



MDES

THAI DATA PRIVACY AND EU GDPR

Choice or Chance
Compliance to Competitive



MDES
WanawitA

ABOUT SPEAKER

Senior Advisor
International Affairs : MDES

Mr. WANAWIT Ahkuputra

- Principal Partner & Founder – Privy Partner Co.,Ltd.
- Senior Advisor on Foreign Affairs - MDES
- 15 Years in Banking, Finance , Securities and SI
- 15 Years in Finland with Security Technology , R&D and Fund Manager
- 7 Years in Government and International Fora



CURRENT ASSIGNMENT RELATED TO PRIVACY

- 2018-Present **Member of the Commission**, Preparatory Committee for Personal Information Protection Act, – Ministry of Digital Economy and Society (Appointed since July,2018)
- 2018-Present **Senior Advisor on International Affairs** – Ministry of Digital Economy and Society
- 2016-Present **Fellow , IETF – Internet Engineering Taskforce** ,Internet Policy and UAG
- 2016-Present **Member, Privacy Advisory Group (PAG)**, UNITED NATIONS Global Pulse
- 2016-Present **Chairman of RCEP WORKING GROUP ON ELECTRONIC COMMERCE**, Regional Comprehensive Economic Partnership (RCEP), Trade Negotiating Committee (RCEP-TNC) Working Group
- 2015 – Present **Delegation, Thailand , APEC ECSG/DPS Electronic Commerce Steering Group / Data Privacy Subgroup** , Asia Pacific Economic Corporation APEC



All about PRIVACY

WHY named data protection ?

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

Privacy & Security Two side of a Coin



Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

Privacy



กรม ก.ม. ขอเชิญชวนเป็นเจ้าพนักงาน

เว็บไซต์: www.komchadluek.net | [kom_chad_luek](https://www.facebook.com/kom_chad_luek) | [komchadluek](https://www.instagram.com/komchadluek)

เชื่อมกว่าที่คิด..
เปิดร่าง พ.ร.บ.คุ้มครอง
ข้อมูลส่วนบุคคล ฉบับใหม่

กรม ก.ม. ขอเชิญชวนเป็นเจ้าพนักงาน

เว็บไซต์: www.komchadluek.net | [kom_chad_luek](https://www.facebook.com/kom_chad_luek) | [komchadluek](https://www.instagram.com/komchadluek)



Credit : Privy Partner Co.,Ltd.



Security



- Access Directive
- Authorization Directive
- Framework Directive
- Universal Service Directive

งานสัมมนาจับความเคลื่อนไหว
ร่างพระราชบัญญัติ
การรักษาความมั่นคง
ปลอดภัยไซเบอร์ พ.ศ.

ETDA

CYBER SECURITY

รู้จัก **W.S.U. คอมพิวเตอร์ฯ**
ฉบับที่ 2 **2560**

Credit : Privy Partner Co.,Ltd.





กล่าวว่า เป็น **Game Changer** ในหลาย Industry

รวมถึงการทำงานในสาย กฎหมายและกระบวนการยุติธรรม

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

9

WHY C-SUIT AND BOARD ?

- Data Privacy is C-Suit Priority : 10 Keys to Manage Reputation Risk
- Fidelity's Corporate Governance -> **Reputation Risk**
- Strategic Alignment
 - Effective Board Oversight
 - Integration of risk into strategic setting and business planning
 - Effective communications, image, and brand building
- Cultural Alignment
 - Strong corporate values, supported by appropriate performance incentives
 - Positive culture regarding compliance with laws, regulations and internal policies
- Quality & Privacy Commitment
 - Priority in Positive Interaction with Stake Holder
 - Quality Reporting System
- Operational Focus
 - Strong Control
 - Industry PAR
- Organization Resiliency
 - Respond to Poli- Crisis

Copyright 2019 © Privy Partner Co.,Ltd



Credit :

Jim DeLoach



Jim DeLoach has over 35 years of experience and is a member of Provitiv's Solutions Leadership Team. With a focus on helping organizations respond to government mandates, shareholder demands and a changing business environment in a cost effective and sustainable manner, Jim assists companies in integrating risk and risk management with strategy setting and performance management. Jim has been appointed to the NACD Directorship 100 list from 2012 to 2017.

MDES
WanawitA

10

LEGAL FRAMEWORK

Not a single legal measure binding us

MDES WanawitA 11

PRIVACY AND DATA PROTECTION ECO-SYSTEM

- International and Country Obligation Level

RCEP
REGIONAL COMPREHENSIVE ECONOMIC PARTNERSHIP

ASEAN +6 & RCEP

APEC
Asia-Pacific Economic Cooperation

21 MEMBERS

- Australia
- Brunei
- Canada
- Chile
- People's Republic of China
- Republic of China (Taiwan)
- Hong Kong
- Indonesia
- Japan
- South Korea
- Malaysia
- Mexico
- New Zealand
- Peru
- Philippines
- Papua New Guinea
- Russia
- Singapore
- Thailand
- United States
- Vietnam

- ✓ ASEAN Agreement on E-Commerce (Nov18)
- ✓ EU GDPR Territorial Scope (May 18)
- ✓ Thailand PDPA (27 May 2019)
- ✓ E-Privacy Regulation (Some where in 2019)
- RCEP Regional Comprehensive Economic Program (Est. 2019)
- APEC – CBPR /PRP Program (Before 2022)

MDES WanawitA 12

Credit : Privy Partner Co.,Ltd.

ASEAN AGREEMENT ON ELECTRONIC COMMERCE

E-commerce Chapter (Signed 2018)

4. Cross-border Transfer of Information by Electronic Means

(a) Member States recognize the importance of allowing information to flow across borders through electronic means, provided that such information shall be used for business purposes, and subject to their respective **laws and regulations**.

(b) Member States agree to facilitate cross-border ecommerce

- by working towards eliminating or minimizing barriers to the flow of information across borders, including personal information, subject to **appropriate safeguards** to ensure security and confidentiality of information, and when other legitimate public policy objectives so dictate.

(c) Subparagraphs (a) and (b) shall not apply to financial services and financial service suppliers as defined in the Annex on Financial Services of GATS.



ASEAN AGREEMENT ON ELECTRONIC COMMERCE

E-commerce Chapter (Signed 2018)

5. Online Personal Information Protection

(a) Each Member State shall adopt or maintain measures to protect the personal information of the users of e-commerce.

(b) A Member State **shall not be obliged** to implement subparagraph (a) before the date on which that Member State enacts laws or regulations **to protect the personal information of e-commerce users**.

(c) In the development of personal information protection measures, each Member State shall take into account **international principles, guidelines and criteria of relevant international bodies**.



