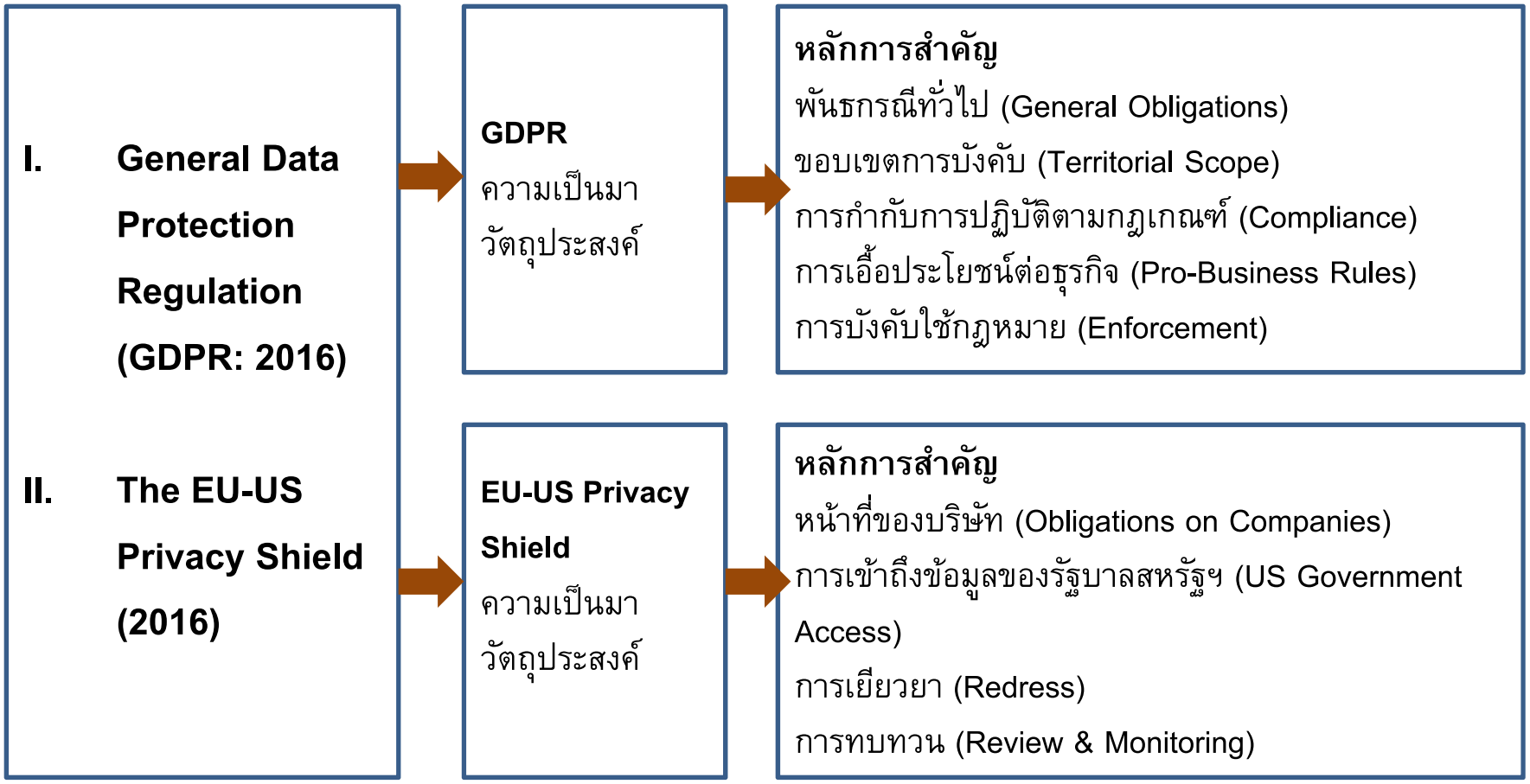
หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล: สหภาพยุโรป

ดร. ประพันธ์พงษ์ ขำอ่อน

สถาบันวิชาการนโยบายกิจการสาธารณะกับธุรกิจและการกำกับดูแล (APaR)

