ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ในการทำธุรกรรมทางอิเล็กทรอนิกส์

สำหรับการประชุมชี้แจง การจัดทำแนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

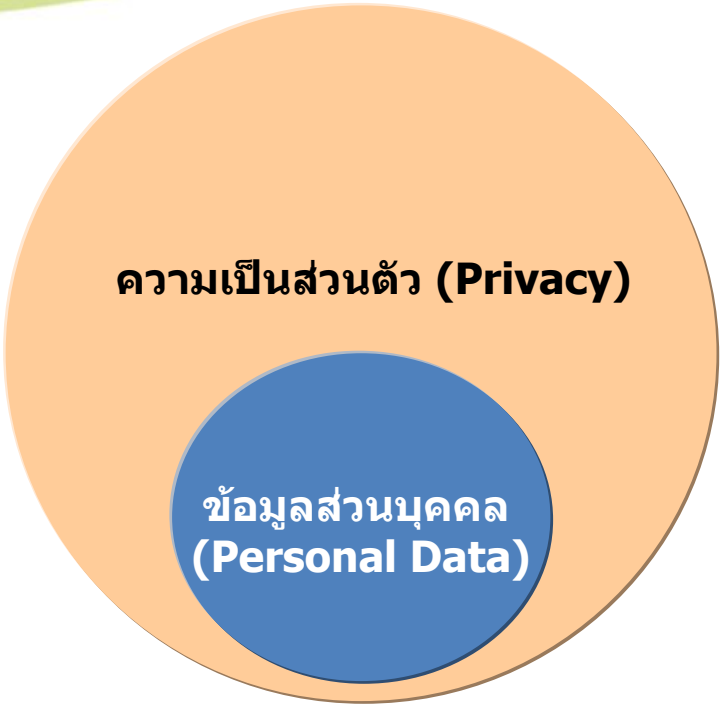
วันอังคารที่ 24 กันยายน 2556
เวลา 10.30-12.00 นาฬิกา
ณ ห้องแกรนด์ บอลรูม ชั้น 1 โรงแรมทีเค พาเลซ

นายจักรพงษ์ ชาวงษ์
ผู้อำนวยการกลุ่มงานกำกับดูแลธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

หัวข้อการนำเสนอ

1	ความเป็นส่วนตัว (Privacy)
2	รูปแบบการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy)
3	ความก้าวหน้าทางเทคโนโลยีกับการละเมิดข้อมูลส่วนบุคคล
4	ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล
5	ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์
	- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
	- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
	- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
6	การพัฒนาการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

ความเป็นส่วนตัว (Privacy)



ความเป็นส่วนตัว (Privacy)

เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์

1. ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy)
2. ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy)
3. ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy)
4. ความเป็นส่วนตัวในเคหสถาน (Territorial Privacy)

รูปแบบการคุ้มครองข้อมูลส่วนบุคคล

	รูปแบบ	ลักษณะ
1	บัญญัติเป็นกฎหมายทั่วไป	หลายประเทศ มีการบัญญัติกฎหมาย โดยเป็นกฎหมายที่วางหลักการทั่วไปครอบคลุมการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลทั้งของหน่วยงานภาครัฐและเอกชนและมีหน่วยงานกลางดูแล ให้มีการปฏิบัติตามกฎหมาย
2	บัญญัติเป็นกฎหมายคุ้มครองแต่ละเรื่องไว้โดยเฉพาะ	เป็นการบัญญัติกฎหมายที่วางหลักการให้คุ้มครองแต่ละเรื่องไว้เป็นการเฉพาะ เช่น ข้อมูลทางการเงิน
3	การกำกับดูแลตนเอง	กำหนดให้มีกลไกการกำกับดูแลตนเอง (Self-regulation) โดยการที่ผู้ประกอบการร่วมกันกำหนดหลักเกณฑ์ของตนขึ้น และดูแลให้มีการปฏิบัติตามกันเอง โดยไม่มีหน่วยงานกลางกำกับดูแล

ความก้าวหน้าทางเทคโนโลยีกับการละเมิดข้อมูลส่วนบุคคล

เหตุผลและปัจจัยที่ทำให้ข้อมูลต่างๆ ถูกทำให้อยู่ในรูปของอิเล็กทรอนิกส์มากขึ้น

1. **การสร้าง ส่ง หรือเก็บข้อมูล** สามารถทำได้ง่ายและสะดวก
2. การเก็บข้อมูลในรูปของอิเล็กทรอนิกส์ ทำให้เกิดการ**ลดต้นทุนทางธุรกิจ**ในการสร้าง ส่ง หรือเก็บข้อมูล
3. **การก้าวเข้าสู่ยุคสังคมสารสนเทศ** ทำให้ข้อมูลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์มีความสำคัญสามารถซื้อขายหรือทำธุรกรรมใดๆ ได้
4. **คุณสมบัติของโครงสร้างพื้นฐานสารสนเทศ (คอมพิวเตอร์และเครือข่าย)** ที่รองรับการทำธุรกรรมทางอิเล็กทรอนิกส์มากขึ้น เช่น การนำ IT มาประยุกต์ในการใช้งานมากขึ้น

การเก็บรวบรวมข้อมูลส่วนบุคคลเก็บข้อมูล เพื่อประโยชน์ในกิจกรรมของนิติบุคคลหรือการให้บริการของรัฐ