REGIONAL COMPREHENSIVE ECONOMIC PARTNERSHIP: RCEP

E-Commerce Chapter (Expect to finalize text in 2019)

Creating a Conducive Environment for Electronic Commerce

- III.1 Online Consumer Protection (TPP 7)
- **III.2 Online Personal Data Protection (TPP 8)**
- III.3 Unsolicited Commercial E-mail (TPP 14)
- III.4 Domestic Regulatory Frameworks (TPP 5)
- III.5 Custom Duties (TPP 3)
- III.6 Treatment of Digital Products (TPP 4)
- III.7 Transparency *

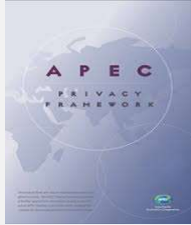


Credit : Privy Partner Co.,Ltd.

ASIA-PACIFIC ECONOMIC COOPERATION (APEC)

ECSG –Electronic Commerce Steering Group – DSP Data Privacy Sub-Group

- APEC Privacy Framework
- CBPRs – Cross Border Privacy Rules System
- PRP - APEC PRIVACY RECOGNITION FOR PROCESSORS SYSTEM



Credit : Privy Partner Co.,Ltd.

ENFORCEMENT !

*By whom it may
concerned*

MDES
WanawitA

THAI PDPA



พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว
ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

Published on Government Gazette

27th May 2019

Coming into Force:

- ▶ Phrase A. → 28 May 2019 :
 - ▶ Chapter I. (PDPA Board Committee) &
 - ▶ Chapter IV. (Office of PDPA Board Committee)

- ▶ Phraser B. → 28 May 2020:
 - ▶ Chapter II. (Protection of Personal Data)
 - ▶ Chapter III. (Usage or Exploitation of Personal Data)
 - ▶ Chapter V. (Complaint-Dispute Resolutions)
 - ▶ Chapter VI (Civil Responsibility)
 - ▶ Chapter VII (Penalty)
 - ▶ Section 94 – Initial Operations for Office of PDPA Board Committee
 - ▶ Section 96 – Supervision on Issuance of Subordinate Laws and Regulations by Gov.

Credit: Chayalawatch Atibaedya

Ministry of Digital Economy & Society as the Interim Office to PDPA Board

- ▶ Phrase A: → Issuance 12 Subordinary Laws or Regulations for Formulation of PDPA Board & Office of PDPA Board by 180 days after promulgation of PDPA.

- ▶ Pharase B: → Issuance 29 Subordinary Laws or Regulations for Technical Features related to Operation of Law by 1 year after promulgation of PDPA (to be monitored by Government Committee)

Credit: Chayalawatch Atibaedya

Legal Aspect of PDPA

Not only respects Human Rights' Protection under Constitution

But

Reveals Consumer Protection Scheme by
supervising Service Providers ("Controller" and "Processor")
and
protecting rights of Consumer ("Data Subject")

Credit: Chayalawatch Atibaedya

Key Considerations of the PDPA

- Penalties**  ≤ 5,000,000

The PDPA Penalties & fines apply to both Controllers and Processors
- Explicit consent** 

Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.
- Limiting Collection, Use, Disclosure** 

collect, use or disclose personal data about an individual for the purposes that a reasonable person would consider appropriate in the circumstances and for which the individual has given consent.
- Breach notification within 72 hours** 


Reported within 72 hours of first having become aware of the breach.
- Right to be forgotten** 

data subject to have the data controller erase his / her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.
- Right to access and portability** 

Data subjects can request confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, in an electronic format (if practicable).
- Appointed Data Protection Officers** 

Appointed in certain cases (public authorities, when monitoring of data subjects on a large scale and when processing special categories of data). To facilitate the need for a organisation to demonstrate their compliance to the PDPA

Credit: Chayalawatch Atibaedya



4.5.2016 EN Official Journal of the European Union L 119/1

I
(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free
movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
(Text with EEA relevance)



1 year
GDPR

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA 24

410

วันแล้ว

หลังจากที่ **GDPR**
มีผลบังคับใช้




EU General Data Protection Regulation
25 May 2018



Credit : Privy Partner Co.,Ltd.

บทเรียน ที่ผู้ประกอบการควรเตรียมการ

- การวางแผนรับมือ Workload จากจำนวนการ ร้องเรียนผ่าน Call Center.
 - หลักการกำหนดคำถามเพื่อ ประกอบการพิจารณา และทำ SAR
 - ระบบการรายงานต่อ DPO ขององค์กร
 - ระบบการตอบ SAR เพื่อระมัดระวัง การร้องเรียนต่ออัยกษาท.และ สำนักงานคุ้มครองข้อมูลส่วนบุคคล
- ลักษณะหัวข้อข้อร้องเรียนที่เกิดขึ้น
 - SAR
 - การขอลบข้อมูล
 - Unfair processing
 - Disclosure
 - Unwanted marketing
 - Employee privacy
- DPA ในเยอรมัน มีประเด็นน่าสนใจ
 - มีจำนวนองค์กรที่ DPO registered มากที่สุด
 - ICANN WhoIS ที่ได้รับคำสั่งศาลของเยอรมัน ที่ต้องปิดการเข้าถึง
 - ติดตามมาตรฐาน ข้อกำหนดในเรื่อง IMRS และปรับปรุงให้สอดคล้อง



GDPR ONE YEAR ANNIVERSARY
Hundreds of thousands of cases — and the DPOs to handle them

280,000+ CASES RECEIVED by DPAs

375,000+ ORGANIZATIONS are DOCUMENTED to have registered DPOs

144,000+ individual COMPLAINTS

500,000 ORGANIZATIONS are ESTIMATED to have registered DPOs

89,000+ data breach NOTIFICATIONS


440+ cross-border CASES

€56,000,000+ FINES

AND THE WORK CONTINUES.
European Data Protection Board Guidance Expected in 2019/2020

- Delisting
- PISD
- Public body international transfers
- Certification and codes of conduct
- Connected vehicles
- Video surveillance
- Data protection by design/default
- Targeting social media users
- Children's data
- Concepts of controller and processor
- Legitimate interest
- Art. 47 of the Law Enforcement Directive
- Rights of access, erasure, objection, and restriction

iapp.org



Credit : Privy Partner Co.,Ltd.

