

การคุ้มครองข้อมูลส่วนบุคคล ของมหาวิทยาลัย : กรณีศึกษา

ฐิติมา ธรรมบำรุง, Ph.D.

นักวิชาการอาวุโส

ฝ่ายบริการความรู้ทางวิทยาศาสตร์และเทคโนโลยี (STKS)
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

เหตุใดต้องสนใจ "ข้อมูลส่วนบุคคล"

Home / Technology / Security

July 08
2019

British Airways fined over £183m for personal data breach under the GDPR

MAY 16, 2019

Red Cross website hacked in latest Singapore cyber attack

The Singapore Red Cross said Thursday its website had been hacked and the personal data of more than 4,000 potential donors compromised in the latest cyber attack on the city.

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

Zack Whittaker @zackwhittaker / 12:11 am +07 • January 5, 2019

Comment

ทรู น้อมรับคำสั่ง กสทช. ระบุนัดดูแล-เยียวยาลูกค้าที่ได้รับผลกระทบ ปมข้อมูลบัตรประชาชนหลุด

ประชาไท / ข่าว

Submitted on Fri, 2018-04-20 15:51

FACEBOOK ยอมจ่ายค่าปรับ 154,000 ล้านบาทและเริ่มแผนคุ้มครองส่วนบุคคล 20 ปี

July 26, 2019 Data Security and Privacy, Facebook, Products, Security

Federal Trade Commission (FTC) ออกแถลงการณ์ยืนยันอย่างเป็นทางการว่า Facebook ยินยอมที่จะจ่ายค่าปรับเป็นจำนวนเงินสูงถึง \$5,000 ล้าน (ประมาณ 154,000 ล้านบาท) จากการละเมิดความเป็นส่วนบุคคลอันเนื่องมาจากคดี Cambridge Analytica รวมไปถึงยอมรับการปรับปรุงกรอบการทำงานขององค์กรเพื่อเพิ่มความแข็งแกร่งในแนวทางปฏิบัติและนโยบายคุ้มครองข้อมูลส่วนบุคคลเป็นระยะเวลานานถึง 20 ปี

<https://phys.org/news/2019-05-red-website-hacked-latest-singapore.html>

<https://techcrunch.com/2019/01/04/marriott-five-million-passport-numbers-stolen-starwood/>