การใช้งานข้อมูลส่วนบุคคลในปัจจุบัน

ข้อมูลส่วนบุคคล

ประวัติการทำงาน

ข้อมูลสินเชื่อ

ข้อมูลการเงิน/การธนาคาร

ประวัติบุคคล

ข้อมูลทะเบียนราษฎร์

ข้อมูลผู้สมัครสมาชิก

การให้ความสำคัญ

การคุ้มครอง/ดูแล

ข้อมูลการใช้บริการ

ข้อมูลทรัพย์สิน

ประวัติครอบครัว

ข้อมูลลูกจ้าง

ข้อมูลภาษี

ข้อมูลเงินเดือน

ประวัติการรักษาพยาบาล

ข้อมูลลูกค้า

ข้อมูลคดี /อาชญากรรม

ข้อมูลประกันสังคม

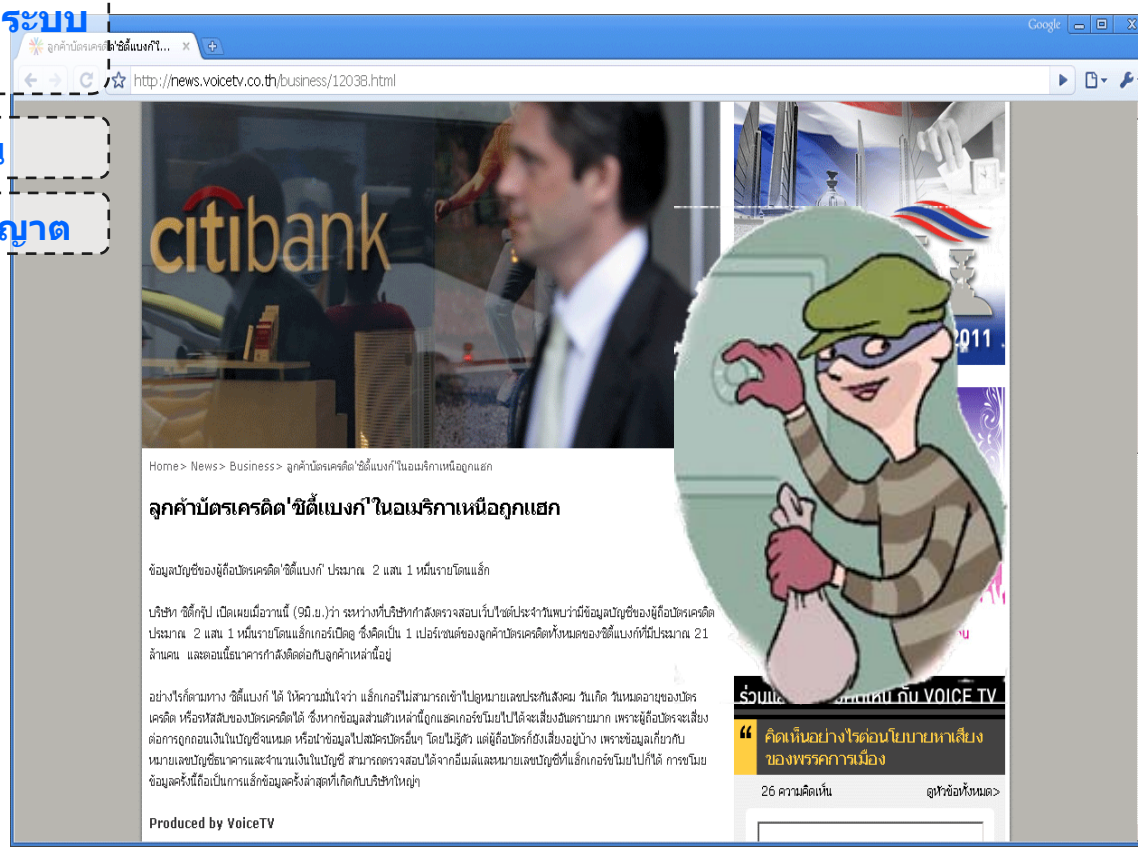
ข้อมูลบัตรเดบิต/เครดิต

ข้อมูลการล้มละลาย

การใช้งานข้อมูลส่วนบุคคลในปัจจุบัน

ความก้าวหน้าทางเทคโนโลยีกับการละเมิดข้อมูลส่วนบุคคล

- เผยแพร่อีเมล์ของผู้ใช้บริการโดยไม่ได้ตั้งใจ
- ส่งต่อข้อมูลให้บุคคลที่สาม
- การขโมยข้อมูลจากความบกพร่องของระบบความปลอดภัย
- การใช้ข้อมูลส่วนตัวเพื่อกลั่นแกล้งผู้อื่น
- การส่งต่อภาพถ่ายส่วนตัวโดยไม่ได้รับอนุญาต



ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล

แนวทางการคุ้มครองข้อมูลส่วนบุคคลในองค์การระหว่างประเทศ

Organization for Economic Cooperation and Development (OECD)
องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา

Guidelines on the Protection or Privacy and Transborder flows of Personal Data

European Union (EU)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

United Nations (UN)

Guidelines concerning computerized personal data files

1. หลักข้อจำกัดในการเก็บรวบรวมข้อมูล

2. หลักคุณภาพของข้อมูล

3. หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ

4. หลักข้อจำกัดในการนำไปใช้

5. หลักการรักษาความมั่นคงปลอดภัยข้อมูล

6. หลักการเปิดเผยข้อมูล

7. หลักการมีส่วนร่วมของบุคคล

8. หลักความรับผิดชอบ

การคุ้มครองข้อมูลส่วนบุคคลในข้อตกลงระหว่างประเทศ

- แนวทางของ OECD
- ข้อบังคับ EU
- แนวทางของ UN

กำหนดหลักการปฏิบัติมาตรฐานสากลเกี่ยวกับข้อมูลส่วนบุคคล

- การเก็บ
- ประมวลผล
- ส่งข้อมูล

- หลักข้อจำกัดในการเก็บ
- หลักการกำหนดวัตถุประสงค์
- หลักคุณภาพ
- หลักการรักษาความปลอดภัย
- หลักความยินยอม
- หลักการห้ามเก็บข้อมูลที่มีความอ่อนไหว
- หลักการส่งข้อมูลข้ามแดน

กฎหมายไทยที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

1	รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550
2	ประมวลกฎหมายแพ่งและพาณิชย์ / ประมวลกฎหมายอาญา
3	พระราชบัญญัติการทะเบียนราษฎร พ.ศ. 2534
4	พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535
5	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
6	พระราชบัญญัติการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ. 2545
7	พระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546
8	ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม พ.ศ. 2549
9	พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
	- ประกาศคณะกรรมการธุรกรรมฯ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
10	พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550
11	ร่าง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....
..	...

คำนิยาม “ข้อมูลส่วนบุคคล”

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550	มาตรา 4 ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาคของบุคคลย่อมได้รับความคุ้มครอง มาตรา 35 สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครองการกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ **บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ**
พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540	“**ข้อมูลข่าวสารส่วนบุคคล**” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่ายและให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย
ร่าง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.	“**ข้อมูลส่วนบุคคล**” หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย
ประกาศ กทช เรื่องมาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคลฯ	“**ข้อมูลส่วนบุคคล**” หมายความว่า ข้อมูลผู้ใช้เลขหมายโทรคมนาคม ข้อเท็จจริง รายละเอียดเกี่ยวกับผู้ใช้บริการที่สามารถระบุตัวผู้ใช้บริการหรืออาจระบุตัวผู้ใช้บริการนั้นได้ไม่ว่าทางตรงหรือทางอ้อม ข้อมูลการใช้บริการ เลขหมายโทรคมนาคม รวมทั้งพฤติกรรมการใช้บริการโทรคมนาคมของผู้ใช้บริการ แต่ไม่รวมถึงข้อมูลทางเทคนิคที่ใช้เท่าที่จำเป็น เพื่อประโยชน์ในการบริหารโครงข่ายโทรคมนาคม เพื่อประโยชน์ในการติดต่อสื่อสาร และเพื่อประโยชน์ในการดำเนินธุรกิจในภาพรวมของผู้รับใบอนุญาต