AN ESTIMATED 500K ORGANIZATIONS HAVE REGISTERED DPO ACROSS EUROPE

Study of IAPP

- In 2017, an IAPP study estimated the GDPR would create a need for at least **75,000 DPOs** worldwide.
- The new estimate, which indicates a **half-million organizations** already registered DPOs, combined with new data from IAPP's latest salary survey, sheds light on the rapid growth of the privacy profession and the expanding role of DPOs in Europe and beyond.
- Since the last salary survey in 2017, median salaries overall have risen by more than \$8,000 to \$123,050, and additional compensation in the form of bonuses and raises is also up – the median value of **additional compensation last year was \$20,000**
- Meanwhile, the median salary of privacy professionals who hold a title that was neither CPO nor DPO (i.e., privacy counsel, director of privacy, privacy manager, etcetera) is \$120,000.
 - Chief privacy officer: \$200,000
 - Lead privacy counsel: \$183,000
 - Director of privacy: \$147,000
 - Deputy chief privacy officer: \$141,000
 - Privacy engineer: \$136,000
 - Data privacy manager: \$134,000
 - Privacy counsel: \$130,000
 - Privacy officer: \$121,000
 - Privacy manager: \$105,000
 - Data protection officer: \$100,000
 - Privacy analyst: \$76,000

Add a footer
Credit : Privy Partner Co.,Ltd.

MDES
WanawitA 27



The Privacy Advisor

Dr. Ana Menezes Monteiro, CIPP/E, CIPM, CIPT, FIP





Sabe o que aconteceu no Centro Hospitalar em 2018?



- เป็นโรงพยาบาลแรกใน EU ที่โดนปรับจาก GDPR ในเดือน มกราคม 2019
- โรงพยาบาลขนาด 500 เตียง
- โทษปรับมูลค่า 400,000 ยูโร หรือ ประมาณ 14 ล้านบาท
- DPA – Data Protection Authority ของ โปรตุเกส – CNPD เป็นผู้สอบสวน
- โรงพยาบาล มีความผิดละเมิด GDPR 3 ข้อกล่าวหา



Credit : Privy Partner Co.,Ltd.

MDES
WanawitA 28

ความคิดที่ 1 : ละเมิดหลักการ การดำเนินการเกี่ยวกับข้อมูลอย่างจำกัด (Minimization principle) และการอนุญาตให้เข้าถึงข้อมูลแบบ ไม่จำกัดสิทธิ์ที่เหมาะสม เป็นการละเมิดมาตรา 5 (1)(c) และทำให้เกิดค่าปรับ ตามมาตรา 83 (5)(a) ซึ่งความผิดดังกล่าวนี้ กำหนดค่าปรับในกรณีนี้ 150,000 ยูโรซึ่งความผิดนี้สามารถปรับได้สูงสุด 20 ล้านยูโร

CHAPTER II

Principles

Article 5. Principles relating to processing of personal data

1. Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

CHAPTER VIII

Remedies, liability and penalties

Article 83. General conditions for imposing administrative fines

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;



ความคิดที่ 2 : ละเมิดหลักการ Integrity and Confidentiality เป็นการละเมิดมาตรา 5 (1)(f) ซึ่งเกิดจากไม่มีกลไก Technical & Organization Measure ต่อการประมวลผลข้อมูลส่วนบุคคล และทำให้เกิดค่าปรับ ตามมาตรา 83 (5)(a) ในการละเมิดข้อกำหนดหลักการปฏิบัติต่อข้อมูลส่วนบุคคล ซึ่งความผิดดังกล่าวนี้ กำหนดค่าปรับในกรณีนี้ 150,000 ยูโร

CHAPTER II

Principles

Article 5. Principles relating to processing of personal data

1. Personal data shall be:

- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

CHAPTER VIII

Remedies, liability and penalties

Article 83. General conditions for imposing administrative fines

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;



ความคิดที่ 3 : ปรับโรงพยาบาลในฐานะ Controller มีหน้าที่ตามมาตรา 32 (1)(b) ในการกวดขัน การดำเนินการต่อการประมวลผล และการให้บริการที่กระทำต่อ ข้อมูลส่วนบุคคล โดยมีหลักการ Confidentiality, Integrity, Availability and Resilience อีกทั้งไม่ได้จัดให้มีการดำเนินการในด้าน Technical and Organization Measure ที่ทำให้มีระดับการรักษาความปลอดภัยของข้อมูล สอดคล้องกับความเสี่ยง และขาดการทดสอบประเมินผล กลไกในด้าน Technical and Security Measure ดังกล่าว ซึ่งความคิดดังกล่าวนี้ กำหนดค่าปรับในกรณีนี้ 150,000 ยูโร ซึ่งความคิดนี้สามารถปรับได้ถึง 10 ล้านยูโร หรือ 2% ของรายรับ



CHAPTER IV

Controller and processor

Article 32. Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA 31

ข้อเท็จจริงที่สรุปจาก CNPD

บทเรียนสำคัญ

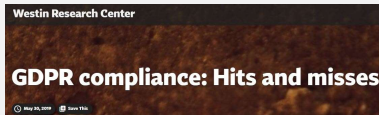
- โรงพยาบาลได้กล่าวอ้างว่า ระบบงานนั้นเป็นระบบของกระทรวงสาธารณสุข มิใช่ของโรงพยาบาลเอง แต่ CNPD เห็นว่า ความรับผิดชอบของระบบโรงพยาบาลเป็นของโรงพยาบาลในฐานะ Controller
- ไม่มีเอกสารที่เทียบเคียง ถึงการกำหนดระดับความรู้สามารถ ของผู้ใช้งาน (ความเชี่ยวชาญทางการแพทย์) กับ ระดับที่กำหนดเป็น Profile ในการเข้าถึงข้อมูลคนไข้
- ไม่มีกฎระเบียบ และระบบการกำหนดการสร้าง และบริหารบัญชีผู้ใช้งานระบบของโรงพยาบาล
- เจ้าหน้าที่เทคนิค 9 คน สามารถเข้าถึงข้อมูลทางการแพทย์ที่ส่งวนไว้เฉพาะกลุ่มแพทย์ และสามารถให้คำแนะนำแก่ผู้ใช้งานระบบโรงพยาบาลในประเด็นที่เกี่ยวกับขั้นตอนทางการแพทย์ได้
- ผู้ใช้งานในกลุ่มแพทย์ นั้น ระบบมิได้แบ่งแยกความเชี่ยวชาญเฉพาะ หรือคลินิกที่ทำงานอยู่ ทำให้สามารถเข้าถึงข้อมูลได้ทั้งระบบ ซึ่งผิดหลักการ Need to Know & Minimisation
- มีบัญชีผู้ใช้งานในระบบที่เป็น Profile กลุ่มแพทย์ 985 คน แต่มีบัญชีแพทย์ในโรงพยาบาลเพียง 296 คน
- ตั้งแต่ พฤศจิกายน 2559 มีการยกเลิกบัญชีแพทย์ในระบบเพียง 18 ราย ขาดการบริหารในเรื่องชื่อผู้ใช้งานระบบอย่างมีนัยสำคัญ
- เจ้าหน้าที่ที่มีการปฏิบัติ แบบอิสระ มิได้มีสภาพบังคับ และตระหนักว่าสิ่งที่กระทำนั้น ละเมิดข้อกำหนดในกฎหมาย

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA 32

GDPR COMPLIANCE: HITS AND MISSES

Westin Research Center , 30 May 2019



The misses

- Compliance just scratched the surface — Privacy requirements must be **translated to products and services**
- DSARs overwhelmed – **Automation** to come
- The role of the DPO is **unsettled** – Restructuring is needed
- New processor liability slowed deals – **Insurance options** would help
- One-stop shop did not always translate in practice – Wait and see for now
- Applicability unsettled – Awaiting **additional guidance**

The hits

- Registers of processing forced a cleanup(**art.30 ROP**)
- Privacy risk elevated in **importance** for companies
- Individual awareness of privacy rights **skyrocketed**

Add a footer
Credit : Privy Partner Co.,Ltd.

