แนวปฏิบัติเพื่อกำหนดข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูลทั้งในกรณีที่ได้ข้อมูลส่วนบุคคลจากเจ้าของข้อมูลเองและในกรณีที่ได้ข้อมูลส่วนบุคคลจากแหล่งอื่น

งานสัมมนา “แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อรองรับการมีผลบังคับใช้ของ GDPR”

2 กรกฎาคม 2561

EY
Building a better working world

The information contained in this presentation is intended to provide general information of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional and/or legal advice. We can accept no responsibility for loss arising from any action taken or not taken by anyone using this information.

หัวข้อ

- EU GDPR โดยย่อและหลักการเพื่อคุ้มครองข้อมูลส่วนบุคคล
- สิทธิของเจ้าของข้อมูลตาม EU GDPR
- ข้อกำหนดว่าด้วยข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล
- ความท้าทายในทางปฏิบัติเพื่อกำหนดข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล
- ตัวอย่างกรอบมาตรฐานที่ใช้อ้างอิง
- แนวปฏิบัติเพื่อกำหนดข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

EU GDPR โดยย่อและหลักการเพื่อคุ้มครองข้อมูลส่วนบุคคล

On April 27, 2016 the European Parliament passed the **GDPR,** which is an omnibus data protection law that has been effective since **May 25, 2018**. The GDPR regulation includes the following requirements:

- Penalties for failing to comply with the basic processing principles of GDPR may subject the organization to fines up to €20m or 4% of the organization's total global revenue of the preceding financial year, whichever is greater.
- The GDPR imposes new obligations for both controllers and processors of personal data.
- The GDPR places a greater emphasis on accountability, requiring greater documentation and records.

GDPR applicability:

Companies across all industries, processor/controller relationships and geographies use EU personal data.

User-Centric Extra-Territorial **Awareness of Risks, Rules, Safeguards & Rights** Disproportionate effort

Industries

- Finance/insurance
- Retail
- Health
- Technology
- Business services

Geographies

Controllers and processors

- Processing activities of personal data
  - of the establishment of a controller or processor in the EU
  - of data subjects located in the EU related to
    - The offering of goods or services to such data objects OR
    - The monitoring of their activities taking place within the EU

Key definitions

Controller "the decision-maker"	A body (alone or jointly with others) that determines the purposes and means of the processing of personal data
Processor "the doer"	A body that processes personal data on behalf of the controller; processing can include collecting, organizing, storing, disclosing, using, etc.
Personal data "the what"	Any info (single or multiple data points) relating to an identified or identifiable natural person, such as name, employee identification number or location data

EU GDPR โดยย่อและหลักการเพื่อคุ้มครองข้อมูลส่วนบุคคล
คำจำกัดความที่สำคัญและตัวอย่าง

Personal Data

- Any information relating to an identified or identifiable natural person ("data subject")
- Taking into consideration such factors as cost and amount of time required for identification, technology, an identifiable person is one who can be identified, directly or indirectly), in particular by reference to
  - An identifier such as a name, an identification number, location data, online identifier or
  - One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Processing