มหาวิทยาลัยหอการค้าไทย

Content


I. General Data Protection Regulation (GDPR: 2016)
II. The EU-US Privacy Shield (2016)
GDPR
ความเป็นมา
วัตถุประสงค์
EU-US Privacy Shield
ความเป็นมา
วัตถุประสงค์
หลักการสำคัญ
พันธกรณีทั่วไป (General Obligations)
ขอบเขตการบังคับ (Territorial Scope)
การกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance)
การเอื้อประโยชน์ต่อธุรกิจ (Pro-Business Rules)
การบังคับใช้กฎหมาย (Enforcement)
หลักการสำคัญ
หน้าที่ของบริษัท (Obligations on Companies)
การเข้าถึงข้อมูลของรัฐบาลสหรัฐฯ (US Government Access)
การเยียวยา (Redress)
การทบทวน (Review & Monitoring)

General Data Protection Regulation (GDPR: 2016)

General Data Protection Regulation 2016 (Regulation 2016/679)

แทนที่ Data Protection Directive 1995 (Directive 95/46/EC)

- EU Commission รับรองวันที่ 27 พฤษภาคม ค.ศ. 2016 แต่ยังไม่บังคับใช้กับประเทศสมาชิก EU จนกระทั่งเดือนพฤษภาคม ค.ศ. 2018

วัตถุประสงค์:

- ให้ประชาชนมีสิทธิควบคุมข้อมูลส่วนบุคคลของตน ซึ่งถือเป็นสิทธิขั้นพื้นฐาน

  GDPR Preamble (1): “The protection of natural persons in relation to the processing of personal data is a **fundamental right**. Article 8 (1) of the Charter of Fundamental Rights of the European Union …provide that everyone has the right to protection of personal data concerning him or her.”

- ให้สหภาพยุโรปมีมาตรฐานการคุ้มครองข้อมูลที่เป็นอันหนึ่งอันเดียวเพื่อให้เกิดการเคลื่อนย้ายโดยเสรีของข้อมูล

  GDPR Preamble (3):”…harmonise the protection of fundamental rights and freedom to ensure the **free flow of personal data** between Member States”

General Data Protection Regulation (GDPR: 2016)

พันธกรณีทั่วไป (General Obligations)

- **Free and Easy Access** ให้ประชาชนเข้าถึงข้อมูลส่วนบุคคลของตนได้ง่ายและไม่มีค่าใช้จ่าย
- **Notice and Collection** แจ้งให้ทราบถึงวัตถุประสงค์ ต้องมีความโปร่งใสในการรวบรวมข้อมูลส่วนบุคคล
- **Consent** เมื่อมีการนำข้อมูลไปประมวลผล จะต้องได้รับความยินยอมที่ชัดเจนจากเจ้าของข้อมูล (Clear and Affirmative Consent)
- **Uses of Personal Information** การใช้ข้อมูลควรเป็นไปตามวัตถุประสงค์ที่แจ้งเท่านั้น
- **Data protection by designs and by default** จัดให้มีระบบการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ขั้นแรกของการออกแบบบริการ และให้การตั้งค่าเป็นมิตรต่อการคุ้มครองข้อมูลส่วนบุคคล (Privacy-Friendly Setting)
- **Data Portability** ให้สิทธิประชาชนในการขอข้อมูลส่วนบุคคลของตนจากผู้ประกอบการเพื่อโอนข้อมูลนั้นไปยังผู้ประกอบการอื่นได้
- **Right to be Forgotten** ให้สิทธิเจ้าของข้อมูลส่วนบุคคลเรียกร้องให้มีการลบข้อมูลของตนออกจากระบบเมื่อไม่มีความจำเป็นที่ผู้ประกอบการจะต้องเก็บข้อมูลนั้นไว้ หรือเจ้าของข้อมูลไม่ประสงค์ให้นำข้อมูลดังกล่าวไปประมวลผลอีกต่อไป

General Data Protection Regulation (GDPR: 2016)

Right to be Forgotten

***Google v. AEPD and Gonzáles 2014* (ECJ Ruling C-131/12)**

ศาลยุโรป (European Court of Justice):