MDES
WanawitA 33

GDPR สารโดยสรุป

- 11 ข้อบท (Chapter), 99 มาตรา (Article), 173 คำบรรยาย (Recitals) มี Directive พื้นฐานอีกตั้งแตปี 1995 ที่ต้องทำความเข้าใจ
- เจตนารมณ์กฎหมายออกมาเพื่อ สนับสนุนนโยบาย Digital Single Market (DSM) มิใช่เป็น NTMs – Non Tariff Measure
- มีข้อบท ที่ต้องศึกษาให้ละเอียด เพราะกระทบต่อธุรกิจโดยตรง
- ข้อบท 3 มี 12 มาตรา เกี่ยวกับสิทธิของบุคคล (Data Subject)
- ข้อบท 4 มี 20 มาตรา เกี่ยวกับหน้าที่ ความรับผิดชอบ รายละเอียดของ Controller และ Processor

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

4.5.2016
Official Journal of the European Union
L 119/1

I
(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
(Text with EEA relevance)

GDPR

- Chapter 1 (Art. 1 – 4) v
General provisions
- Chapter 2 (Art. 5 – 11) v
Principles
- Chapter 3 (Art. 12 – 23) v
Rights of the data subject
- Chapter 4 (Art. 24 – 43) v
Controller and processor
- Chapter 5 (Art. 44 – 50) v
Transfers of personal data to third countries or international organisations
- Chapter 6 (Art. 51 – 59) v
Independent supervisory authorities
- Chapter 7 (Art. 60 – 76) v
Cooperation and consistency
- Chapter 8 (Art. 77 – 84) v
Remedies, liability and penalties
- Chapter 9 (Art. 85 – 91) v
Provisions relating to specific processing situations
- Chapter 10 (Art. 92 – 93) v
Delegated acts and implementing acts
- Chapter 11 (Art. 94 – 99) v
Final provisions

MDES
WanawitA

Credit : Privy Partner Co.,Ltd.

4.5.2016
Official Journal of the European Union
L 119/1

Chapter 1 (Art. 1 – 4) ^

General provisions

- Art. 1 – Subject-matter and objectives
- Art. 2 – Material scope
- Art. 3 – Territorial scope
- Art. 4 – Definitions

Chapter 2 (Art. 5 – 11) ^

Principles

- Art. 5 – Principles relating to processing of personal data
- Art. 6 – Lawfulness of processing
- Art. 7 – Conditions for consent
- Art. 8 – Conditions applicable to child's consent in relation to information society services
- Art. 9 – Processing of special categories of personal data
- Art. 10 – Processing of personal data relating to criminal convictions and offences
- Art. 11 – Processing which does not require identification

Chapter 3 (Art. 12 – 23) ^

Rights of the data subject

- Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject
- Art. 13 – Information to be provided where personal data are collected from the data subject
- Art. 14 – Information to be provided where personal data have not been obtained from the data subject
- Art. 15 – Right of access by the data subject
- Art. 16 – Right to rectification
- Art. 17 – Right to erasure ('right to be forgotten')
- Art. 18 – Right to restriction of processing
- Art. 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Art. 20 – Right to data portability
- Art. 21 – Right to object
- Art. 22 – Automated individual decision-making, including profiling
- Art. 23 – Restrictions

MDES
WanawitA

Credit : Privy Partner Co.,Ltd.

<p>Chapter 4 (Art. 24 – 43)</p> <p>Controller and processor</p> <p>Art. 24 – Responsibility of the controller</p> <p>Art. 25 – Data protection by design and by default</p> <p>Art. 26 – Joint controllers</p> <p>Art. 27 – Representatives of controllers or processors not established in the Union</p> <p>Art. 28 – Processor</p> <p>Art. 29 – Processing under the authority of the controller or processor</p> <p>Art. 30 – Records of processing activities</p> <p>Art. 31 – Cooperation with the supervisory authority</p> <p>Art. 32 – Security of processing</p> <p>Art. 33 – Notification of a personal data breach to the supervisory authority</p> <p>Art. 34 – Communication of a personal data breach to the data subject</p> <p>Art. 35 – Data protection impact assessment</p> <p>Art. 36 – Prior consultation</p> <p>Art. 37 – Designation of the data protection officer</p> <p>Art. 38 – Position of the data protection officer</p> <p>Art. 39 – Tasks of the data protection officer</p> <p>Art. 40 – Codes of conduct</p> <p>Art. 41 – Monitoring of approved codes of conduct</p> <p>Art. 42 – Certification</p> <p>Art. 43 – Certification bodies</p>	<p>Chapter 5 (Art. 44 – 50)</p> <p>Transfers of personal data to third countries or international organisations</p> <p>Art. 44 – General principle for transfers</p> <p>Art. 45 – Transfers on the basis of an adequacy decision</p> <p>Art. 46 – Transfers subject to appropriate safeguards</p> <p>Art. 47 – Binding corporate rules</p> <p>Art. 48 – Transfers or disclosures not authorised by Union law</p> <p>Art. 49 – Derogations for specific situations</p> <p>Art. 50 – International cooperation for the protection of personal data</p> <p>Chapter 6 (Art. 51 – 59)</p> <p>Independent supervisory authorities</p> <p>Art. 51 – Supervisory authority</p> <p>Art. 52 – Independence</p> <p>Art. 53 – General conditions for the members of the supervisory authority</p> <p>Art. 54 – Rules on the establishment of the supervisory authority</p> <p>Art. 55 – Competence</p> <p>Art. 56 – Competence of the lead supervisory authority</p> <p>Art. 57 – Tasks</p> <p>Art. 58 – Powers</p> <p>Art. 59 – Activity reports</p>	<p>Chapter 7 (Art. 60 – 76)</p> <p>Cooperation and consistency</p> <p>Art. 60 – Cooperation between the lead supervisory authority and the other supervisory authorities concerned</p> <p>Art. 61 – Mutual assistance</p> <p>Art. 62 – Joint operations of supervisory authorities</p> <p>Art. 63 – Consistency mechanism</p> <p>Art. 64 – Opinion of the Board</p> <p>Art. 65 – Dispute resolution by the Board</p> <p>Art. 66 – Urgency procedure</p> <p>Art. 67 – Exchange of information</p> <p>Art. 68 – European Data Protection Board</p> <p>Art. 69 – Independence</p> <p>Art. 70 – Tasks of the Board</p> <p>Art. 71 – Reports</p> <p>Art. 72 – Procedure</p> <p>Art. 73 – Chair</p> <p>Art. 74 – Tasks of the Chair</p> <p>Art. 75 – Secretariat</p> <p>Art. 76 – Confidentiality</p>
--	---	--

Credit : Privy Partner Co.,Ltd.