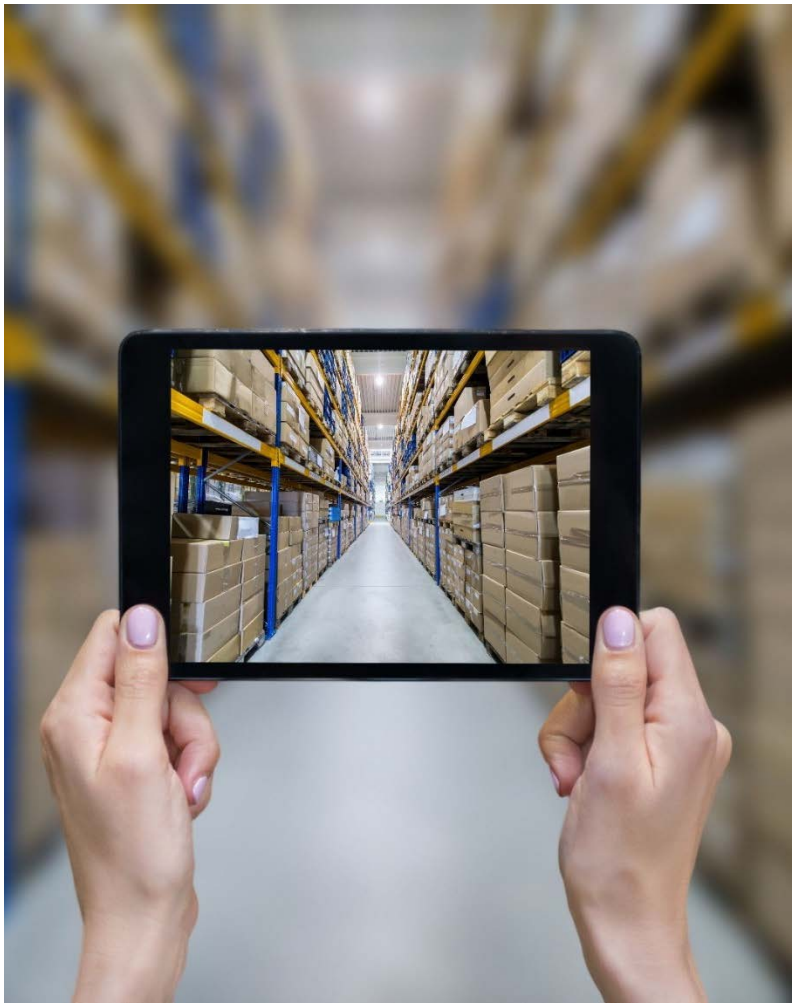
- Any operation or set of operations which is performed on personal data or on sets of personal data, **whether or not by automated names** such as
  - Collection
  - Recording
  - Organization
  - Structuring
  - Storage
  - Adaptation or Alteration
  - Retrieval
  - Consultation
  - Use
  - Disclosure by Transmission
  - Dissemination or otherwise making available
  - Alignment or Combination
  - Restriction
  - Erasure or Destruction

Recital 26, Article 4(1), 4(2)

EU GDPR โดยย่อและหลักการเพื่อคุ้มครองข้อมูลส่วนบุคคล
คำจำกัดความที่สำคัญและตัวอย่าง

- First name and last name
- First initial and last name
- Email address
- Online account names/logons
- Street address
- Telephone numbers (including fax)
- US Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full-face photographs and any comparable images
- Digitized or electronic signatures
- Genetic data
- Health related information
- Location data
- Occupational data (job function, performance detail, salary, education)
- Cookie strings
- Online identifiers
- Behavioral data (online and offline)
- Sensitive data, including religious affiliation, trade union membership, political affiliation race and sexual preference

EU GDPR โดยย่อและหลักการเพื่อคุ้มครองข้อมูลส่วนบุคคล



GDPR มาตรา 5 กำหนดหลักการในการประมวลผลข้อมูลส่วนบุคคล

- Lawfulness
- Fairness
- Transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

สิทธิของเจ้าของข้อมูลตาม EU GDPR

สิทธิของเจ้าของข้อมูลกำหนดไว้ในส่วนที่ 3 ของ GDPR

Data subject right	Related article
▸ **Right to information notice**	**12,13&14**
▸ Right of access	15
▸ Right to rectification	16
▸ Right to be forgotten/Right to erasure	17
▸ Right to restriction of processing	18
▸ Right to data portability	20
▸ Right to object to processing	21
▸ Right not to be subject to automated decision-making, including profiling	22

ข้อกำหนดว่าด้วยข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

Section	Title	Description in summary
Chapter III	***Rights of the data subject***	
Section 2	***Information and Access to Data***	
Article 13	Information to be provided where personal data are collected from the data subject	The information that must be made available to a data subject when data is collected has been strongly defined and includes the identity and the contact details of the controller, the purposes of the processing for which the personal data are intended, the legal basis of the processing, the existence of the right to access, rectify or erase the personal data, the right to data portability, and the right to withdraw consent at any time.
Article 14	Information to be provided where personal data have not been obtained from the data subject	The information that must be made available to a data subject when the data has not been obtained directly from the data subject includes from which source the personal data originates and the existence of any profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

ข้อกำหนดว่าด้วยข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

Information provision:

information which should be provided to the data subject are collected in the privacy notice, which is provided to the data subject by the controller.