คำนิยาม "ข้อมูลส่วนบุคคล"

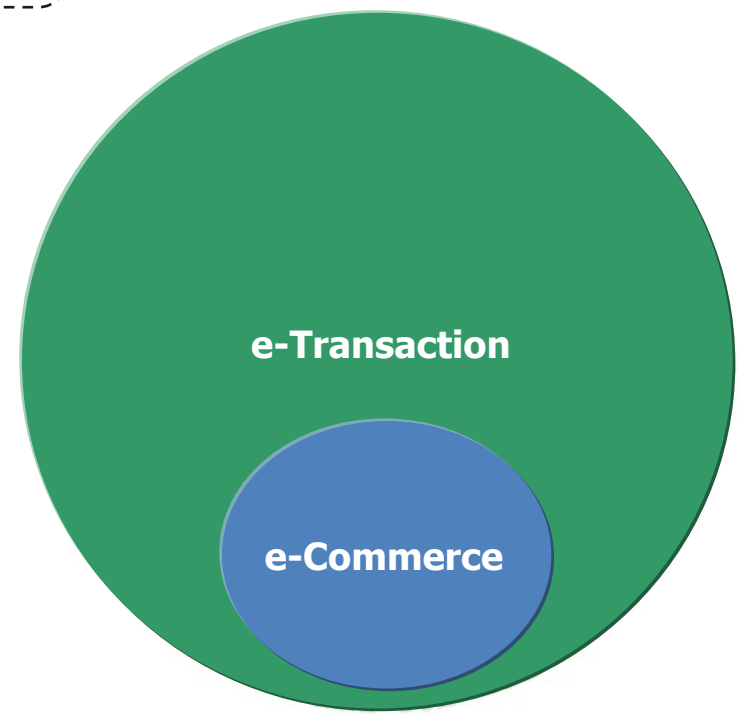
พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545	"**ข้อมูล**" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงของข้อมูลเครดิตไม่ว่าการสื่อความหมายนั้นจะทำโดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิลม์ การบันทึกภาพ หรือเสียง การบันทึกโดยคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งบันทึกไว้ปรากฏได้
พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549	ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่**ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม** ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย
OECD Guidelines on the Protection or Privacy and Transborder flows of Personal Data	"**personal data**" means any information relating to an identified or identifiable individual (data subject) "**ข้อมูลส่วนบุคคล**" หมายถึง ข้อความใดๆ อันระบุตัว หรืออาจระบุตัวบุคคลได้
EU Directive 95/46/EC of the European Parliament and of the Council	"**personal data**" shall means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; "**ข้อมูลส่วนบุคคล**" หมายความว่า ข้อความใดๆ ที่เกี่ยวกับบุคคลธรรมดาอันระบุตัวหรืออาจระบุตัวบุคคลนั้นได้ ซึ่งบุคคลที่อาจถูกระบุตัวได้ไม่ว่าโดยตรงหรือโดยอ้อมนี้อาจทำได้โดยการอ้างอิงจากหมายเลขเฉพาะของบุคคล (Identification number) หรือจากปัจจัยอื่นๆ ที่มีลักษณะเฉพาะในทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจ เอกลักษณ์ทางวัฒนธรรมและสังคมของบุคคลนั้น

ลักษณะทั่วไปของการทำธุรกรรมทางอิเล็กทรอนิกส์

e-Commerce

การพาณิชย์อิเล็กทรอนิกส์ เป็นการซื้อขายสินค้าหรือบริการ โดยส่งข้อมูลด้วยสื่ออิเล็กทรอนิกส์ผ่านทางเครือข่าย เช่น โทรศัพท์ คอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต

B2B	การทำธุรกรรมระหว่างธุรกิจด้วยกันเอง เช่น การจัดระบบการสั่งซื้อวัตถุดิบและชิ้นส่วนระหว่างคู่ค้า
B2C	การทำธุรกรรมระหว่างพ่อค้าและผู้บริโภค เช่น การขายหนังสือหรือเพลง ผ่านอินเทอร์เน็ต
C2C	การทำธุรกรรมระหว่างผู้บริโภคด้วยกันเอง เช่น การขายสินค้ามือสอง หรือสินค้าฝากขาย
G2B	การทำธุรกรรมระหว่างภาครัฐและเอกชน เช่น การจัดซื้อจัดจ้างของภาครัฐที่ใช้สื่ออิเล็กทรอนิกส์



e-Transaction

ธุรกรรมทางอิเล็กทรอนิกส์ เป็นการทำกิจกรรมที่กระทำโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน เช่น การซื้อขายสินค้าทางอินเทอร์เน็ต การสมัครสมาชิกผ่านระบบออนไลน์ การตกลงทำสัญญาซื้อขายบนเครือข่าย เป็นต้น

การทำธุรกรรมทางอิเล็กทรอนิกส์และ ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

บริการอิเล็กทรอนิกส์ (e-Service) เป็นรูปแบบหนึ่งของการพาณิชย์เล็กทรอนิกส์ที่นำมาประยุกต์ใช้สำหรับให้บริการผ่านสื่ออิเล็กทรอนิกส์ในธุรกิจด้านต่าง ๆ ทั้งนี้เพื่อความสะดวกแก่ลูกค้า สมาชิก หรือแม้แต่พนักงานในองค์กรเอง

ตัวอย่าง

การบริการธนาคารอิเล็กทรอนิกส์ (Electronic Banking Service) ธนาคารที่เปิดดำเนินการธุรกรรม (ให้ผู้ใช้บริการสามารถทำธุรกรรมได้ผ่านระบบอิเล็กทรอนิกส์) เช่น

- การถอนเงินสดจากตู้ ATM
- การตรวจสอบยอดคงเหลือ
- การปรับสมุดบัญชี
- การตรวจสอบรายการทางการเงิน
- การโอนเงิน / การชำระค่าสินค้า
- Internet Banking
- Mobile Banking

รัฐบาลอิเล็กทรอนิกส์ (e-Government) เป็นวิธีการบริหารจัดการภาครัฐสมัยใหม่ โดยการใช้เทคโนโลยีคอมพิวเตอร์และเครือข่ายสื่อสาร เพื่อเพิ่มประสิทธิภาพการดำเนินงานภาครัฐ

กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

1. การทำธุรกรรมในปัจจุบันมีแนวโน้มที่จะปรับเปลี่ยนวิธีการในการติดต่อสื่อสารที่อาศัยการพัฒนา ICT ที่มีความสะดวก รวดเร็ว และมีประสิทธิภาพ
2. <u>การทำธุรกรรมทางอิเล็กทรอนิกส์มีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่</u>
   - ข้อกำหนดเกี่ยวกับการทำเป็นหนังสือ
   - ข้อกำหนดเกี่ยวกับการมีหลักฐานเป็นหนังสือ
   - ข้อกำหนดเกี่ยวกับลายมือชื่อ
   - ข้อกำหนดเกี่ยวกับเอกสารต้นฉบับ
   - ข้อกำหนดเกี่ยวกับการนำสืบพยานหลักฐาน
3. ทำให้ต้องมี**การรองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอกับ**
   - **การทำเป็นหนังสือ หรือมีหลักฐานเป็นหนังสือ**
   - **การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์**
   - **การใช้ลายชื่อ**
   - **การรับฟังพยานหลักฐาน**
4. เพื่อเป็น**การส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลในทางกฎหมาย** เช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม

กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
Electronic Transactions Act B.E. 2544 (A.D. 2001)

ผลบังคับใช้ 3 เมษายน 2545

เจตนารมณ์ เพื่อรองรับผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์

แนวทางการตรากฎหมาย

- UNCITRAL Model Law on Electronic Commerce 1996
- UNCITRAL Model Law on Electronic Signature 2001

ขอบเขตการบังคับใช้

ภาคเอกชน

ครอบคลุมทั้งหมดที่เป็นธุรกรรมในทางแพ่งและพาณิชย์ ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ (B2B, B2C และ C2C) ยกเว้นนิติกรรมเฉพาะตัว (ครอบครัว และ มรดก)

ภาครัฐ

- **ใช้บังคับแก่กิจกรรมภาครัฐ G2B G2Cและ G2G**
- พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
- องค์กรที่มีกฎหมายจัดตั้งเป็นการเฉพาะ

การบังคับใช้กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

รองรับผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์ให้สามารถใช้เป็นพยานหลักฐานในศาล

พ.ร.ฎ. กำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับ พ.ศ. 2549 (ม.3)

- ธุรกรรมเกี่ยวกับครอบครัว
- ธุรกรรมเกี่ยวกับมรดก

พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 (ม.35)

หน่วยงานของรัฐที่ทำธุรกรรมฯ ต้อง
- กำหนดคุณลักษณะของระบบเอกสารอิเล็กทรอนิกส์
- จัดทำแนวนโยบายและแนวปฏิบัติ Security
- จัดทำแนวนโยบายและแนวปฏิบัติ Data Privacy (ถ้ามี)

พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 (ม.32)

ผู้ประกอบธุรกิจ e-Payment จะถูกกำกับใน 3 รูปแบบ
- แบบแจ้งให้ทราบ
- แบบขึ้นทะเบียน
- แบบขอรับใบอนุญาต

พ.ร.ฎ. ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 (ม.25)

- กำหนดประเภทของธุรกรรมทางอิเล็กทรอนิกส์
- หลักเกณฑ์มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในแต่ละระดับ (พื้นฐาน กลาง เคร่งครัด)
- หน่วยงาน โครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure) ต้องปฏิบัติตามมาตรฐาน ด้านความมั่นคงปลอดภัยโดยเคร่งครัด

ร่าง พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจการให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ พ.ศ. .... (ม.32)

ผู้ประกอบธุรกิจ CA จะต้องถูกกำกับใน 2 รูปแบบ
-แจ้งให้ทราบ
-ขอใบอนุญาต

ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ในการทำธุรกรรมทางอิเล็กทรอนิกส์

คงเป็นเรื่องที่ไม่ดีแน่ ถ้าข้อมูลส่วนบุคคลของผู้ใช้บริการ ซึ่งให้ไว้กับหน่วยงานภาครัฐ ถูกเผยแพร่ โดยที่ผู้ใช้บริการไม่อนุญาต ข้อมูลส่วนบุคคลนี้ไม่ใช่เพียงแค่หมายเลขบัตรเครดิตเท่านั้น แต่ยังรวมไปถึง ชื่อ-ชื่อสกุล ที่อยู่ เบอร์โทรศัพท์ โทรสาร อีเมล์ เป็นต้น

ซึ่งผู้ที่ดูแลเว็บไซต์ที่ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ จะต้องจัดให้มีกลไกหรือระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่ให้บริการ ที่เชื่อถือได้ว่าข้อมูลส่วนบุคคลเหล่านี้ จะไม่ถูกลักลอบนำออกไปจากระบบได้ รวมถึงมีแนวปฏิบัติที่คุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการด้วย

การคุ้มครองข้อมูลส่วนบุคคล ในการดำเนินงานของรัฐ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

มีผลต่อความชอบด้วยกฎหมายของ

การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

Privacy & Security

การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

ที่มา

มาตรา 3 วรรคสาม ของ พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้กำหนดให้ "พระราชบัญญัตินี้ใช้บังคับแก่ธุรกรรมในการดำเนินงานของรัฐตามที่กำหนดในหมวด 4 ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ"

และบทบัญญัติมาตรา 35 แห่ง พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ได้กำหนดให้การทำ

(1) (2) (3) (4) (5) (6)

"คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ

(7)

หรือการดำเนินการใดๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ

ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด" ทั้งนี้ในพระราชกฤษฎีกาอาจกำหนดให้บุคคลที่เกี่ยวข้องต้องกระทำหรืองดเว้นการกระทำใดๆ หรือให้หน่วยงานของรัฐออกระเบียบเพื่อกำหนดรายละเอียดในบางกรณีด้วยก็ได้

การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

ความหมายของมาตรา 35 ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

หากในการดำเนินการกับภาครัฐในเรื่องใด มีข้อกำหนดในกฎหมายบางประการที่ต้องปฏิบัติโดยใช้วิธีการแบบดั้งเดิม (ใช้เอกสารกระดาษ) การดำเนินการนั้นก็สามารถใช้ข้อมูลอิเล็กทรอนิกส์ได้ โดยถือว่าได้ปฏิบัติตามข้อกำหนดในกฎหมายนั้นแล้ว (โดยไม่จำเป็นต้องไปแก้ไขกฎหมายนั้นๆ)