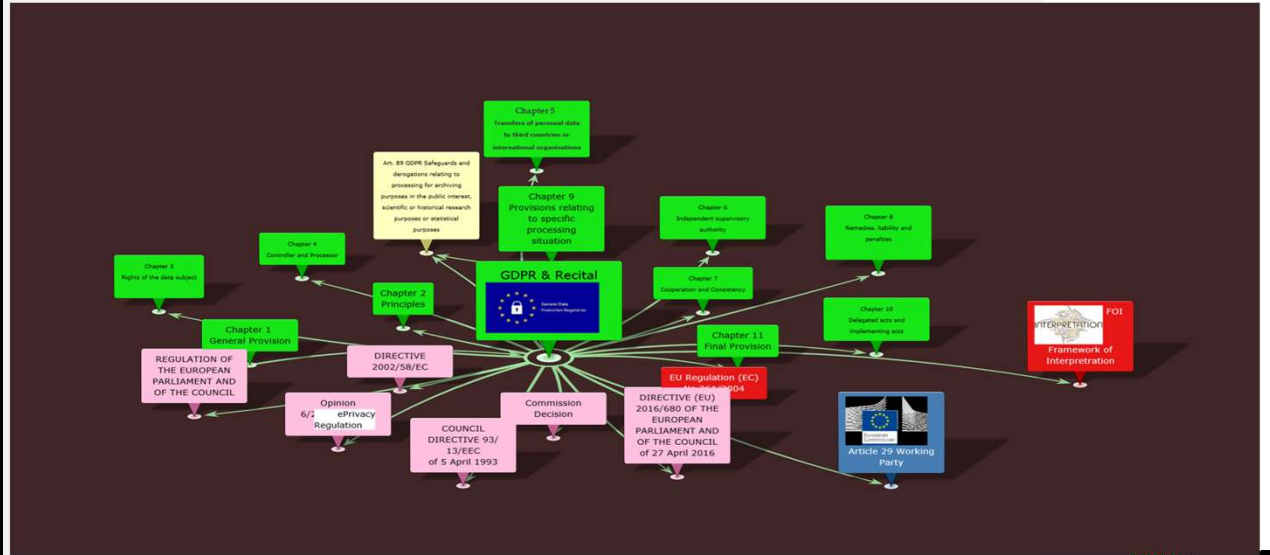
WanawitA

<p>Chapter 8 (Art. 77 – 84)</p> <p>Remedies, liability and penalties</p> <p>Art. 77 – Right to lodge a complaint with a supervisory authority</p> <p>Art. 78 – Right to an effective judicial remedy against a supervisory authority</p> <p>Art. 79 – Right to an effective judicial remedy against a controller or processor</p> <p>Art. 80 – Representation of data subjects</p> <p>Art. 81 – Suspension of proceedings</p> <p>Art. 82 – Right to compensation and liability</p> <p>Art. 83 – General conditions for imposing administrative fines</p> <p>Art. 84 – Penalties</p> <p>Chapter 9 (Art. 85 – 91)</p> <p>Provisions relating to specific processing situations</p> <p>Art. 85 – Processing and freedom of expression and information</p> <p>Art. 86 – Processing and public access to official documents</p> <p>Art. 87 – Processing of the national identification number</p> <p>Art. 88 – Processing in the context of employment</p> <p>Art. 89 – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes</p> <p>Art. 90 – Obligations of secrecy</p> <p>Art. 91 – Existing data protection rules of churches and religious associations</p> <p>Chapter 10 (Art. 92 – 93)</p>	<p>Chapter 10 (Art. 92 – 93)</p> <p>Delegated acts and implementing acts</p> <p>Art. 92 – Exercise of the delegation</p> <p>Art. 93 – Committee procedure</p> <p>Chapter 11 (Art. 94 – 99)</p> <p>Final provisions</p> <p>Art. 94 – Repeal of Directive 95/46/EC</p> <p>Art. 95 – Relationship with Directive 2002/58/EC</p> <p>Art. 96 – Relationship with previously concluded Agreements</p> <p>Art. 97 – Commission reports</p> <p>Art. 98 – Review of other Union legal acts on data protection</p> <p>Art. 99 – Entry into force and application</p>
--	--

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

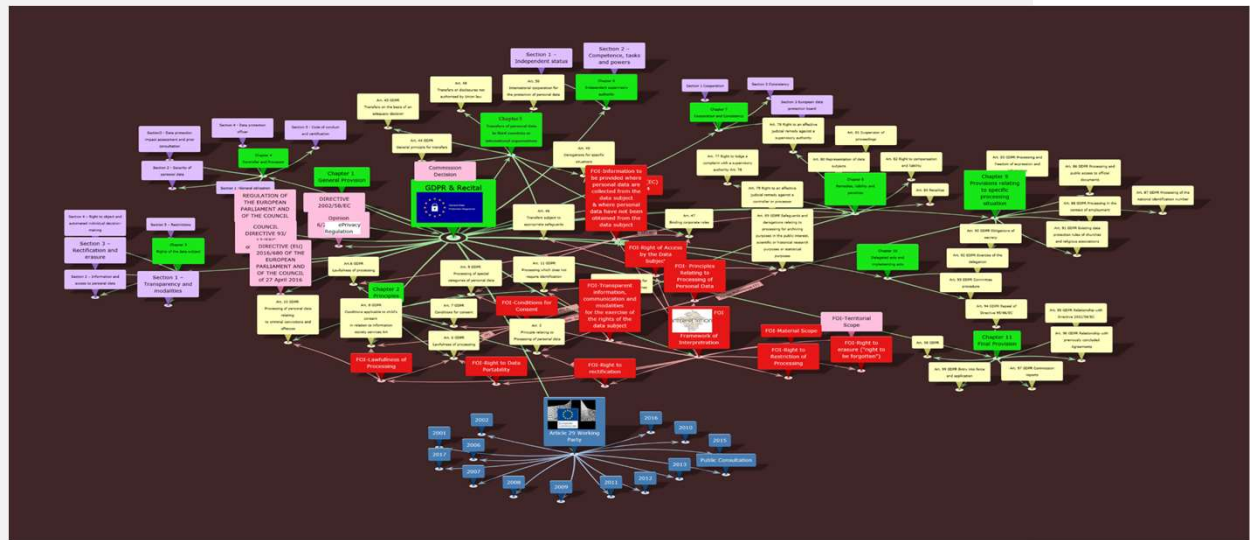
Knowledge Base Level 1: GDPR Regulation, Directive DP/93 and Other Relevant Directive