<https://prachatai.com/journal/2018/04/76480>

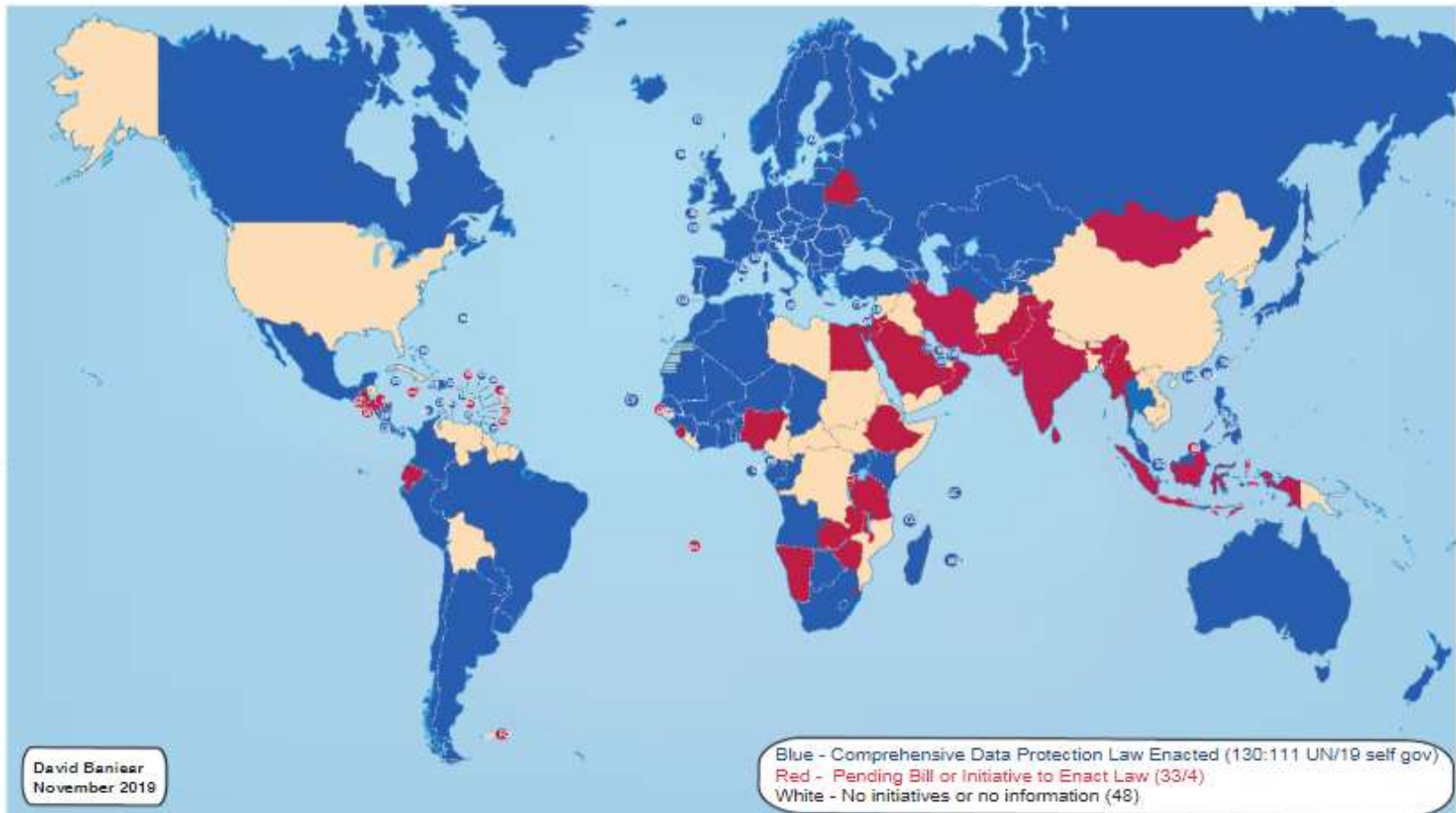
<https://www.mayerbrown.com/en/perspectives-events/publications/2019/07/british-airways-fined-over-183m-for-personal-data-breach-under-the-gdpr>

<https://www.varonis.com/blog/data-privacy/>

เหตุใดต้องสนใจ “ข้อมูลส่วนบุคคล”

130 ประเทศที่มีกฎหมาย อีก 40 ประเทศ กำลังยกร่าง

National Comprehensive Data Protection/Privacy Laws and Bills 2019



ประเทศไทยประกาศใช้กฎหมายเฉพาะนี้แล้ว



พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ

พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒

เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

ข้อมูลส่วนบุคคล หมายถึงอะไร

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม (พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (General Data Protection Regulation (GDPR), EU)

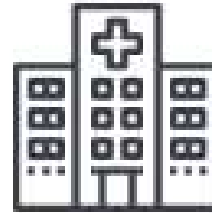
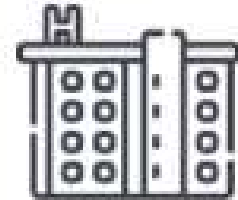
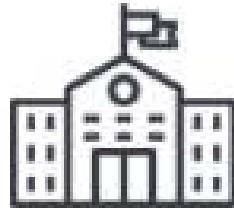
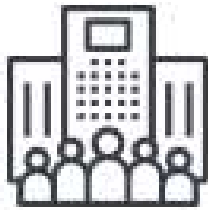
ตัวอย่างข้อมูลส่วนบุคคล

- ชื่อ-นามสกุล
- ที่อยู่
- อีเมล เช่น ชื่อ@ชื่อหน่วยงาน/บริษัท.com
- หมายเลขโทรศัพท์
- เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต
- IP address, Cookie ID
- ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, फिल्मเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม
- ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ, สัญชาติ, น้ำหนัก, ส่วนสูง, ข้อมูลตำแหน่ง/พิกัดสถานที่ที่อยู่ (Location data), ข้อมูลการแพทย์, ข้อมูลการศึกษา, ข้อมูลทางการเงิน, ข้อมูลการทำงาน

ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว

1. เชื้อชาติ
2. เผ่าพันธุ์
3. ความคิดเห็นทางการเมือง
4. ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
5. พฤติกรรมทางเพศ
6. ประวัติอาชญากรรม
7. ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
8. ข้อมูลสหภาพแรงงาน
7. ข้อมูลพันธุกรรม
8. ข้อมูลชีวภาพ
 - ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยี ที่เกี่ยวข้องกับ การนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตน ของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือ ข้อมูลจำลองลายนิ้วมือ
9. ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