-การแจ้งย้ายที่อยู่
-การขอแก้ไขรายการในเอกสารทะเบียนราษฎร์
-การขอคัดหรือรับรองสำเนาทะเบียนบ้าน
-การเสียภาษีบำรุงท้องที่
-การขออนุญาตเกี่ยวกับการโฆษณา
-การขอทำตั๋วพิมพ์รูปพรรณสัตว์พาหนะ
-การขออนุญาตฆ่าสัตว์ (ต่อเทศบาลตำบล)
-การเสียภาษีเงินได้ (บุคคลธรรมดา)
-การขออนุญาตตั้งโรงงาน
-การขอจดทะเบียนเรือไทย
-การขออนุญาตค้าขายสุรา, บุหรี่
-การขอจดทะเบียนการค้า
-การยื่นแบบส่งเงินสมทบประกันสังคม
-การยื่นแบบนำเข้า-ส่งออก

แต่มีเงื่อนไขว่า

- ต้องมีการใช้ข้อมูลอิเล็กทรอนิกส์แทนวิธีการดั้งเดิม โดยทำตามหลักเกณฑ์ที่กำหนดในพระราชกฤษฎีกา

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ เนื่องจากประเทศไทยได้เริ่มเข้าสู่ยุคสังคมสารสนเทศซึ่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น สมควรสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตนโดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับให้หน่วยงานของรัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์

การบังคับใช้กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

สาระสำคัญ ของพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549

มาตรา 3 การทำระบบเอกสารในรูปข้อมูลอิเล็กทรอนิกส์

(1) รูปแบบที่เหมาะสมของเอกสาร (เพื่อให้เป็นไปในแนวทางเดียวกัน)

(2) กำหนดระยะเวลาเริ่มต้น & สิ้นสุด (เพื่อประโยชน์...ผลของสัญญา สิทธิ หน้าที่ ดอกเบี้ย การสิ้นสุดของสัญญา อายุความ)

(3) วิธีการระบุตัวบุคคล & ลายมือชื่ออิเล็กทรอนิกส์ (เพื่อประโยชน์...ผลผูกพันทางกฎหมาย)

(4) การตอบแจ้งการรับเพื่อประโยชน์ (เพื่อความชัดเจน & ลดข้อโต้แย้งเรื่องการส่ง & รับ)

มาตรา 5 การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย อย่างน้อย ดังนี้

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(2) การจัดให้มีระบบสารสนเทศ การสำรองข้อมูล & สภาพพร้อมใช้งาน & ทำแผนฉุกเฉิน

(3) การตรวจสอบ & ประเมินความเสี่ยงอย่างสม่ำเสมอ

มาตรา 6 การคุ้มครองข้อมูลส่วนบุคคล

ในกรณีหน่วยงานของรัฐมีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลด้วย

การบังคับใช้กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 6 การคุ้มครองข้อมูลส่วนบุคคล

8 หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

1. หลักข้อจำกัดในการเก็บรวบรวมข้อมูล
2. หลักคุณภาพของข้อมูล
3. หลักการกำหนดวัตถุประสงค์ในการเก็บรวบรวม
4. หลักข้อจำกัดในการนำไปใช้
5. หลักการรักษาความมั่นคงปลอดภัยข้อมูล
6. หลักการเปิดเผยข้อมูล
7. หลักการมีส่วนร่วมของเจ้าของข้อมูล
8. หลักความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางของ OECD

แนวนโยบายและแนวปฏิบัติ Data Privacy

หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

1. หลักข้อจำกัดในการเก็บรวบรวมข้อมูล

ในการจัดเก็บข้อมูลส่วนบุคคล ข้อมูลที่จัดเก็บจะต้องมีขอบเขตจำกัด โดยวิธีการที่ถูกต้องและชอบด้วยกฎหมาย โดยต้องให้บุคคลผู้เป็นเจ้าของข้อมูลรับทราบและยินยอมในการจัดเก็บข้อมูลนั้น

2. หลักคุณภาพของข้อมูล

ข้อมูลส่วนบุคคลที่จัดเก็บให้เป็นไปตามอำนาจหน้าที่ และเป็นข้อมูลที่มีความเกี่ยวข้องกับวัตถุประสงค์ในการใช้ โดยต้องเป็นข้อมูลที่ถูกต้องสมบูรณ์ และปรับปรุงให้ตรงตามความเป็นจริงอยู่เสมอ

หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

3. หลักการกำหนดวัตถุประสงค์ในการเก็บรวบรวม

ต้องมีการกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคลก่อนที่จะมีการจัดเก็บข้อมูลส่วนบุคคลนั้น

4. หลักข้อจำกัดในการนำไปใช้

การใช้ข้อมูลจะกระทำโดยขัดต่อวัตถุประสงค์ในการจัดเก็บมิได้ เว้นแต่
1. ได้รับความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล
2. ได้รับอนุญาตตามเงื่อนไขที่กฎหมายกำหนด

หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

5. หลักการรักษาความมั่นคงปลอดภัย

ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการจัดเก็บข้อมูลเพื่อป้องกันความเสี่ยง การสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

6. หลักการเปิดเผยข้อมูล

ต้องกำหนดวิธีการทั่วไปในการเปิดเผยข้อมูล รูปแบบของการเปิดเผยข้อมูล หลักเกณฑ์ในการขอให้มีการเปิดเผยข้อมูล ซึ่งต้องไม่กระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูล

หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

7. หลักการมีส่วนร่วมของเจ้าของข้อมูล

กำหนดให้เจ้าของข้อมูลมีสิทธิ
1. ได้รับการแจ้งว่ามีข้อมูลของตนจัดเก็บอยู่
2. ตรวจสอบข้อมูลของตนที่ถูกจัดเก็บ
3. ขอให้แก้ไขข้อมูลที่ไม่ถูกต้อง
4. ปฏิเสธในการจัดเก็บข้อมูลของตน

8. หลักการรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

กำหนดความรับผิดชอบในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล

การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

ม.35

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

หน่วยงานของรัฐต้องปฏิบัติตามหลักเกณฑ์ขั้นต่ำที่กำหนด

1. คุณลักษณะของเอกสารในรูปข้อมูลอิเล็กทรอนิกส์
   - 1.1 เลือกรูปแบบเอกสารอิเล็กทรอนิกส์ที่เหมาะสม
   - 1.2 เลือกลายมือชื่อที่ใช้
   - 1.3 กำหนดเรื่องเวลา
   - 1.4 ตอบแจ้งการรับ
2. จัดทำ
   - 2.1 แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
   - 2.2 แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัย เชื่อถือได้ และมีผลตามกฎหมาย

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

ประกาศในราชกิจจานุเบกษา

เมื่อวันที่ 1 พฤศจิกายน 2553 และมีผลบังคับใช้ตั้งแต่วันที่ 2 พฤศจิกายน 2553

สาระสำคัญ / ขอบเขตการบังคับใช้

ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ หากมีการรวบรวม จัดเก็บ ใช้หรือเผยแพร่ข้อมูลส่วนบุคคลในรูปของข้อมูลอิเล็กทรอนิกส์ ประกาศดังกล่าว เป็นแนวทางเบื้องต้นให้หน่วยงานรัฐใช้ในการกำหนดนโยบายและข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล โดยมีสาระสำคัญตามที่ประกาศฉบับนี้กำหนด

1. การประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการอัตโนมัติ (electronic or automatic)
2. ใช้บังคับกับหน่วยงานของรัฐที่มีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

จุดมุ่งหมายของประกาศ

เพื่อเป็นข้อกำหนดในการปฏิบัติที่สามารถสร้างผลลัพธ์ในทิศทางที่สอดคล้องกันภายใต้กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กล่าวคือ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัย ความน่าเชื่อถือ และมีการคุ้มครองข้อมูลส่วนบุคคล

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

บทเกริ่นนำ

ข้อ 1 กำหนดให้หน่วยงานของรัฐที่มีการรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์จัดทำ**นโยบาย**ดังกล่าว โดย<u>มีสาระสำคัญ</u>

(1) การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

(2) คุณภาพของข้อมูลส่วนบุคคล

(3) การระบุวัตถุประสงค์ในการเก็บรวบรวม

(4) ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

(5) การรักษาความมั่นคงปลอดภัย

(6) การเปิดเผยเกี่ยวกับการดำเนินการแนวปฏิบัติและแนวนโยบายเกี่ยวกับข้อมูลส่วนบุคคล

(7) การมีส่วนร่วมของเจ้าของข้อมูล

(8) หลักความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

ข้อ 2 กำหนดให้มี**ข้อปฏิบัติ**ในการคุ้มครองส่วนบุคคลของผู้ใช้บริการ โดยมีรายการอย่างน้อยดังนี้

(1) ข้อมูลเบื้องต้น

(2) การเก็บรวบรวมข้อมูลส่วนบุคคล

(3) การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น

(4) การรวบรวมข้อมูลจากที่มาหลายๆ แห่ง

(5) การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

(6) การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

(7) การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

(8) การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

(9) การติดต่อกับเว็บไซต์

การพัฒนาการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

ประเด็นพิจารณาในการคุ้มครองข้อมูลส่วนบุคคล

การพิจารณากำหนดประเภทของข้อมูล

- ข้อมูลธรรมดาทั่วไป เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ อายุ เพศ การศึกษา ฯลฯ
- ข้อมูลห้ามประมวลผล หรือ ข้อมูลห้ามจัดเก็บ หรือข้อมูลลับ เช่น เชื้อชาติ เผ่าพันธุ์ ความเชื่อทางศาสนา ความคิดเห็นทางการเมือง

การพิจารณา ใครคือ Data Subject

เจ้าของข้อมูล

?

บุคคลผู้มีหน้าที่รวบรวมข้อมูลและประมวลผลข้อมูล

?

ผู้ที่มีข้อมูลของเจ้าของข้อมูล

การพิจารณา การประมวลผลข้อมูล

- ครอบคลุมกิจกรรมทุกอย่างที่เกี่ยวข้องกับข้อมูล หรือ
- ระบุเฉพาะกิจการบางอย่าง เช่น การรวบรวม การจัดเก็บ การใช้ หรือการเปิดเผยข้อมูล

ประเด็นปัญหาในการคุ้มครองข้อมูลส่วนบุคคล

ปัญหาในการเก็บรวบรวมข้อมูล

- การเก็บรักษาความลับข้อมูล
- การยินยอมของผู้ให้ข้อมูล
- การรับรู้ของผู้ให้ข้อมูลต่อการมีอยู่ของฐานข้อมูล
- การรับรู้ของผู้ให้ข้อมูลต่อการใช้ฐานข้อมูล

ปัญหาของระบบการจัดเก็บข้อมูล

- ความปลอดภัยของระบบการจัดเก็บฐานข้อมูล
- การเข้าไปในฐานข้อมูลโดยไม่ได้รับอนุญาต

ปัญหาการใช้ฐานข้อมูล

- ข้อมูลที่ไม่ถูกต้องหรือมีความผิดพลาด
- ความเกี่ยวข้องของข้อมูล
- ความยินยอมของผู้ให้ข้อมูลต่อการใช้ข้อมูลดังกล่าว
- การรับรู้ของผู้ให้ข้อมูลต่อการใช้ข้อมูล

ปัญหาในการส่งผ่านข้อมูล

- การเชื่อมโยงฐานข้อมูลที่ต่างกัน
- การรวมข้อมูลและการวิเคราะห์ฐานข้อมูล
- การส่งข้อมูลข้ามประเทศ

การจัดทำนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

ประเด็นการพิจารณา

นิยาม ขอบเขตของคำว่า “ข้อมูลส่วนบุคคล” ตามประกาศคณะกรรมการฯ

- ไม่ได้กำหนดชัดเจน

- แต่กำหนดในหลักการไว้ในมาตรา 6 ของพระราชกฤษฎีกาฯ ดังนี้

“มาตรา 6 ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม”

<u>ข้อสังเกตเพิ่มเติม</u>

สิ่งที่ระบุ หรืออาจระบุตัวบุคคล

การจัดทำนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

ประเด็นการพิจารณา

ขอบเขตของคำว่า

- การเก็บข้อมูลส่วนบุคคล
- การเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆ

<u>การเก็บข้อมูลส่วนบุคคล</u>

- ข้อมูลตามทะเบียนราษฎร์ทั่วไป
  - คำนำหน้านาม
  - ชื่อ นามสกุล
  - วันเดือนปีเกิด
  - สถานที่เกิด
- ข้อมูลเพิ่มเติมเฉพาะของหน่วยงาน
  - สถานที่/ที่อยู่จริงที่ติดต่อได้
  - หมายเลขโทรศัพท์ และโทรศัพท์มือถือ
  - บุคคลที่ใกล้ชิด ติดต่อได้ในกรณีฉุกเฉิน
- ข้อมูลทางชีวภาพ (biometric data) (ถ้ามี)

<u>การเชื่อมโยงข้อมูลกับหน่วยงานราชการอื่นๆ</u>

- การเชื่อมโยงในฐานะผู้ขอใช้ข้อมูล
  - การเชื่อมโยงข้อมูลทะเบียนราษฎร์ (บัตรประชาชน ทะเบียนบ้าน) จากกรมการปกครอง มีการทำ MOU
- การเชื่อมโยงในฐานะผู้ให้ข้อมูล
  - การเชื่อมโยงให้ข้อมูลกับหน่วยงานอื่น มีการลงนามใน MOU ระหว่างกัน การส่งผ่านข้อมูล

