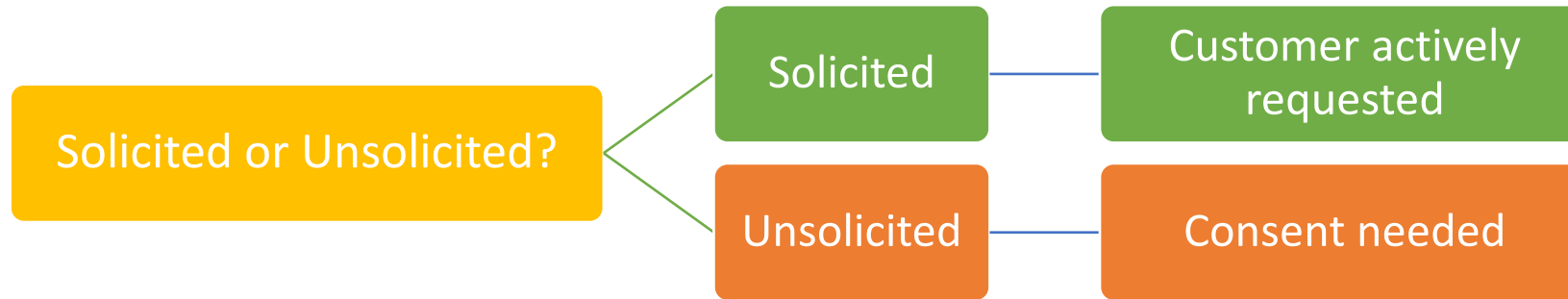
Help us protect your info

Your phone number helps us keep your account secure.

Your date of birth helps us provide you with things like age-appropriate settings. We won't display it without your permission.

ยินดีต้อนรับ!
Welcome!

- คุณทราบโปรโมชั่นนี้จากช่องทางใด
- ยืนยันอีเมลอีกครั้ง | Confirm your email address
- ชื่อเล่น | Nickname
- ชื่อจริง | First name
- นามสกุล | Last name
- คุณใส่เสื้อยืดไซส์อะไร | What size t-shirt do you wear?
- เพศ | Gender
- สถานภาพสมรส | What's your marital status
- จังหวัดที่อาศัยอยู่ในปัจจุบัน | Which province do you currently reside in?
- ปีเกิด (ค.ศ.) | Birth year
- เบอร์โทรศัพท์มือถือ | Mobile phone
- ชอบสีอะไร | What is your favorite color?
- LINE ID (เพื่อรับอัปเดตล่าสุด | For latest updates)
- หนังสือหรือออนไลน์คอนเทนต์ที่ดูล่าสุดคืออะไร | What's the latest book or online content you read / watched?
- คุณทำอาชีพอะไร | What is your affiliation?



Newsletters and direct marketing to the customer	• Consent
Service notifications	• Legitimate interest
Profiled direct marketing	• Consent
Providing similar products or services in the context of a customer relationship	• Legitimate interest
Social Network Request	• TOS
Lead	• Consent to share and use

ได้รับความยินยอมจากผู้รับ (Consent)

ระบุวิธีการบอกเลิกไม่รับข้อมูล (Unsubscribe)

- วิธีการทางอิเล็กทรอนิกส์
- ระบุ URL หรือแบบฟอร์ม
- ห้ามเรียกเงินหรือข้อมูล

มีกระบวนการยกเลิกภายใน 7 วัน

การสื่อสารเชิงพาณิชย์ที่มีลักษณะต่อไปนี้ไม่ถือเป็น SPAM

Data Policy

This Policy describes the information we process to support Facebook, Instagram, Messenger and other products and features offered by Facebook ([Facebook Products](#) or [Products](#)). You can find additional tools and information in the [Facebook settings](#) and [Instagram settings](#).

II. How do we use this information?

We use the information that we have (subject to choices you make) as described below, and to provide and support the Facebook Products and related services described in the [Facebook Terms](#) and [Instagram Terms](#). Here's how:

- **Face recognition:** If you have it turned on, we use face recognition technology to recognise you in photos, videos and camera experiences. The face recognition templates that we create may constitute [data with special protections](#) under the laws of your country. Learn more about [how we use face recognition technology](#), or control our use of this technology in [Facebook settings](#). If we introduce face recognition technology to your Instagram experience, we will let you know first, and you will have control over whether we use this technology for you.
- **Ads and other sponsored content:** We use the information we have about you – including information about your interests, actions and connections – to select and personalise ads, offers and other sponsored content that we show you. Learn more about how we [select and personalise ads](#), and your choices over the data we use to select ads and other sponsored content for you in the [Facebook Settings](#) and [Instagram Settings](#).