> "*Gonzáles* ขอศาลให้บริษัท Google ลบข้อมูลที่บ่งบอกว่า *Gonzáles* เป็นบุคคลที่อยู่ในกระบวนการพิจารณาล้มละลายซึ่งในปัจจุบันไม่เป็นความจริงอีกต่อไป
>
> บริษัท Google ในฐานะผู้ควบคุมข้อมูลมีหน้าที่ต้องลบข้อมูลส่วนบุคคลที่ไม่ถูกต้อง หรือไม่ครบถ้วนตามจริง (inaccurate, inadequate, irreverent or excessive) ถ้าหากข้อมูลส่วนบุคคลเช่นว่านั้นสามารถนำไปประมวลผลได้ เมื่อบริษัท Google เพิกเฉยต่อหน้าที่นี้ ถือว่าละเมิดกฎหมายสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล"

General Data Protection Regulation (GDPR: 2016)

ขอบเขตการบังคับ (Territorial Scope)

- **Established in EU** ประชาชนและธุรกิจที่จัดตั้งใน EU ได้รับการคุ้มครองข้อมูลส่วนบุคคลภายใต้กฎหมายนี้ไม่ว่าการประมวลผลข้อมูลนั้นจะเกิดขึ้นใน EU หรือนอก EU
- **Adequate Decisions for Data Transfer outside EU** ข้อมูลส่วนบุคคลจะโอนไปยังผู้ประกอบการนอกสหภาพยุโรปได้ก็ต่อเมื่อประเทศปลายทางมีระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเทียบเท่าสหภาพยุโรป

  Preamble (101): "**Transfer to third countries** and international organisations may only be carried out **with full compliance** with this Regulation…"

  Preamble (103): The Commission may decide with effects for the entire Union that a third country … offers an **adequate level** of data protection"
- **Expanded Territorial Reach** หากผู้ประมวลผลข้อมูลนอกยุโรปให้บริการหรือขายสินค้าให้กับผู้บริโภคชาวยุโรป หรือ "สังเกตพฤติกรรม" ของชาวยุโรป ผู้ประกอบการจะต้องตกอยู่ภายใต้บังคับของกฎหมายฉบับนี้ด้วย

  Art. 3 "a controller or processor **not established in EU** … where the processing activities are related to **the offering of goods and services …in the EU** or **monitoring of their behaviour**"

General Data Protection Regulation (GDPR: 2016)

การกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance):

- **Data Protection Risk Assessment** ธุรกิจที่มีความเสี่ยงสูง (High Risks) ต่อความปลอดภัยของข้อมูลส่วนบุคคล เช่นธุรกิจที่ใช้การประมวลผลข้อมูลระดับใหญ่ (Large Scale) หรือมีการใช้เทคโนโลยีในการประมวลผลแบบใหม่ จะต้องประเมินตนเองว่าธุรกิจของตนมีความเสี่ยงสูงต่อการละเมิดข้อมูลส่วนบุคคลหรือไม่
- **Prior Consultation with Data Protection Authority (DPA) if high risk** ธุรกิจมีหน้าที่ต้องปรึกษากับ DPA ถ้ามีการประเมินผลแล้วพบว่ามีความเสี่ยงต่อความปลอดภัยของข้อมูลส่วนบุคคล
- **Appoint Data Processing Officer (DPO) if high risk/large scale** ธุรกิจมีหน้าที่ต้องแต่งตั้ง DPO เพื่อมาช่วยธุรกิจที่มีความเสี่ยงสูงหรือประมวลผลข้อมูลระดับใหญ่ให้ดำเนินงานเป็นไปตามกฎหมาย
- **Notification of breach** ให้ผู้ประกอบการแจ้งหน่วยงานคุ้มครองผู้บริโภค (DPA) ภายใน 72 ชั่วโมงหลังจากข้อมูลส่วนบุคคลสูญหาย ถูกทำลาย หรือมีการเข้าถึงข้อมูลจากผู้ที่ไม่ได้รับอนุญาต
- **Role of Data Processor** กำหนดหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) เป็นการเฉพาะ เช่น หน้าที่จัดเก็บบันทึกกิจกรรมการประมวลผลข้อมูลที่ดำเนินการแทนผู้ควบคุมข้อมูล และหน้าที่การแจ้งให้ผู้ควบคุมข้อมูลทราบทันทีเมื่อมีการละเมิดข้อมูล เป็นต้น