องค์กรใดบ้างที่ได้รับผล



"ทุก" องค์กรที่มีการเก็บรวบรวม ใช้ หรือเปิดเผย
ข้อมูลส่วนบุคคล

ม. เก็บข้อมูลส่วนบุคคลจากใครบ้าง

ผู้สมัครเป็น
นักศึกษาและ
บุคลากร

นักศึกษาและ
พนักงาน

ศิษย์เก่า

ผู้เข้าชมและใช้งาน
เว็บไซต์

ผู้เข้าร่วมการวิจัย

ผู้สมัครเป็นนักศึกษา	ผู้สมัครเป็นบุคลากร	นักศึกษา	พนักงาน
<ul style="list-style-type: none"> • ข้อมูลส่วนตัว • ข้อมูลการศึกษา • ข้อมูลการสนับสนุนทางการเงิน • ความคิดเห็นเกี่ยวกับขั้นตอนการสมัครและบริการของ ม. • บันทึกการเข้าร่วมกิจกรรมการรับสมัครและข้อมูลภาพถ่ายของเหตุการณ์ดังกล่าว • ข้อมูลภูมิหลังทางเศรษฐกิจและสังคม • ข้อมูลเชื้อชาติ ชาติพันธุ์ รสนิยมทางเพศและความเชื่อทางศาสนา • ข้อมูลสุขภาพ ความพิการ หรือเงื่อนไขทางการแพทย์ • ข้อมูลความผิดทางอาญา 	<ul style="list-style-type: none"> • ข้อมูลส่วนตัว • ข้อมูลการศึกษาและการจ้างงาน • ข้อมูลเกี่ยวกับเชื้อชาติ ชาติพันธุ์ รสนิยมทางเพศและความเชื่อทางศาสนา • ข้อมูลเกี่ยวกับสุขภาพ ความพิการ หรือเงื่อนไขทางการแพทย์ • ข้อมูลเกี่ยวกับความผิดทางอาญา 	<ul style="list-style-type: none"> • ข้อมูลส่วนตัว • ข้อมูลติดต่อกรณีฉุกเฉิน • ข้อมูลการศึกษา • ข้อมูลภูมิหลังส่วนบุคคลอื่นที่รวบรวมระหว่างขั้นตอนการรับสมัคร • บันทึกการรับสมัคร ข้อมูลคะแนนการทดสอบและการสัมภาษณ์ และการตัดสินใจรับเข้า บันทึกการสอบ • บันทึกค่าธรรมเนียมและการสนับสนุนทางการเงิน • กิจกรรมการนิเทศ การสอนและการมีส่วนร่วมกับเครื่องมือออนไลน์ • บันทึกการเรียนการสอนหรือกิจกรรมการวิจัยที่เป็นผู้เข้าร่วม • ข้อมูลการใช้ห้องสมุด • ข้อมูลการมีส่วนร่วมในขั้นตอนต่างๆ ของ ม. • ข้อมูลภาพถ่ายในเหตุการณ์เพื่อประชาสัมพันธ์ • ข้อมูลเกี่ยวกับการใช้ระบบข้อมูล และการสื่อสารของ ม. • ข้อมูลที่รวบรวมผ่านกล้อง CCTV และการเข้าอาคาร • ข้อมูลเชื้อชาติ ชาติพันธุ์ รสนิยมทางเพศและความเชื่อทางศาสนา • ข้อมูลเกี่ยวกับสุขภาพ ความพิการ หรือเงื่อนไขทางการแพทย์ • ข้อมูลเกี่ยวกับความผิดทางอาญา 	<ul style="list-style-type: none"> • ข้อมูลส่วนตัว • ข้อมูลติดต่อกรณีฉุกเฉิน • ข้อมูลธนาคาร ภาษีและข้อมูลทางการเงินอื่น • ข้อมูลเงินเดือน การลาและผลประโยชน์ • ข้อมูลการรับสมัคร • บันทึกการจ้างงานและการปฏิบัติงาน (รวมถึงตำแหน่ง ประวัติทำงาน ชั่วโมงและสถานที่ทำงาน • ประวัติการพัฒนาส่วนบุคคลและการฝึกอบรม • ข้อมูลด้านสุขภาพและความปลอดภัยและการเป็นสมาชิกวิชาชีพ) • ข้อมูลเกี่ยวกับการใช้ระบบข้อมูล และการสื่อสารของ ม. • ข้อมูลที่รวบรวมผ่านกล้อง CCTV และการเข้าอาคาร • รูปถ่าย • ข้อมูลเชื้อชาติ ชาติพันธุ์ รสนิยมทางเพศและความเชื่อทางศาสนา • ข้อมูลเกี่ยวกับสุขภาพ ความพิการ หรือเงื่อนไขทางการแพทย์ • ข้อมูลเกี่ยวกับความผิดทางอาญา