Sharing with third-party partners

We work with third-party partners who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, which makes it possible to operate our companies and provide free services to people around the world. We don't sell any of your information to anyone and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide. Here are the types of third parties that we share information with:

Partners who use our analytics services.

We provide aggregated statistics and insights that help people and businesses understand how people are engaging with their posts, listings, Pages, videos and other content on and off the Facebook Products. For example, Page admins and Instagram business profiles receive information about the number of people or accounts who viewed, reacted to or commented on their posts, as well as aggregate demographic and other information that helps them understand interactions with their Page or account.

Advertisers.

We provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but we don't share information that personally identifies you (information such as your name or email address that by itself can be used to contact you or identifies who you are) unless you give us permission. For example, we provide general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. We also confirm which Facebook ads led you to make a purchase or take an action with an advertiser.

Measurement partners.

We share information about you with companies that aggregate it to provide analytics and measurement reports to our partners.

Partners offering goods and services in our Products.

When you subscribe to receive premium content, or buy something from a seller in our Products, the content creator or seller can receive your public information and other information that you share with them, as well as the information needed to complete the transaction, including shipping and contact details.

5. Other Important Information

5.1. Security

We implement security safeguards designed to protect your data, such as HTTPS. We regularly monitor our systems for possible vulnerabilities and attacks. However, we cannot warrant the security of any information that you send us. There is no guarantee that data may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards. Please visit our [Safety Center](#) for additional information about safely using our Services, including [two-factor authentication](#).

5.2. Cross-Border Data Transfers

We process data both inside and outside of the United States and rely on legally-provided mechanisms to lawfully transfer data across borders. [Learn more](#). Countries where we process data may have laws which are different, and potentially not as protective, as the laws of your own country.

5.3 Lawful Bases for Processing

We will only collect and process personal data about you where we have lawful bases. Lawful bases include [consent](#) (where you have given consent), contract (where processing is necessary for the performance of a contract with you (e.g. to deliver the LinkedIn Services you have [requested](#))) and “legitimate interests”. [Learn more](#).

Where we rely on your consent to process personal data, you have the right to withdraw or decline your consent at any time and where we rely on legitimate interests, you have the right to object. [Learn More](#). If you have any questions about the lawful bases upon which we collect and use your personal data, please contact our Data Protection Officer [here](#).

5.4. Direct Marketing and Do Not Track Signals

We currently do not share personal data with third parties for their direct marketing purposes without your permission. [Learn more](#) about this and about our response to “do not track” signals.

Linked in

Sign In Join Now

Privacy Policy

To learn more about Privacy at LinkedIn please visit our [Privacy Hub](#).

Effective May 8, 2018

Our Privacy Policy has been updated. Click here to see a [summary of changes](#).

See a [guided tour](#) of the main changes.

Your Privacy Matters

LinkedIn’s mission is to connect the world’s professionals to allow them to be more productive and successful. Central to this mission is our commitment to be transparent about the data we collect about you, how it is used and with whom it is shared.

This Privacy Policy applies when you use our Services (described below). We offer our users choices about the data we collect, use and share as described in this Privacy Policy, [Cookie Policy](#), [Settings](#) and our [Help Center](#).

Table of Contents:

[Introduction](#)
[Data We Collect](#)
[How We Use Your Data](#)
[How We Share Information](#)
[Your Choices & Obligations](#)
[Other Important Information](#)

2.1 Services

We use your data to authorize access to our Services.

Stay Connected

Our Services allow you to stay in touch and up to date with colleagues, partners, clients, and other professional contacts. To do so, you will “connect” with the professionals who you choose, and who also wish to “connect” with you. Subject to your [settings](#), when you connect with other Members, you will be able to search each others’ connections in order to exchange professional opportunities.

We will use data about you (such as your profile, profiles you have viewed or data provided through address book uploads or partner integrations) to help others find your profile, suggest connections for you and others (e.g. Members who share your contacts or job experiences) and enable you to invite others to become a Member and connect with you. You can also opt-in to allow us to use your precise location or proximity to others for certain tasks (e.g. to suggest other [nearby](#) Members for you to connect with, calculate the commute to a new job, or notify your connections that you are at a professional event).