<u>แนวปฏิบัติ</u>

- การลงทะเบียนผู้ใช้งาน
- การควบคุม และการจำกัดสิทธิของผู้ใช้งานอย่างจำกัดและเหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคล
- กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

การจัดทำนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

ประเด็นการพิจารณา

แนวปฏิบัติ ข้อ 2 (6) : ข้อมูลที่เก็บเป็นข้อมูลที่ต้องให้เลือกได้ว่า “จะให้หรือไม่ให้” ก็ได้

ตัวอย่าง : Opt-in Opt-out

Opt-in หมายถึง การสื่อสารไปยังผู้บริโภคหรือผู้รับ โดยที่ผู้บริโภคอนุญาตให้ติดต่อ เช่น การส่งด้วยสื่อโฆษณาอีเมลที่ผู้รับลงทะเบียนเอง เป็นต้น

Opt-out จะหมายความตรงกันข้ามกับ Opt-in

กล่าวคือ Opt-out หมายถึง เมื่อเราสื่อสารไปยังผู้บริโภคที่ไม่ได้เต็มใจรับสื่อของคุณแต่แรก หรือไม่เคยลงทะเบียนรับข่าวสารจากเราเลย และเมื่อไรที่พวกเขายกเลิกการรับสื่อของเรา ที่เรียกว่า Opt-out หรือยกเลิกการเป็นสมาชิก (Unsubscribe) เราก็จะต้องยกเลิกการสื่อสารกับผู้บริโภคในครั้งต่อไปทันที มิฉะนั้นแล้ว จะเข้าข่ายของ Spam

การจัดทำนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

การเริ่มดำเนินการ / การสำรวจและเตรียมความพร้อมต่อข้อมูลส่วนบุคคล

	หัวข้อ	มี	ไม่มี	รายละเอียด
(1)	มีการเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่			
(2)	ข้อมูลส่วนบุคคลประเภทใดบ้างที่มีการเก็บรวมรวม			
(3)	มีการเก็บรวบรวมข้อมูลอย่างไร (เก็บจากเจ้าของข้อมูลโดยตรง หรือเก็บจากบุคคลที่สาม)			
(4)	ได้มีการเตือนให้เจ้าของข้อมูลทราบถึงการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นหรือไม่			
(5)	บุคคลใดเป็นผู้ตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลอะไรบ้าง และจะเก็บรวบรวมอย่างไร			
(6)	มีบุคคลอื่นนอกจากเว็บไซต์ที่เก็บรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์นี้หรือไม่			
(7)	เพราะเหตุใดจึงต้องมีการเก็บรวบรวมข้อมูลส่วนบุคคล			
(8)	บุคคลใดเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมไป			

การจัดทำนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

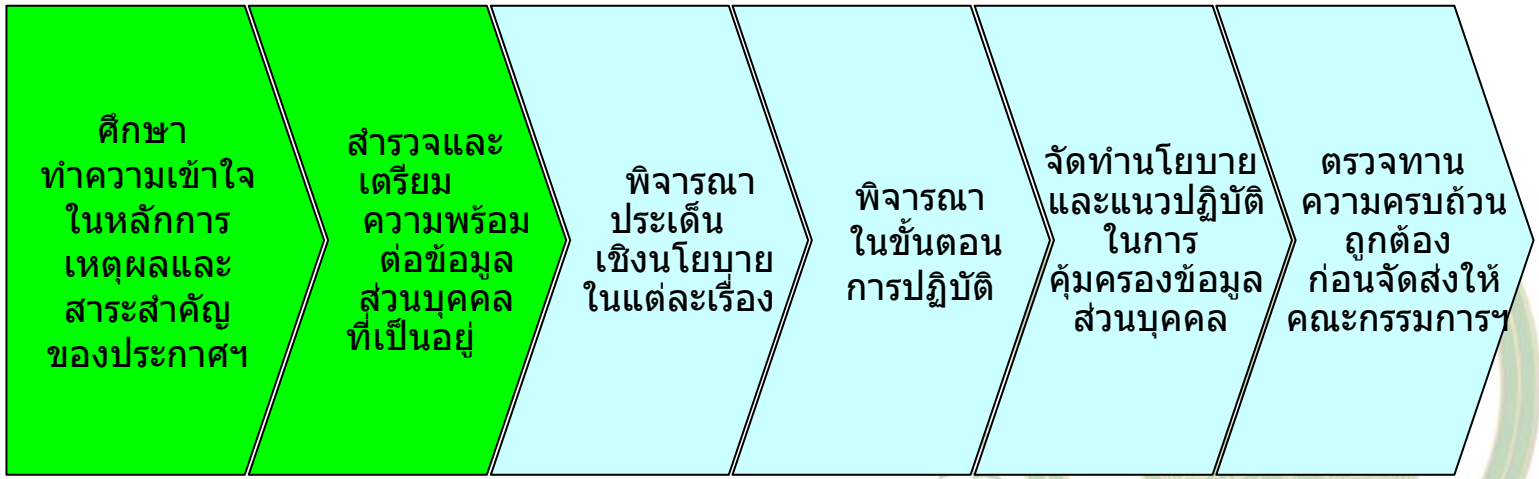
การเริ่มดำเนินการ / การสำรวจและเตรียมความพร้อมต่อข้อมูลส่วนบุคคล (ต่อ)

	หัวข้อ	มี	ไม่มี	รายละเอียด
(9)	ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมไปมีการเปิดเผยต่อบุคคลที่สามหรือไม่ และหากมีการเปิดเผย เปิดเผยไปเพราะเหตุใด			
(10)	ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมไป ถูกเก็บรักษาไว้ที่ไหน และเก็บรักษาอย่างไร			
(11)	มีการใช้มาตรฐานหรือแนวทางปฏิบัติที่หน่วยงานอื่นกำหนดในการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลหรือไม่			
(12)	เจ้าของข้อมูลมีทางเลือกอย่างไรบ้างเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล			
(13)	อนุญาตให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตนหรือไม่			
(14)	กรณีเจ้าของข้อมูลมีคำร้องขอใดๆ เกี่ยวกับข้อมูลส่วนบุคคล (ขอให้แก้ไข หรือขอให้ลบทิ้ง) ต้องทำอย่างไร			

ที่มา : Privacy Policy & Trustmark กลไกการคุ้มครองข้อมูลส่วนบุคคลกับการสร้างความน่าเชื่อถือในการทำ e-Business

การจัดทำนโยบายและแนวปฏิบัติ ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