General Data Protection Regulation (GDPR: 2016)

การเอื้อประโยชน์ต่อธุรกิจ (Pro-Business Rules):

- **Less notification obligations for low risk** ธุรกิจที่ประเมินตนเองแล้วว่าความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลต่ำมีภาระที่น้อยลงต่อ DPA แต่ธุรกิจที่ความเสี่ยงสูงหรือดำเนินการประมวลผลข้อมูลขนาดใหญ่มีหน้าที่ต้องแจ้งและรายงานต่อ DPA ในระดับที่มากกว่า
- **Encouraging codes of conduct** ส่งเสริมให้ธุรกิจทำ Code of Conduct ในเรื่อง Best Practices และ Guidelines ของการปฏิบัติตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (เช่น fair and transparency requirements, collection of data, notification etc.)
- **Binding Corporate Rules (BCRs)** เป็นหลักการที่ให้ธุรกิจในเครือ (Intra-Group Companies) ที่ประกอบธุรกิจทั้งในและนอกสหภาพยุโรป สามารถโอนข้อมูลส่วนบุคคลระหว่างกันได้โดยอิสระ และได้รับความคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายฉบับนี้ถึงแม้บริษัทในเครือบางแห่งจะประกอบธุรกิจในประเทศที่อยู่นอกสหภาพยุโรปก็ตาม

General Data Protection Regulation (GDPR: 2016)

การบังคับใช้ตามกฎหมาย (Enforcement):

- **Data Protection Authority (DPA)** ให้แต่งตั้งหน่วยงานคุ้มครองผู้บริโภคในประเทศสมาชิกซึ่งทำหน้าที่กำกับดูแลให้เป็นไปตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป และเป็นจุดตอบข้อซักถามของผู้ที่เกี่ยวข้อง (Single Point of Contact)
- **One-Stop-Shop Enforcement** สำหรับธุรกิจที่มีสถานประกอบการหลายแห่งในหลายประเทศสมาชิก ธุรกิจนั้นจะอยู่ภายใต้การกำกับดูแลของ DPA ในประเทศที่ธุรกิจนั้นมีสถานประกอบการหลัก (Main Base)

The US – EU Privacy Shield Framework Principles (2016)

ความเป็นมา:

***Maximillian Schrems v Data Protection Commissioner 2015* (ECJ C-362/14)**

- Schrems ในฐานะผู้ใช้บัญชี facebook เชื่อว่าข้อมูลที่เขาโพสต์ลงใน facebook ถูกโอนจากสำนักงานสาขาของ facebook ที่ประเทศไอร์แลนด์ไปยังผู้ให้บริการประมวลผลข้อมูลที่อยู่ในสหรัฐอเมริกา และถูกสอดแนมโดยสำนักงานความมั่นคงแห่งชาติสหรัฐอเมริกาและหน่วยงานข่าวกรองอื่นๆ ของสหรัฐอเมริกา

- Schrems กล่าวหาว่ากฎหมายและแนวปฏิบัติของสหรัฐอเมริกา Safe Habour Privacy Principles (2001) ไม่เพียงพอที่จะคุ้มครองประชาชน แต่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของยุโรปสั่งยกคำร้องโดยให้เหตุผลว่ามาตรการของอเมริกาคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอแล้ว

- ในปี ค.ศ. 2015 คดีขึ้นไปถึงศาล ECJ ซึ่งในที่สุดตัดสินให้ความตกลง Safe Habour เป็นโมฆะ และศาลยังมีความเห็นเพิ่มเติมว่าเนื่องจากความตกลง Safe Habour ดังกล่าวไม่ใช้บังคับกับการดำเนินการของหน่วยงานภาครัฐของสหรัฐอเมริกา

The US – EU Privacy Shield Framework Principles (2016)