ผู้เข้าร่วมการวิจัย	ผู้เข้าชมและใช้งานเว็บไซต์	ศิษย์เก่า
<ul style="list-style-type: none"> • ผู้ที่ตกลงจะเข้าร่วมการวิจัยโดยนักวิจัยของ ม. และ / หรือ • ผู้ที่ให้ข้อมูลส่วนบุคคลกับองค์กรอื่นที่ส่งต่อข้อมูลนั้นมายัง ม. เพื่อการวิจัย 	<ul style="list-style-type: none"> • ข้อมูลทางเทคนิค (เช่น ประเภทของอุปกรณ์ IP address ข้อมูลการเข้าสู่ระบบ ประเภทเบราว์เซอร์และเวอร์ชัน การตั้งค่าโฆษณาประเภทและเวอร์ชันปลั๊กอินของเบราว์เซอร์ ระบบปฏิบัติการ ข้อมูลเครือข่ายมือถือและแพลตฟอร์ม) และ • ข้อมูลการเยี่ยมชมเว็บไซต์ (เช่น หน้าที่ดูระยะเวลาในการเข้าชม ข้อมูลการโต้ตอบของเพจ) 	<ul style="list-style-type: none"> • ข้อมูลชีวประวัติ • รายละเอียดเกี่ยวกับความสัมพันธ์และการมีส่วนร่วมกับ ม.

ห้องสมุดเก็บข้อมูลส่วนบุคคลอะไรบ้าง

- ชื่อ-นามสกุล
- ภาพถ่าย
- ที่อยู่รายละเอียดการติดต่อ โทรศัพท์ อีเมล
- วันเดือนปีเกิด
- หมายเลขหนังสือศึกษา/พนักงาน/ประชาชน
- สาขา คณะ และสถาบัน / หน่วยงานที่สังกัด
- ประวัติการใช้บริการยืมคืน (ทั้งที่ดำเนินการโดยห้องสมุดและบุคคลที่ 3)
- การบันทึกภาพบุคคลเข้าออก
- ภาพในกล้องวงจรปิดที่เก็บ
- ความคิดเห็น ข้อเสนอแนะและการตอบสนอง เช่น จากการสำรวจและการศึกษาผู้ใช้

1
ชอบด้วยกฎหมาย โปร่งใส
ตรวจสอบได้

1

2
ภายใต้ขอบเขตและ
วัตถุประสงค์

2

6 หลักการคุ้มครอง ข้อมูลส่วนบุคคล

6
มีมาตรการความมั่นคง
ปลอดภัยที่เหมาะสม

6

5
ตามระยะเวลาเท่าที่จำเป็น

5

3
พอเพียง เกียวข้อง เท่าที่
จำเป็นตามวัตถุประสงค์

3

4
ถูกต้องและเป็นปัจจุบัน
(กรณีจำเป็น)

4

ประเด็นสำคัญของ การคุ้มครองข้อมูลส่วนบุคคล

จะดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล
ส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคล
ไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น

เว้นแต่บทบัญญัติแห่ง พ.ร.บ. นี้หรือกฎหมายอื่น
บัญญัติให้กระทำได้

กิจการที่ไม่ต้องถูกบังคับโดยกฎหมายนี้

- 1 เพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น
- 2 มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์
- 3 เพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น
- 4 การพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมการการแล้วแต่กรณี
- 5 พิจารณาพิพากษาคดีของศาล และการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา
- 6 การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิต และสมาชิกตามกฎหมายว่าด้วย การประกอบธุรกิจข้อมูลเครดิต