It is your choice whether to invite someone to our Services, send a connection [request](#), or allow another Member to become your connection. When you invite someone to connect with you, your invitation will include your name, photo, network and contact information. We will send invitation reminders to the person you invited. You can [choose](#) whether or not to share your own list of connections with your connections.

Visitors have [choices](#) about how we use their data.

Subscribe to marketing updates

To subscribe to marketing updates from [\[Company Name\]](#) simply fill out the form below.

If you are a student please add your university name and postcode rather than your practice name and postcode.

Please review our [Privacy Policy](#) - which provides information on how we use and process your data -
time if you no longer wish to receive direct marketing for any of the above purposes by e-mailing

[You can also contact us at any](#)

We would like to send you news, offers and information about [\[Company Name\]](#) products and services.

☐ Email

☐ SMS

☐ Telephone

☐ Post

Name *

Email address *

Yes please, keep me up-to-date via email:

- ☒ with the latest news and special offers from
- ☒ genuinely relevant offers and news from our sister brands in the For a list
of our brands please go here <http://www.l>
- ☒ with genuinely relevant offers and promotions from ON behalf of our carefully selected
partners. These emails will always be sent by us.

☒ I consent ☐ I do not consent [To marketing activities](#)

Send you relevant marketing information and carry out market research about our products and services so that you don't miss out on current offers. We normally contact our customers by automated or electronic means including e-mail, phone (e.g. SMS, MMS, fax). We sometimes use other means such as web sites, mobile apps, post or automated calls.

☒ I consent ☐ I do not consent [To profiling activities](#)

Analyse your personal preferences, interests or behaviours so that we can send you customised communications that we think you might like.

☒ I consent ☐ I do not consent
[To the communication of the Data to third parties for their own marketing activities](#)

Share your data with companies in our group and selected partners with whom we work closely so that they can send you relevant offers which might interest you. This could include partners in the automotive, financial, insurance and telecommunication sectors. We normally contact our customers by automated or electronic means including e-mail, phone (e.g. SMS, MMS, fax). We sometimes use other means such as web sites, mobile apps, post or automated calls.

Table 1. Formats and Participation Rates, Experiment 1

Question	Percent Participating
(1) <input type="checkbox"/> Notify me about more health surveys.	48.2
(1) <input type="checkbox"/> Do NOT notify me about more health surveys.	96.3
(3) <input checked="" type="checkbox"/> Notify me about more health surveys.	73.8
(4) <input checked="" type="checkbox"/> Do NOT notify me about more health surveys.	69.2

Table 2. Formats and Participation Rates, Experiment 2

Question	Percent Participating
(1) Do NOT notify me about more health surveys. <input type="radio"/> Yes <input checked="" type="radio"/> No	76.9
(2) Do NOT notify me about more health surveys. <input type="radio"/> Yes <input type="radio"/> No	70.8
(3) Do NOT notify me about more health surveys. <input checked="" type="radio"/> Yes <input type="radio"/> No	44.2
(4) Notify me about more health surveys. <input type="radio"/> Yes <input checked="" type="radio"/> No	59.9
(5) Notify me about more health surveys. <input type="radio"/> Yes <input type="radio"/> No	88.5
(6) Notify me about more health surveys. <input checked="" type="radio"/> Yes <input type="radio"/> No	89.2

Eric J Johnson, Steven Bellman & Gerald L Lohse, *Defaults, Framing and Privacy: Why Opting In-Opting Out*, 13 MARKETING LETTERS 11 (2002).

	Newsletters and direct marketing to the customer	Service notifications	Profiled direct marketing	Providing similar products or services in the context of a customer relationship
Explanation	Regular newsletters or messages (cold emails).	The company receives electronic contact details of the customer in connection with the sale of the product or the provision of the service. Welfare notifications.	Customer behaviour patterns (based on purchase history) are used for targeted messages.	The company receives electronic contact details of the customer in connection with the sale of the product or the provision of the service. Contact information for direct sales of similar products or services to the customer may be used.
Basis of data processing	Consent or clear declaration of will, for example, entering an email on the company's website in the newsletter field or click at tickbox. Must be able to get out of direct marketing. <i>Opt-in and Opt-out</i>	Legitimate interest to send notices- you can rely on legitimate interests for marketing activities. However, in case you have to show that you use people's data proportionately. Meaning, it has a minimal privacy impact, and people would not be likely to object. <i>Opt-out</i>	Consent, e.g. acceptance of personal data processing. The right to object at any time to the processing of personal data. The information shall be provided clearly and separately from any other information. <i>Opt-in and Opt-out</i>	The previous sale of a product or service. During the initial collection of data, and whenever the data is used, the customer has a clear and understandable way to prohibit the use of such contact information in a free and easy way. <i>Opt-out</i>