Copyright 2019 © Privy Partner Co., Ltd

MDES WanawitA

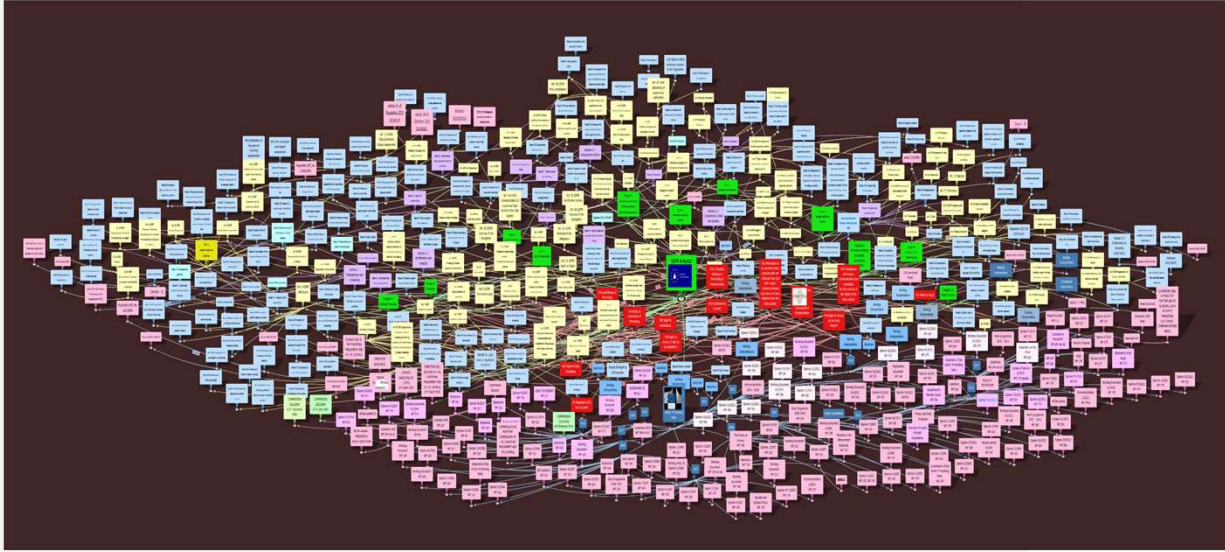
Knowledge Base Level 2: + 173 Recitals and FOI-Framework of Interpretation



Credit : Privy Partner Co., Ltd.

MDES WanawitA

**Knowledge Base Level 3: 100+ WP29-Working Documents ,
20+ Guidelines from WP29 , 50+ Opinions of WP29**



Copyright 2019 © Privy Partner Co.,Ltd

MDES
WanawitA

REGULATIONS

REGULATION (EU) No 536/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 16 April 2014
on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC
(Text with EEA relevance)

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

42

GDPR IN BRIEF

WHAT NEED TO KNOW ABOUT IT?

- **NOTHING NEW** - it start from **DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995** on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- **HARDENING** not **TIGHTENING** . From DIRECTIVE to REGULATION - Big Deal? 22 Years Journey of DP. (TH – 18 Years !!! from first draft to Final Draft)
- Definition of Personal Data **extended** to other identifiable especially in Technical Identifier Context ---- CDR, Traffic Log , IP.....
- Hardening **measures** -> DPIA-Data Privacy Impact Assessment, DPA – Data Protection/Processing Agreement contractual compliance, Privacy by Design/ Default, Data Breach Notification 72 Hours, Consents and Lawfulness of processing activity.

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

GDPR Extra- Territorial Effect

Material Scope

Processing -Personal Data-Automate Means Filing System



Credit Card Transaction **Processing** : PCI DSS
National ID Scheme/PASSPORT : Processing without **Safeguard**
Booking information from OTA

Territorial Scope

Processing -Personal Data-Activity- Establishment
- Controller/Processor - Place

Establishment in/outside the EU
Establishment independent of Legal Form
Stable Arrangement
Processing activity (Automate)
Large amount (> 5000 ?)
Monitor /Target consecutively more than (12) Months?

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

44

PII – PERSONAL IDENTIFIABLE INFORMATION

PII

National ID, HN No., Credit Card no...

Art.9 Special Cat.

Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Others Information

Big Data, Tracking, Profiling, Analytic Data,

Credit : Privy Partner Co.,Ltd.