ต้องจัดให้มี การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน

ยกเว้นให้เก็บรวบรวมข้อมูล ใช้ข้อมูล โดยไม่ต้องขอความยินยอม

1 เพื่อการจัดทำ เอกสาร ประวัติศาสตร์หรือ จดหมายเหตุฯ

2 เพื่อป้องกันหรือระงับ อันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

3 เป็นการจำเป็นเพื่อการ ปฏิบัติตามสัญญาซึ่ง เจ้าของข้อมูลส่วนบุคคล เป็นคู่สัญญา หรือเพื่อใช้ ในการดำเนินการตามคำ ขอบของเจ้าของข้อมูล

4 เป็นการจำเป็นเพื่อ การปฏิบัติหน้าที่ใน การดำเนินการกิจเพื่อ ประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ใน การใช้อำนาจอรัฐที่ได้ มอบให้แก่ผู้ควบคุม ข้อมูลส่วนบุคคล

5 เป็นการจำเป็นเพื่อประโยชน์ โดยชอบด้วยกฎหมายของผู้ ควบคุมข้อมูลส่วนบุคคล

6 เป็นการปฏิบัติตาม กฎหมายของผู้ควบคุม ข้อมูลส่วนบุคคล

ต้องจัดให้มี การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน

หลักการพื้นฐานสำคัญของกฎหมายที่ต้องปฏิบัติ

1. **แจ้งวัตถุประสงค์**ว่าจะเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อะไรและเพื่ออะไร ในขณะที่ขอความยินยอม
2. หลักความยินยอม **ขอความยินยอม**ในการเก็บรวบรวม การใช้ หรือการเปิดเผย จากเจ้าของ ข้อมูลส่วนบุคคล
3. การเก็บ การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล **เท่าที่จำเป็น** และดำเนินตามวัตถุประสงค์ที่ได้แจ้งไว้
4. **ดูแลรักษาข้อมูลส่วนบุคคลให้ดี** จัดให้มีมาตรการรักษาความปลอดภัย
5. **การกำหนดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล**
6. เจ้าของข้อมูลส่วนบุคคล จะถอนความยินยอมเมื่อใดก็ได้ โดยต้องถอนได้ง่าย
7. **เคารพสิทธิของเจ้าของข้อมูลส่วนบุคคล**

สิทธิของเจ้าของข้อมูลส่วนบุคคล

1. สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)
2. สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)
3. สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
4. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
5. สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure (also known as right to be forgotten))
6. สิทธิขอให้ระงับการใช้ข้อมูล (Right to restrict processing)
7. สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล (Right of rectification)

การเตรียมพร้อมสำหรับ การคุ้มครองข้อมูลส่วนบุคคล



ประกาศการคุ้มครองข้อมูลส่วนบุคคล

คืออะไร....เอกสารสาธารณะที่องค์กรซึ่งประมวลผลข้อมูลส่วนบุคคลแสดงแก่เจ้าของข้อมูลส่วนบุคคล เพื่ออธิบายวิธีการประมวลผลข้อมูลส่วนบุคคลของบุคคลดังกล่าวว่าจะดำเนินการอย่างไรและมีมาตรการการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวอย่างไร

ทำไมต้องมี....เป็นข้อกำหนดตามกฎหมายฯ

- เจ้าของข้อมูลส่วนบุคคล ได้รับทราบวิธีการประมวลผลข้อมูลส่วนบุคคลของตนเองก่อนให้ความยินยอม
- องค์กร ใช้เป็นเอกสารรับรองกิจกรรมการประมวลผลข้อมูลส่วนบุคคลขององค์กร ช่วยให้องค์กรมีเหตุผลในการดำเนินการประมวลผลข้อมูลส่วนบุคคล หากมีผู้ยื่นเรื่องร้องเรียนกับหน่วยงานกำกับดูแล

ประกาศการคุ้มครองข้อมูลส่วนบุคคลควรมี รายละเอียดดังต่อไปนี้ (เป็นอย่างน้อย)

1. นิยามของข้อมูลฯ และประเภทของข้อมูลฯ ที่จะถูกประมวลผล
2. วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล
3. หลักการคุ้มครองข้อมูลฯ และฐานในการประมวลผลข้อมูลฯ
4. ข้อมูลจะถูกประมวลผลอย่างไร และ นานเพียงใด
5. มาตรการความมั่นคงและปลอดภัยของข้อมูลฯ
6. สิทธิของเจ้าของข้อมูล
7. ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลฯ ที่เก็บรวบรวมอาจจะถูกเปิดเผย
8. รายละเอียดการติดต่อ