Recruitment (Online Application)



Contact details



Eligibility to work in
the country



Roles or Position



Level of Education



Username and
password for the
online platform



How you heard
about the Company



Relatives or friends
at the Company



Current Work with
the Company



Work experiences
with the Group

Recruitment (Voluntary Basis)



What type of employment you prefer;



When your available start date is;



Work availability such as weekends, early shift, etc.;



What percentage you are willing to travel;



Whether you are willing to relocate;



Work experience: job title, company, location, description, references from previous employers;



Education: school or university, degree, field of study, overall result (GPA);



Skills;



Websites (<http://>);



Proof of academic title;



Other information about yourself that you provide in a CV;



Whether you would like to be considered for alternative positions (options yes/no);

Recruitment (Job interview)



Functional/technical and personal skills, past experience and performance relevant for the aspired position, career aspirations and plans;



Other information that you provide upon request around your expected employment benefit package, including (base) salary, short term incentive, long term incentive, options, car allowance, expense allowances, pension schemes, healthcare benefits and other employment benefits;



Further information you may decide to disclose, such as interests, your interest in the role or working, how you currently work and collaborate with others, development areas, etc.;



Information as observed by interviewers in any such interview, such as communication style, tone, engagement, personality traits (curiosity, creativity, etc.), team working, collaboration, leadership skills, and management skills to the extent apparent from the interview and relevant to your recruitment.

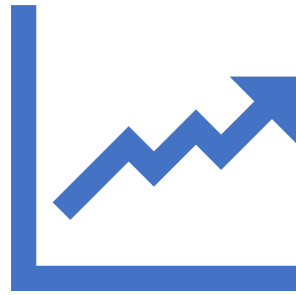


Information as collected by your interview panel and compiled into a Candidate Evaluation Scorecard including technical capabilities, personality traits (curiosity, creativity, etc.), confidence to hire and leadership capability (where relevant) to assist the talent selection process.



Information as collected during an assessment or test as well as a business-related simulation.

Duties & Responsibility



Data Controller



Data Processor

Duties & Responsibility

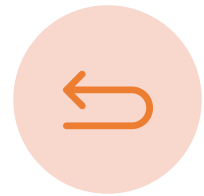


General Duties (D1)

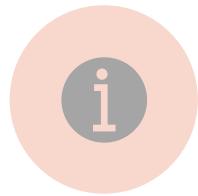


User Requests (D3)

Data Subject Rights



Right to withdraw
consent



Right to be informed



Right of Access



Right to Rectification



Right to Erasure



Right to Restrict
Processing



Right to Data
Portability



Right to Object



Right in Relation to
Automated Decision
Making and Profiling

สิทธิในการถอนความยินยอม (Right to Withdraw Consent)



สามารถถอนความยินยอมได้ง่ายพอๆกับตอนที่ให้ความยินยอม

ถ้าไม่สามารถดำเนินการได้ก็ต้องแจ้งให้ทราบล่วงหน้า



ไม่ได้รับผลกระทบจากการถอนความยินยอม

ไม่เสียค่าใช้จ่าย

ไม่ลดการบริการ



ผู้ควบคุมข้อมูลต้องยุติการประมวลผล

การประมวลผลที่เกิดขึ้นก่อนยอมไม่เสียไป

หากไม่มีฐานการประมวลผลเพื่อเก็บข้อมูลต่อไป ก็ควรต้องลบข้อมูลนั้น



ในกรณีที่ประสงค์จะใช้ข้อมูลต่อโดยเปลี่ยนฐานการประมวลผลต้องแจ้งให้เจ้าของข้อมูลทราบ

สิทธิในการได้รับแจ้งข้อมูล (Right to be Informed)