Transparency principle:

An organisation should inform the data subject to ensure fair and transparent processing

According to what specified under **Article 12**, the **privacy notice** should be:

- Concise, transparent, intelligible and easily accessible manner
- Using clear and plain language
- Provided in writing, or by other means, including, where appropriate, by electronic means
- May be provided orally if requested by the data subject
- Provided free of charge

ข้อกำหนดว่าด้วยข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

Article 13 & 14 (Recital 60-62) and 83

- Data subjects have the right of information which to be provided by the controller. Annex 1 of the Guidelines on Transparency under Regulation 2016/679 by Article 29 Working Party provides guidance on information that must be provided to a data subject
- Information must be provided when personal data are collected from the data subject
- When personal data have not been obtained from the data subject, information must be provided within a reasonable time after obtaining the personal data, or the time of first communication with the data subject, or the latest at the time of the first disclosure to another recipient, but no later than one month
- Changes to information that has previously provided to the data subject, other than that related to further process for other purpose in which case the information needs to be provided prior to that further processing, must be provided within a reasonable time
- There are certain exceptions such as no need to provide the information if the data subject already has the information or when it is not possible or involve a disproportionate effort but appropriate measures are in place to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available
- Infringement will be subject to administrative fines up to 20,000,000 EUR or 4%% of the organization's total global revenue of the preceding financial year, whichever is higher

Data Processor Considerations

- Processors are responsible for implementing measures to assist the controller in complying with the rights of data subjects.

Sample questions for the Organization

How does the organization provide information to the data subject regarding:

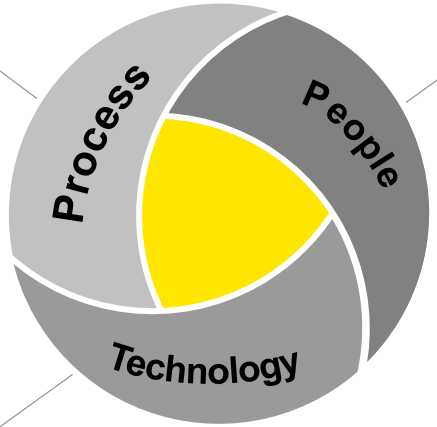
- How their personal data is being processed and purpose of processing
- The recipients or categories of recipients who will have access or receive the data
- How long their data will be maintained
- How to request updates or deletion of data
- How to lodge a complaint
- How any additional data related to them are collected
- The existence of automated decision making

ความท้าทายในทางปฏิบัติเพื่อกำหนดข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

GDPR is a transformational effort that touches on all aspects of an organization, reaching across people, processes and technology.

Process

- Organizations will need to determine which business and IT processes are impacted by GDPR requirements.
- GDPR will require organizations to redesign their processes to incorporate steps that address key privacy requirements.
- Organizations must implement process monitoring controls to provide transparency that the processes consistently satisfy GDPR requirements and are updated as necessary.



People

- Organizations will need to identify the relevant stakeholders across business units, including HR, who can contribute to compliance remediation planning and execution.
- The GDPR will require organizations to adequately train employees responsible for handling EU data with their obligations for supporting GDPR compliance.

Technology

- Organizations must understand their IT environment, data assets and data processing applications to identify the impacts that GDPR requirements present and to develop a remediation plan to update the IT environment to support GDPR compliance.
- Organizations should look into various tools available for automating GDPR compliance operations to an enterprise scale.

As a result of the broad impact of the GDPR, establishing a robust project management office (PMO) team that supports the transformation of the company is a critical step for a successful implementation. Considering the program management and transformational issues can make certain that teams are aligned, communicating effectively and receiving the support needed across the enterprise.