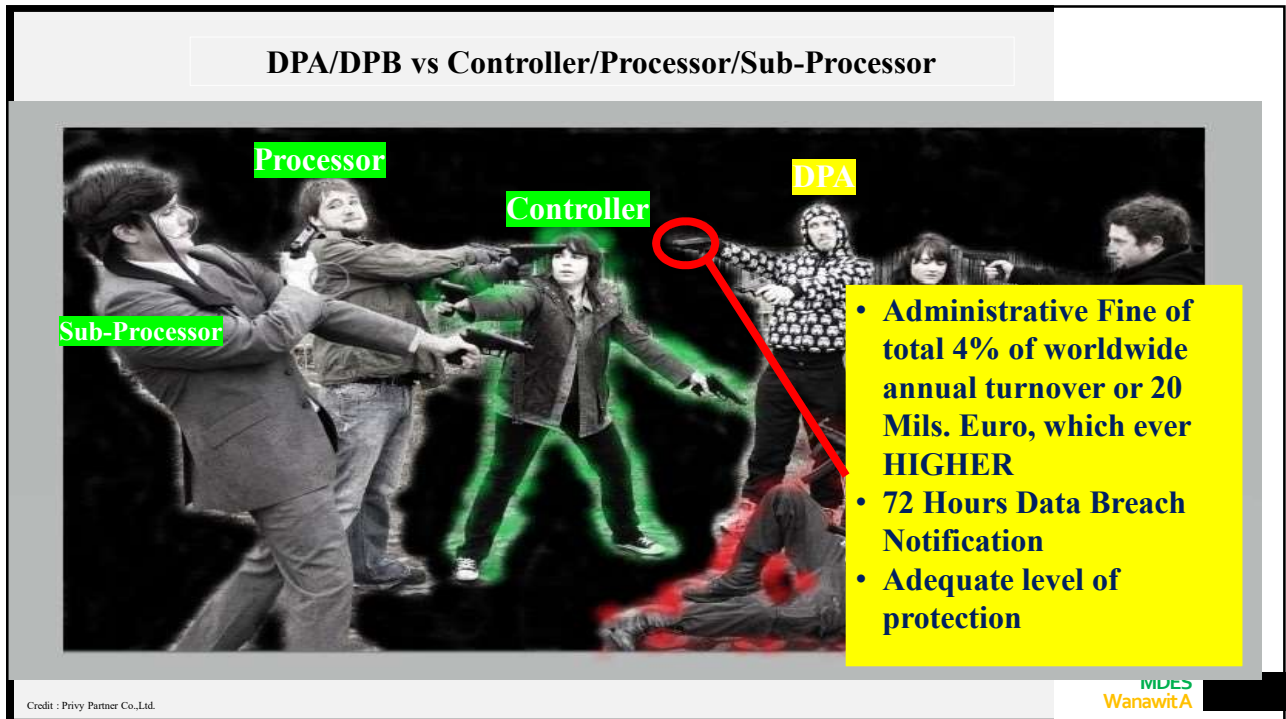
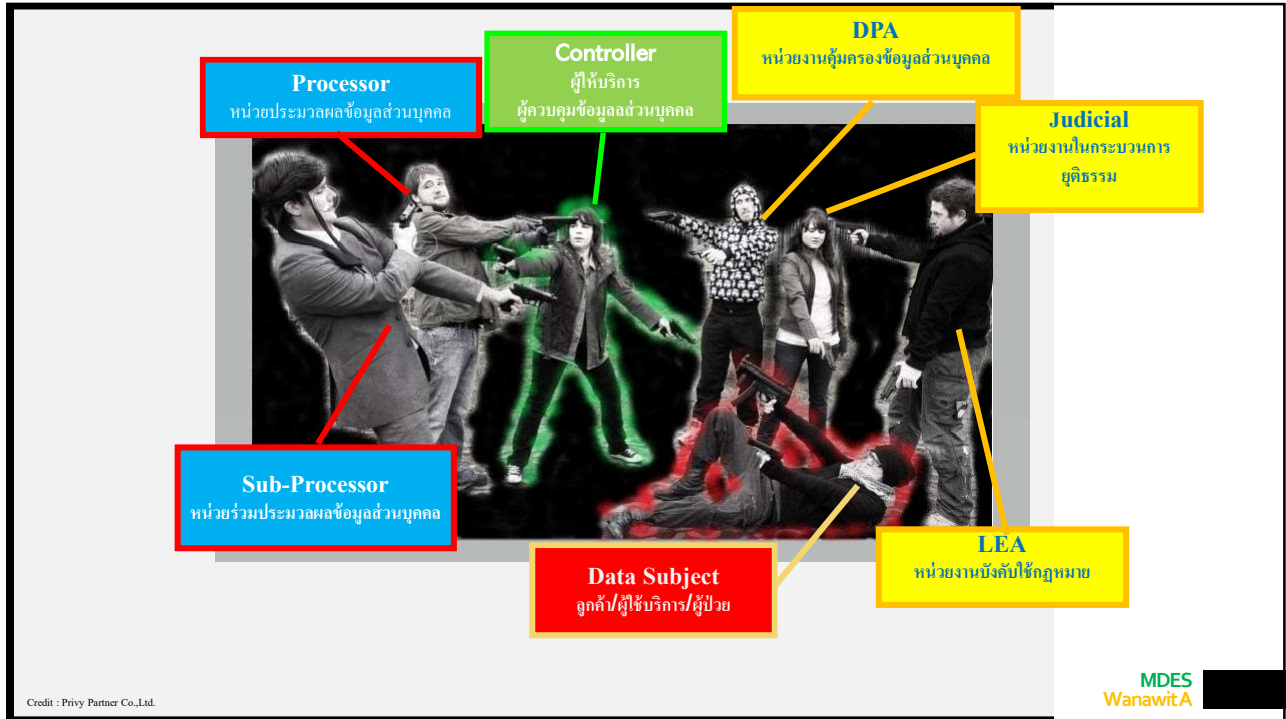
MDES
WanawitA

All the threats are **equally balanced** to ensure a **Mutual Disadvantage**

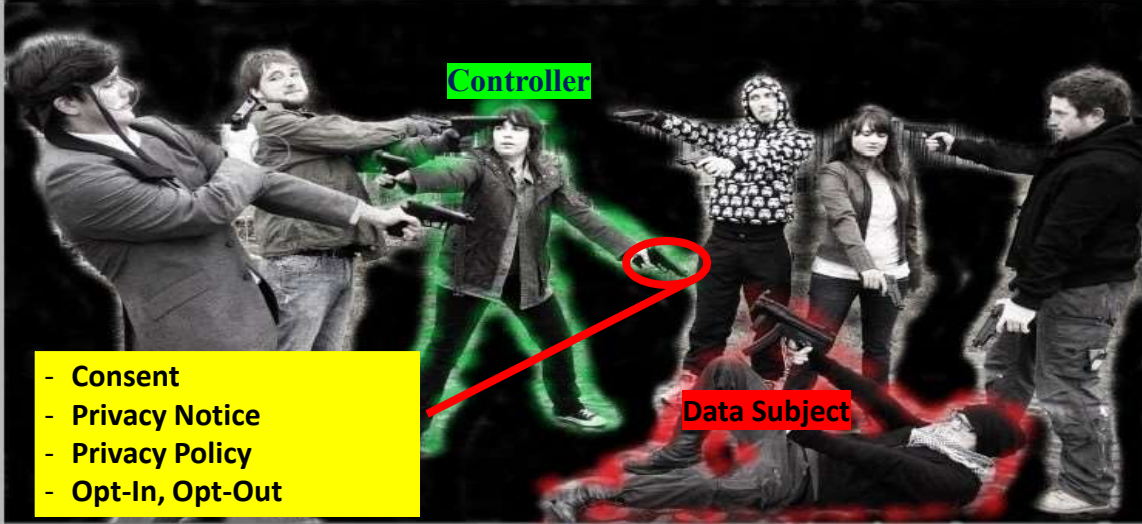


Credit : Privy Partner Co.,Ltd.