ชื่อและที่ติดต่อของผู้ควบคุมข้อมูล



ชื่อและที่ติดต่อของ DPO



วัตถุประสงค์และฐานการประมวลผล



ผู้ใช้งานประโยชน์โดยชอบด้วยกฎหมาย



ข้อมูลอ่อนไหวที่ใช้



ผู้รับข้อมูลส่วนบุคคล



รายละเอียดของประเทศที่ส่งข้อมูลรวมถึงมาตรการที่ใช้



ระยะเวลาในการจัดเก็บข้อมูล รวมถึงหลักเกณฑ์ที่ใช้



สิทธิของเจ้าของข้อมูล รวมถึง การเข้าถึง, แก้ไข, ลบ, ระงับ, คัดค้าน, โอน และถอน



สิทธิในการร้องเรียนยังสำนักงาน



เงื่อนไขตามกฎหมายหรือสัญญา



แหล่งข้อมูลต้นทาง



การประมวลผลอัตโนมัติ

สิทธิเข้าถึงข้อมูล (Right of Access)



หนังสือรับรองการประมวลผล



สำเนาข้อมูลส่วนบุคคล



ข้อมูลเพิ่มเติม



วัตถุประสงค์และฐานการประมวลผล



ประเภทข้อมูลที่ใช้



ผู้รับข้อมูลส่วนบุคคล



รายละเอียดของประเทศที่ส่งข้อมูลรวมถึงมาตรการที่ใช้



ระยะเวลาในการจัดเก็บข้อมูล รวมถึงหลักเกณฑ์ที่ใช้



สิทธิของเจ้าของข้อมูล รวมถึง การเข้าถึง, แก้ไข, ลบ, ระงับ, คัดค้าน, โอน และถอน



สิทธิในการร้องเรียนยังสำนักงาน



แหล่งข้อมูลต้นทาง



การประมวลผลอัตโนมัติ

สิทธิแก้ไขข้อมูลให้ถูกต้อง (Right to Rectification)



ข้อมูลวินิจฉัยไม่ถูกต้อง



ข้อมูลความเห็น



ระงับการประมวลผล



Manifestly unfounded



Excessive

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/>

สิทธิลบข้อมูล (Right to Erasure)



ไม่จำเป็นต้องใช้



ได้ถอนความยินยอม



ได้คัดค้านการประมวลผล (LI / DM)



ไม่มีฐานการประมวลผล



ทำตามกฎหมาย



ข้อมูลผู้เยาว์



เสรีภาพในการแสดงออก



ปฏิบัติตามกฎหมายกำหนด



ภารกิจของรัฐ



งานวิจัย สถิติ ประวัติศาสตร์ จดหมายเหตุ



การใช้สิทธิตามกฎหมาย



จำเป็นเพื่อการสาธารณสุข



จำเป็นเพื่อการแพทย์



Manifestly
unfounded



Excessive



Backup (beyond
use)

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/>

สิทธิระงับการประมวลผล (Right to Restriction)



กำลังตรวจสอบความถูกต้องของข้อมูล

สิทธิแก้ไขข้อมูลให้ถูกต้อง



กำลังตรวจสอบประโยชน์โดยชอบด้วยกฎหมาย

สิทธิคัดค้านการประมวลผล



ไม่มีฐานการประมวลผลแต่ไม่ต้องการให้ลบ



ถูกร้องขอให้เก็บข้อมูลไว้เพื่อใช้สิทธิตามกฎหมาย



ย้ายข้อมูลออกชั่วคราว



ทำให้ข้อมูลใช้งานไม่ได้



ถอนข้อมูลออกจากเว็บไซต์ชั่วคราว



Manifestly
unfounded



Excessive

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/>

สิทธิในการโอนข้อมูล (Right to Data Portability)



ข้อมูลที่คุณควบคุมได้

Structured, commonly used and machine-readable
Observation (web history, traffic and location, raw data
such as smart meters & wearables)



Inferred or derived data

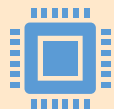


การประมวลผลด้วยฐาน

ความยินยอม หรือ
สัญญา



Technical feasibility



การประมวลผลด้วยระบบอัตโนมัติ



Without hindrance



Manifestly
unfounded



Excessive

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/>

สิทธิคัดค้านการประมวลผล (Right to Object)



การตลาดแบบตรง (สิทธิเด็ดขาด)



การประมวลผลตามภารกิจของรัฐ

เพื่อประโยชน์สาธารณะ

เป็นการดำเนินการต่อเจ้าของข้อมูล



ประโยชน์โดยชอบของเจ้าของข้อมูลหรือบุคคลอื่น



งานวิจัย สถิติ ประวัติศาสตร์ จดหมายเหตุ



Manifestly
unfounded



Excessive

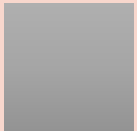
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/>