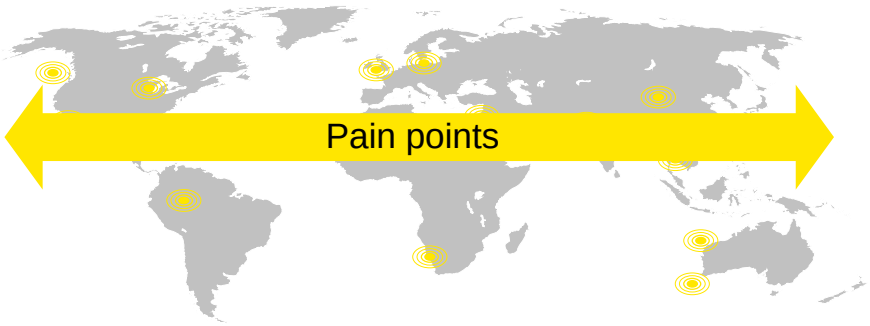
ความท้าทายในทางปฏิบัติเพื่อกำหนดข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

Common profile

- **Complex internal architecture and inconsistent or significantly lacking data management**
- **Reactive approach to compliance**
- **Compliance in policy, but a failure to carry over to business operations and IT**
- **Internal Audit lacks subject-matter expertise or resources to provide assurance of discrete global privacy compliance requirements**
- **C-suite and Board of Directors are unaware of privacy-related risks and potential for material penalties**
- **Limited resources, competing projects, tight budgets, less than robust change management**

Potential fine: Up to 4% of global revenue

Financial impact: In addition to the potential penalties, companies face significant costs associated with internal churn created by uncertainty of compliance.



Data unbound

Business impact: Organizations have collected and stored massive amounts of data, but have little understanding of what it is, where it's stored and what to do next.

72 hours

Response time: Effective management of incident response is essential and only one example where companies must achieve full alignment across their organizations to meet the compliance obligations.

ความท้าทายในทางปฏิบัติเพื่อกำหนดข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

Privacy governance

- Privacy is no longer solely situated within the legal realm, and has evolved into a multidisciplinary issue.
- Organizations are struggling to position a data protection officer (DPO) and establish a comprehensive model to lead privacy transformation.
- A new, collaborative model is needed to unite the multiple dimensions of privacy within the organization.

Data-flow mapping

- Many firms are unaware of their data flows and have launched ambitious data flow mapping initiatives.
- Data-flow mapping exercises are often very detailed and resource consuming.
- Data discovery tooling can be used to further detect structured and unstructured data.