MDES
WanawitA



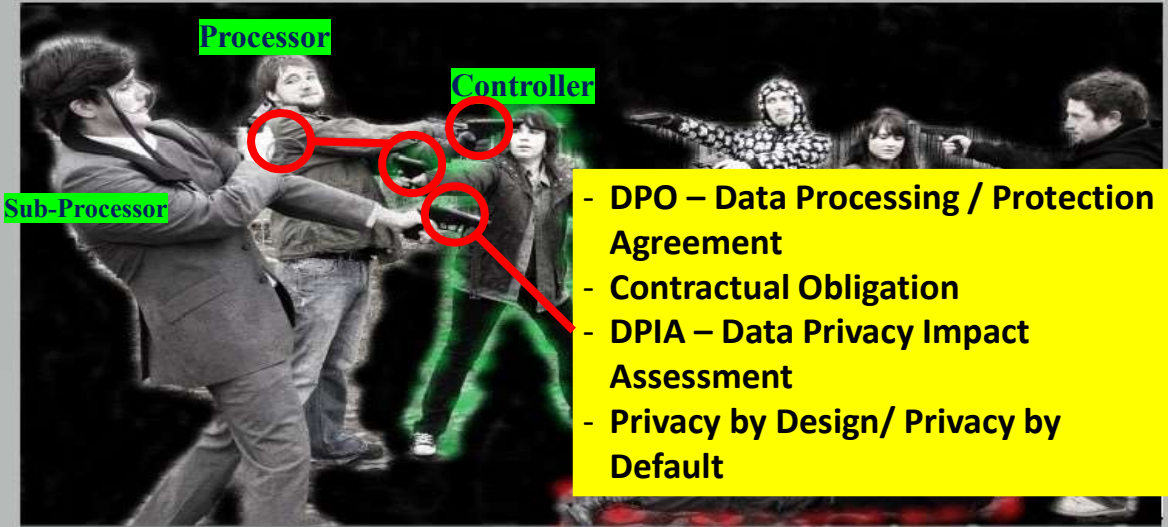
Controller vs Data Subject



Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

Controller vs Processor vs Sub-Processor



Copyright 2019 © Privy Partner Co.,Ltd

MDES
WanawitA

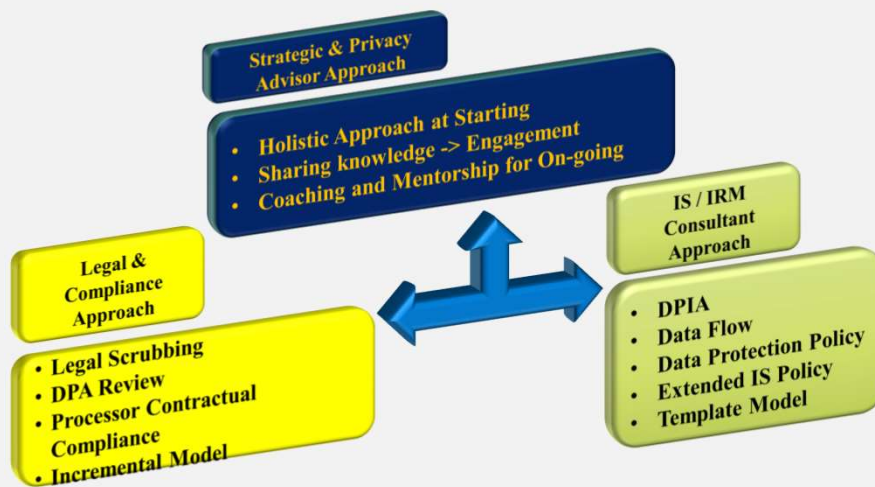
THREE WORKING APPROACH IN GDPR PROJECT : FOCUS AREA



Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

THREE WORKING APPROACH IN GDPR PROJECT : OUTCOME

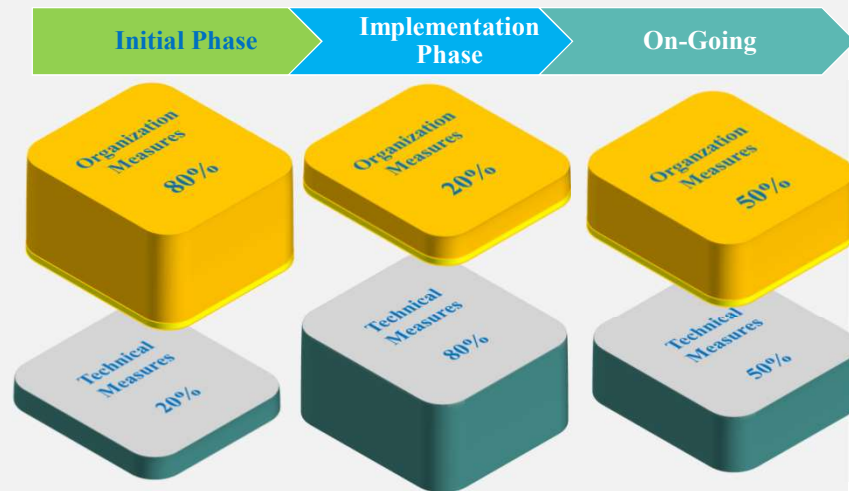


Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

TOMS : TECHNICAL AND ORGANIZATION MEASURE

PHASE AND RESOURCE ALLOCATION : FTE, TIME, MATERIAL, BUDGET



Credit : Privy Partner Co.,Ltd.

MDES
WanawitA

GDPR'S Transfer of Personal Data outside of EU/EEA

Article 44: of the GDPR **prohibits** the transfer of personal data beyond EU/EEA, unless the recipient country can prove it provides adequate data protection. Descriptions of acceptable proof are detailed in

Articles 45 – 49.

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA



GDPR'S Transfer of Personal Data outside of EU/EEA

ADEQUACY DECISION

Article 45: Transfers on the basis of an adequacy decision



- **Whitelisted Jurisdictions**
- **Privacy Shield Framework**

BCRs

Article 47: Binding corporate rules
BCRs are internal rules used by a multinational company to define personal data transfers to company entities located in countries that do not provide an adequate level of protection



Derogations

Article 49: Derogations for specific situations

- Explicitly *consented* to by the Data Subject
- Necessary for the *performance of a contract* or *vital interests* of a Data Subject
- From a public register



APPROPRIATE SAFEGUARDS

Article 46: Transfers subject to appropriate safeguards



- **Standard Contractual Clause (SCC)**
 - o Data Controllers to Data Controllers
 - o Data Controllers to Data Processors located outside the EU/EEA
- **Codes of Conduct and Certification**

International Agreements

Article 48: Transfers or disclosures not authorized by Union law (international agreements)
Personal data may be transferred or disclosed only when ordered by a court or tribunal, if based on an international agreement between the requesting country and the EU/EEA



WHAT NEXT TO BE DONE

As the processor/vendor

WHAT NEED TO BE ADDRESS TO PARADIGM SHIFT

Since YESTERDAY

- Review all contract with your customer.
 - Standard contractual compliance (SCC) that require to be in place.
 - Review all technical measure for data protection
 - External Audit your software and have assessment report
 - Certification ?
- Provide service for your customer
 - Privacy – Organization Measure as a Service
 - SAR – Subject Access Request as a Service

Credit : Privy Partner Co.,Ltd.

MDES
WanawitA 57



SECURITY
Use your Head....
PRIVACY
....Use your Heart

MDES
WanawitA 58

THANK YOU

Wanawit Ahkuputra ☎ +66 8 9301 8818

✉ Wanawit.a@mdes.go.th