สิทธิเกี่ยวกับการประมวลผลอัตโนมัติ

(Rights related to automated decision-making including profiling)



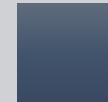
การประมวลผลเพื่อกำหนดวงเงินกู้



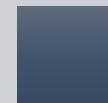
การทดสอบประเมินความสามารถด้วยโปรแกรม



ข้อมูลหรือคำอธิบายที่สมเหตุสมผล



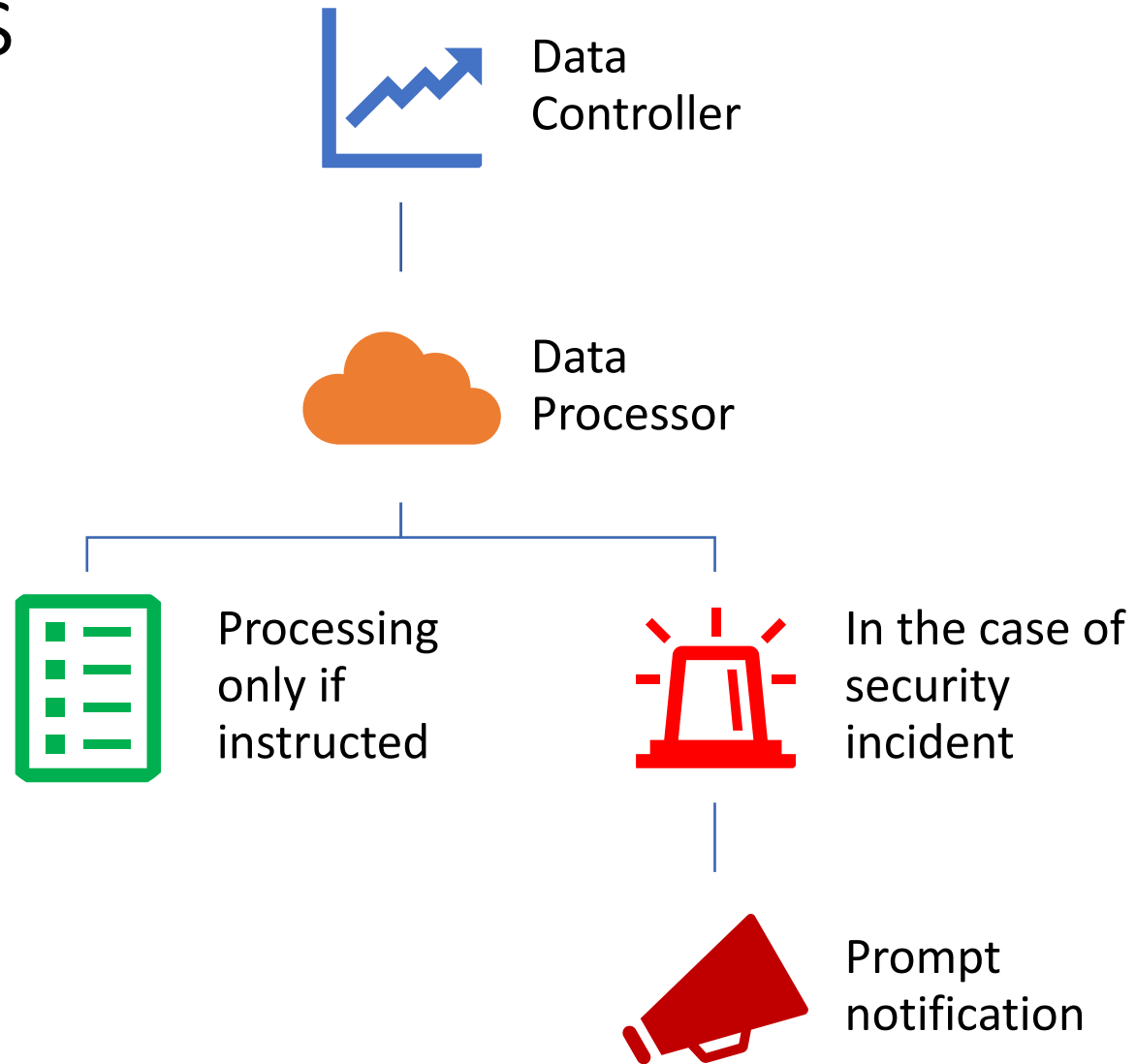
ป้องกันไม่ให้มีความผิดพลาดหรืออคติ



ให้สิทธิโต้แย้งและทบทวน
กระบวนการ

Key Clauses

To what **extent**
personal data will be
processed and what if
there is an **accident**?



ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Cross-border Data Transfer)



Transfer



Transit

ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Cross-border Data Transfer)

Adequacy Decision (มาตรา 28 วรรค 1)

Appropriate Safeguards

- Legal binding instrument between public authorities (1)
- Binding corporate rules (1)

Derogations

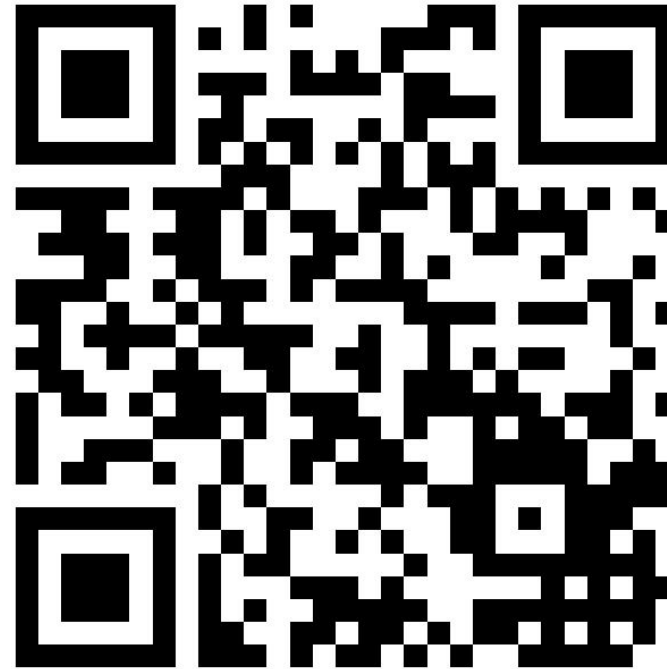
- Legal claim (1)
- Explicit consent (2)
- Necessary for pre-contractual measures (3)
- Necessary for data subject's interest (4)
- Vital interest (5)
- Important Public Interest (6)

Faculty of Law, Chulalongkorn University

THAILAND DATA PROTECTION

GUIDELINES 2.0

แนวปฏิบัติเกี่ยวกับการคุ้มครอง
ข้อมูลส่วนบุคคล



<http://www.law.chula.ac.th/event/7721/>

ISBN 978-616-407-458-3

TDPG2.0



Data Classification

Data Policy
Data Discovery
Data Proliferation
Data Risk Level
Data Protection
Special Categories
/ Sensitive Data



Lawful Basis for Processing

Contract
Consent
Vital Interest
Legal Obligation
Public Task
Legitimate Interest



Controllers & Processors

Duties & Responsibilities
Data Processing Agreement
User Requests
Government Requests



DPIA (Data Protection Impact Assessment)



Cross-Border Data Transfer



Anonymisation

TDPG3.0



Marketing &
Sales



Data Analytics



Human
Resources



Sensitive Data



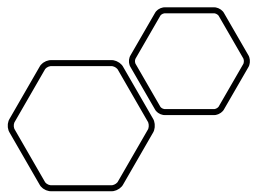
IT Department



Procurement



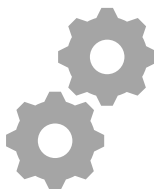
Investment Bank



แผนงาน



Existing Rules & Policies



Processing Activities



Rules, Policies & Forms



Training

Chula Data Protection Program 2020-2021

Privacy by Design



Q/A

piyabutr.b@chula.ac.th

ขอเชิญเข้าร่วมประกวดรางวัล
การเตรียมความพร้อม
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

“PDPA Awards 2020”

รับรางวัลในงาน
“สัมมนาเชิงปฏิบัติการในการเตรียมความพร้อมก่อนการบังคับใช้
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562”

22/12
2563

- ◆ รางวัลการเตรียมความพร้อมดีเด่น
- ◆ รางวัลชมเชยการเตรียมความพร้อม

  **LAW
CHULA** 

เปิดรับสมัคร ตั้งแต่วันที่ – 9 ธันวาคม 2563
รายละเอียดเพิ่มเติม >>>