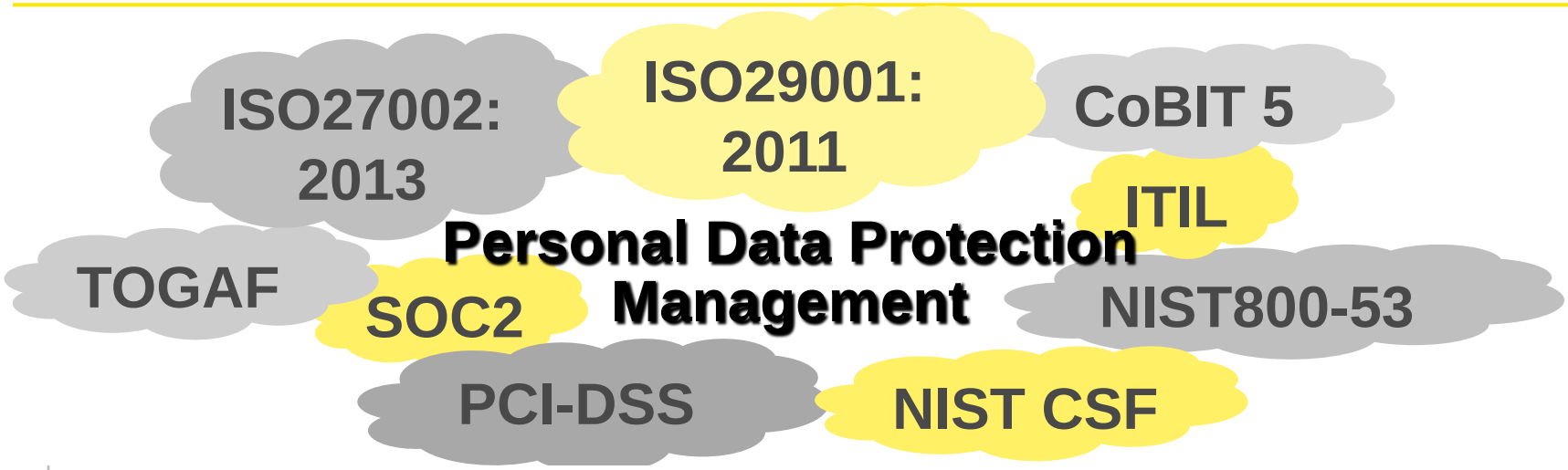
Scope

- The breadth of GDPR means that many organizations have launched ambitious programs with complex requirements.
- Setting items out of GDPR scope and preventing scope creep (for data retention, for instance) is a method of enabling program success.
- Scope definition is dependent on the success of Records of Processing workstream, which should not be underestimated.

IT change

- Proactively educating IT (especially solution architects) on GDPR requirements, scope, options (tactical versus strategic) and delivery expectations is a challenge.
- Setting the right scope for IT change across your organization is critical; excessive scope creep may derail a GDPR program.
- Tools developed for GDPR should be reviewed to assess efficiencies rather than creating complications or excessive costs.

ตัวอย่างกรอบมาตรฐานที่ใช้อ้างอิง



GDPR		ISO 27001/2	
Article	Outline/summary	Control	Notes
***Chapter III* Rights of the data subject**			
13	When personal data are collected, people must be given (or already possess) several specific items of information such as details of the data "controller" and "data protection officer", whether their info will be exported (especially outside the EU), how long the info will be held, their rights and how to enquire/complain *etc.*	A.8.2.1 A.8.2.3 A.12.1.1 A.14.1.1 A.16 *etc.*	Procedures for the provision of fair processing information, information on the data controller and purposes for processing the data need to be defined and implemented. This relies in part on identifying where personal info is in use.
14	Similar notification requirements to Article 13 apply if personal info is obtained indirectly (*e.g.* a commercial mailing list?): people must be informed within a month and on the first communication with them.	A.8.2.1 A.8.2.3 A.12.1.1 A.14.1 A.16 *etc.*	See Article 13.

Source: GDPR & ISO 27001 Mapping Table, ISO2K7 Forum, The British Assessment Bureau, 2016.

ตัวอย่างกรอบมาตรฐานที่ใช้อ้างอิง

GDPR		ISO 27001/2	
Article	Outline/summary	Control	Notes
***Chapter III* Rights of the data subject**			
13	When personal data are collected, people must be given (or already possess) several specific items of information such as details of the data "controller" and "data protection officer", whether their info will be exported (especially outside the EU), how long the info will be held, their rights and how to enquire/complain *etc.*	A.8.2.1 A.8.2.3 A.12.1.1 A.14.1.1 A.16 *etc.*	Procedures for the provision of fair processing information, information on the data controller and purposes for processing the data need to be defined and implemented. This relies in part on identifying where personal info is in use.
14	Similar notification requirements to Article 13 apply if personal info is obtained indirectly (*e.g.* a commercial mailing list?): people must be informed within a month and on the first communication with them.	A.8.2.1 A.8.2.3 A.12.1.1 A.14.1 A.16 *etc.*	See Article 13.

Source: GDPR & ISO 27001 Mapping Table, ISO2K7 Forum, The British Assessment Bureau, 2016.

27001/2 Ref.	Control Area	Control requirement
A.8.2.1	Classification of information	Information should be classified taking into consideration legal requirements, value, criticality, and sensitivity as regards unauthorized disclosure and changes.
A.8.2.3	Handling of assets	Asset handling procedure should be consistent with information classification scheme of the Company.
A.12.1.1	Documented operating procedures	Operating procedures should be documented and available on a need to know/need to use basis.
A.14.1.1	Information security requirements analysis and specification	New systems or system enhancement's requirement should also include Information security requirements.
A.16	Information security incident management	Information security incident should be consistently and effectively managed in terms of responsibilities, incident detection/reporting and response procedures, etc.