พิจารณาว่า ปัจจุบันดำเนินการในเรื่องนี้ อย่างไร



ในกรณีที่ต้องปรับเปลี่ยนวิธีปฏิบัติหรือแนวปฏิบัติต่อข้อมูลส่วนบุคคลให้มีความเหมาะสมนั้น มีประเด็นที่ควรจะต้องทราบ เพิ่มเติม ดังนี้

หลักการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

คณะอนุกรรมการกฎหมายฯ ครั้งที่ 6/54 4 ต.ค. 54

1. หน่วยงานของรัฐควรกำหนดแนวนโยบายและแนวปฏิบัติฯ แยกออกจากกันให้ชัดเจน และเป็นไปตามประกาศคณะกรรมการ

2. การดำเนินการนั้น กฎหมายของหน่วยงาน ได้ให้อำนาจแก่หน่วยงานในการจัดเก็บข้อมูลส่วนบุคคลด้วยหรือไม่ โดยต้องมีการระบุไว้ในประกาศอย่างชัดเจน เนื่องจากเป็นประเด็นที่เกี่ยวข้องกับอำนาจหน้าที่ตามกฎหมาย ซึ่งหากหน่วยงานจัดเก็บข้อมูลส่วนบุคคลเกินกว่าอำนาจหน้าที่จะเป็นการไม่ถูกต้อง

3. ส่วนที่เกี่ยวข้องกับนโยบายฯ หน่วยงานจะต้องเขียนแยกเป็นข้อๆ ให้ครบทั้ง 8 ข้อ ตามที่ประกาศคณะกรรมการฯ กำหนด

   ส่วนที่เกี่ยวข้องกับแนวปฏิบัติฯ หน่วยงานจะต้องเขียนโดยให้มีหัวข้อแยกเป็นข้อๆ และให้ครบตามประกาศคณะกรรมการฯ กำหนดเช่นกัน

   หากเรื่องใดที่หน่วยงานนั้นไม่ได้ดำเนินการก็ให้ระบุไว้ด้วยว่า “ไม่มี” พร้อมทั้งแสดงเหตุผลที่มิได้ดำเนินการประกอบด้วย โดยห้ามตัดหัวข้อนั้นทิ้ง

<u>เพิ่มเติม</u> ในส่วนของแนวปฏิบัติ หากหน่วยงานมีการดำเนินการ (บางข้อ) ต้องนำมาเขียนเพิ่มเติมไว้ในนโยบายในการคุ้มครองข้อมูลส่วนบุคคลด้วย

หลักการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

คณะอนุกรรมการมั่นคงปลอดภัย ต.ค.55

ข้อ 1(5)	การรักษาความมั่นคงปลอดภัย
ข้อ 1(8)	ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล
ข้อ 2(2) (ข)	การใช้คุกกี้ (Cookies)
ข้อ 2(2) (ค)	การจัดประเภทข้อมูลส่วนบุคคลในระบบสารสนเทศ
ข้อ 2(2) (ง)	บันทึกผู้เข้าชมเว็บ (Log Files)
ข้อ 2(8)	การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

<u>เพิ่มเติม</u> ระบุแนวปฏิบัติด้านเทคนิคในส่วนสีเทา และเชื่อมโยงความสอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานให้ชัดเจน

การพัฒนาการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

การให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลเป็นสิ่งจำเป็น เพื่อเพิ่มความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ กับประชาชน และยังเป็นการช่วยขจัดข้อจำกัดในด้านการแลกเปลี่ยนข้อมูลระหว่างประเทศ

นโยบายคุ้มครองความเป็นส่วนตัว (Privacy Policy) คือ สิ่งที่ผู้ประกอบธุรกรรมผ่านทางเว็บไซต์บอกผู้ใช้บริการ/ผู้ที่เกี่ยวข้องได้รับรู้ถึงนโยบายในการเก็บรวบรวม การใช้ การคุ้มครอง รักษาความลับหรือความปลอดภัยสำหรับข้อมูลของผู้ใช้บริการเว็บไซต์ของตน

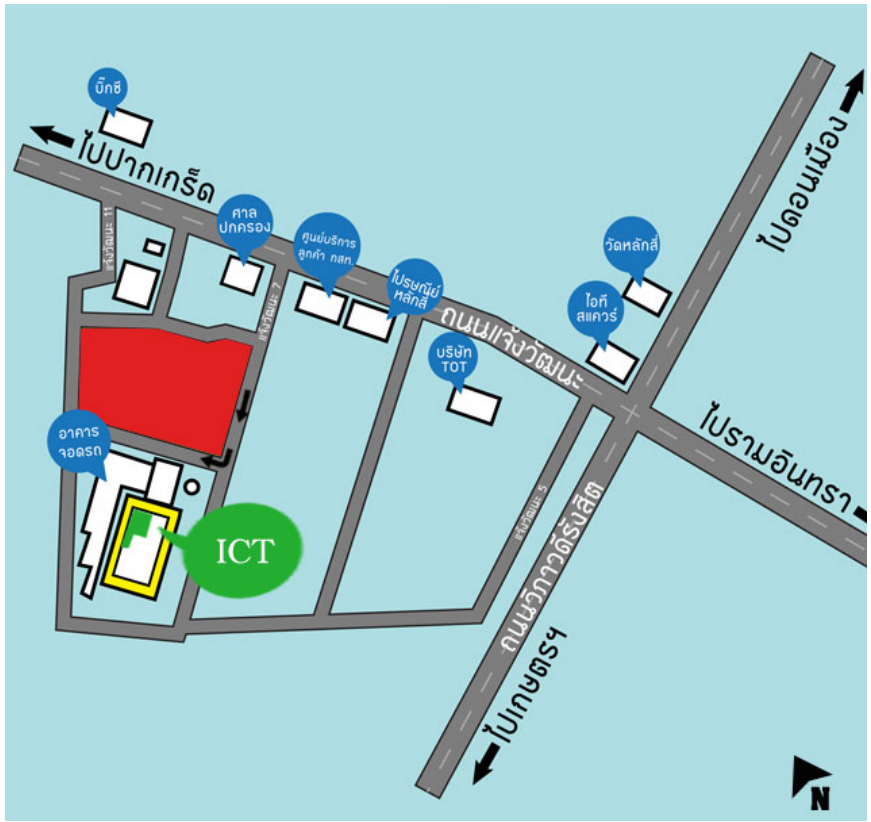
ทั้งนี้ นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ อันนับเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนตัวของประชาชน (Privacy Rights) จะต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ก่อน จึงให้มีผลใช้บังคับได้ (มาตรา 7)

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

โทรศัพท์ 02 141 6991

โทรสาร 02 143 8036-7



http://www.etcommission.go.th

ขอขอบคุณ

www.mict.go.th
www.etcommission.go.th