The EU-US Privacy Shield Framework Principles (2016)

แทนที่ Safe Habour Privacy Principles (2000)

- หลังจาก Safe Habour เป็นโมฆะทั้งสหรัฐอเมริกาและสหภาพยุโรปจึงเจรจากรอบความคุ้มครองข้อมูลส่วนบุคคลระหว่างกันใหม่ภายใต้ความตกลงที่เรียกว่า US –EU Privacy shield Framework Principles (2016) ซึ่ง EU Commission รับรองเมื่อวันที่ 12 กรกฎาคม ค.ศ. 2016

วัตถุประสงค์:

- ส่งเสริมการการเคลื่อนย้ายข้อมูลส่วนบุคคลระหว่างสหภาพยุโรปและสหรัฐอเมริกาซึ่งเป็นปัจจัยสำคัญต่อการเจริญเติบโตของเศรษฐกิจยุโรป (Strong Transatlantic Business)
- หาทางคุ้มครองข้อมูลส่วนบุคคลจากกรอบกฎหมายที่มีความแตกต่างกัน

  US - mixed regulation and self-regulation

  EU – unified data protection rules
- มุ่งเน้นให้ผู้ประกอบการของสหรัฐอเมริกาที่รับข้อมูลส่วนบุคคลของยุโรปดำเนินการตามหลักการของ Privacy Shield Principles เพื่อให้ผ่านมาตรฐานการคุ้มครองข้อมูลของยุโรป

The US – EU Privacy Shield Framework Principles (2016)

The EU-US Privacy Shield Framework Principles (2016)

แทนที่ Safe Habour Privacy Principles (2000)

- EU จะอนุญาตให้มีการส่งข้อมูลแก่บริษัทของ US ที่อยู่ในบัญชี Privacy Shield ของ US Department of Commerce
- EU ออกประกาศรับรองหลักเกณฑ์ (Adequate Decisions) ของ Privacy Shield ว่ามีมาตรฐานเพียงพอ
- US Company ที่ประเมินตนเองว่าเข้ามาตรฐาน สามารถเข้าไปอยู่ในบัญชีของ US Department of Commerce เพื่อรับรองว่าบริษัทนั้นสามารถรับโอนข้อมูลส่วนบุคคลจาก EU ได้

The US – EU Privacy Shield Framework Principles (2016)

หลักการที่สำคัญ:

- **หน้าที่ของบริษัท (Obligations on Companies)** บริษัทต้องรับรองตัวเองว่าเข้ามาตรฐาน (Self-Certify) และปฏิบัติตามหลักการอื่นๆ (transparency, prompt reply to complaints, etc.)
- **การเข้าถึงข้อมูลของรัฐบาลสหรัฐฯ (US Government Access)** รัฐบาลของสหรัฐอเมริกาสามารถเข้าถึงข้อมูลส่วนบุคคลได้ภายใต้เงื่อนไขและวัตถุประสงค์ที่ระบุไว้โดยชัดแจ้งแล้วเท่านั้น เช่น เหตุผลเรื่องความมั่นคง
- **การเยียวยา (Redress)**
  - เจ้าของข้อมูลร้องเรียนโดยตรงกับบริษัท
  - การระงับข้อพิพาททางเลือก
  - ร้องเรียนกับ Data Protection Authority (DPA)
  - ร้องเรียนต่อผู้ตรวจการ (Ombudsman) ซึ่งมีหน้าที่การสืบสวนข้อเท็จจริงเพื่อเยียวยาความเสียหาย
  - Privacy Shield Panel (last resort) เพื่อบังคับให้เป็นไปตามคำตัดสิน
- **การทบทวน (Review & Monitoring)**
  - ทบทวนร่วมกันรายปี (Annual Joint Review)
  - เปิดโอกาสให้ภาคส่วนอื่นๆ แสดงความคิดเห็น (NGOs หรือผู้มีส่วนได้ส่วนเสียอื่น)

The End

More queries please contact:

Academy of Public Enterprise Policy, Business & Regulation (APaR)

School of Law

University of the Thai Chamber of Commerce

prapanpong_khu@utcc.ac.th

Tel +662 697 6805