แนวปฏิบัติเพื่อกำหนดข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

Individuals must be made aware of processing, purposes, risks, rules, safeguards and rights.

- Privacy notice should be concise, transparent, intelligible, easily accessible, using clear and plain language, provided in writing, or by other means, including, where appropriate, by electronic means free of charge, and may be provided orally if requested by the data subject
- Controllers must provide the following information to individuals when obtaining data from individuals and from third parties
  - Controller/representative identity/contact details
  - DPO identity/contact details
  - Processing purposes and legal basis
  - If processing based on legitimate interests, explanation of those interests
  - Categories of data obtained and source of the data in case not obtained directly
  - Recipients or categories of recipients
  - Information on cross-border transfers
  - Data retention periods
  - An individual's right, including rights to complain to DPA and to withdraw consent
  - Details of whether the provision of data mandatory
  - Details of existence of automated decision making, including profiling including logic behind it and consequences

Reference: Recital 39, Articles 12, 13 &14

แนวปฏิบัติเพื่อกำหนดข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

Easily accessible

Example

Every organisation that maintains a website should publish a privacy statement/ notice on the website. A direct link to this privacy statement/ notice should be clearly visible on each page of this website under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice"). Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.

For apps, the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app. One way to meet this requirement is to ensure that the information is never more than "two taps away" (e.g. by including a "Privacy"/ "Data Protection" option in the menu functionality of the app). Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public.

WP29 recommends as a best practice that at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided or that this information is made available on the same page on which the personal data is collected.

Source : Guidelines on transparency under Regulation 2016/679, Article 29 Working Party, 11 April 2018.

แนวปฏิบัติเพื่อกำหนดข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

Clear and plain language

Poor Practice Examples

The following phrases are not sufficiently clear as to the purposes of processing:

- *"We may use your personal data to develop new services"* (as it is unclear what the "services" are or how the data will help develop them);
- *"We may use your personal data for research purposes* (as it is unclear what kind of "research" this refers to); and
- *"We may use your personal data to offer personalised services"* (as it is unclear what the "personalisation" entails).

Good Practice Examples[14]

- *"We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in "* (it is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this);
- *"We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive"* (it is clear what type of data will be processed and the type of analysis which the controller is going to undertake); and
- *"We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read"* (it is clear what the personalisation entails and how the interests attributed to the data subject have been identified).

Source : Guidelines on transparency under Regulation 2016/679, Article 29 Working Party, 11 April 2018.

แนวปฏิบัติเพื่อกำหนดข้อมูลที่ต้องเปิดเผยแก่เจ้าของข้อมูล

1. **Assess and identify whether EU GDPR compliance required?**

2. **Conduct and/or update**
   - **a data inventory including affected systems**
   - **data classification**

3. **Review and update privacy policies and information notices.**

4. **Update and implement the business process or checklist and technology to ensure that the notice is given as required in due time**

5. **Review and/or update contracts with relevant partners who may collect data on the Company's behalf to agree on responsibility for notice review, update, approval**

6. **Conduct enterprise-wide awareness and training program**

Continuously monitor conformance

ช่องทางการติดต่อ

เพ็ญนภา พุกกะรัตน์

หุ้นส่วน บริษัท อีวาย คอร์ปอเรท เซอร์วิสเซส จำกัด

โทรศัพท์: +66 2264 9090 อีเมล: Pennapa.Pookkarat@th.ey.com

ดร. เยาวลักษณ์ ชาติบัญชาชัย

หุ้นส่วน บริษัท อีวาย คอร์ปอเรท เซอร์วิสเซส จำกัด

โทรศัพท์: +66 2264 9090 อีเมล: Yaowaluk.Chadbunchachai@th.ey.com

ขอบคุณ

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

ED None

ey.com