วิธีที่ง่ายที่สุดในการแจ้งประกาศฯ คือโพสต์ไว้บนเว็บไซต์และเชื่อมโยงไปยังทุกครั้งที่ต้องรวบรวมข้อมูลฯ

Imperial College

Data Protection Policy

Imperial College

Doc. Ref. : Data Protection Policy
Version : 1.5
Status : Approved
Date : 20/04/2018
Approved by : The Provost Board
Review by : 30/04/2019

University of Oxford

<https://compliance.admin.ox.ac.uk/>

ANNEX A



University Policy on Data Protection

Contents

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

Compliance



[HOW WE USE YOUR DATA](#)
[SUBMIT AN INFORMATION REQUEST](#)
[POLICIES & STATEMENTS](#)
[STAFF GUIDANCE ON DATA PROTECTION](#)
[ABOUT](#)

Prospective students and staff

Undergraduate applicant privacy policy

Postgraduate applicant privacy policy

Department for Continuing Education (Undergraduate Courses) applicant privacy policy

Current students and staff

Student privacy policy

Staff privacy policy

Research participants

How we use your personal data for research purposes

Website visitors


Alumni & donors


- วัตถุประสงค์ของประกาศ
- คำนิยามคำศัพท์
- ใครใช้ข้อมูลส่วนบุคคล
- ประเภทของข้อมูลส่วนบุคคล
- การเก็บรวบรวมข้อมูลส่วนบุคคล
- การใช้ข้อมูลส่วนบุคคล และฐานการประมวลผล


- การเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่ 3
- การเก็บรักษาและการทำลายข้อมูลส่วนบุคคล
- สิทธิของเจ้าของข้อมูลส่วนบุคคล
- ข้อมูลติดต่อและการเปลี่ยนแปลงประกาศ


Undergraduate applicant privacy policy


How we collect and use the personal data of undergraduate students during their application process


1. WHAT IS THE PURPOSE OF THIS DOCUMENT? 


2. GLOSSARY 


3. WHO IS USING YOUR PERSONAL DATA? 


4. THE TYPES OF DATA WE HOLD ABOUT YOU 


5. HOW THE UNIVERSITY OBTAINED YOUR DATA 


6. HOW THE UNIVERSITY USES YOUR DATA 


7. SPECIAL CATEGORY DATA AND CRIMINAL CONVICTION DATA 


8. DATA SHARING WITH THIRD PARTIES 

9. TRANSFER OF YOUR DATA OUTSIDE OF THE EUROPEAN ECONOMIC AREA (EEA) [3] 

10. RETENTION PERIOD 

11. YOUR RIGHTS 

12. KEEPING YOUR DATA UP-TO-DATE 

13. CHANGES TO THIS PRIVACY POLICY 

แนวทางการเก็บรักษาและทำลายข้อมูล

Introduction

Why do we need a data retention policy?

- We need to comply with the requirement of the General Data Protection Regulation that personal data is not kept for longer than necessary. If we retain personal data for longer than we need to, we will also breach the requirement that personal data must be relevant and limited to what is necessary to meet our purposes.
- We need to keep data for as long as it is required to meet operational purposes or for organisational archiving relating to scientific, historical research or statistical purposes.
- We need to make best use of storage space, both physical and digital.

Scope

- This guidance seeks to provide indicative guidance for those responsible for managing student records and student administration. It covers the main corporate systems such as SITS, CMIS, GSR, OXCORT, DWH, and local Access databases, Excel spreadsheets, email and paper, for example, interview scores held locally in a departmental database.
- Data extracted from master systems and stored in local drives or email should be destroyed after use to avoid unnecessary duplication, and to ensure data is not held for any longer than necessary.
- Excluded: Retention guidelines for maintaining transactional records, for example retention of requests for transcripts.

Retention periods

- The master copy of data should not be deleted before the expiry of the retention period. Supplementary copies (e.g. Excel downloads, or working files) should be deleted before the retention period if they no longer serve a purpose. Careful consideration should be given as to whether supplementary copies of data should be held or could be destroyed.
- When the retention period is reached, the data should be destroyed as soon as practicable and in a secure manner.

Issued by Student Registry

September 2020

Document navigation

- A. [Admissions](#)
- B. [Careers](#)
- C. [Course](#)
- D. [Exams and assessments](#)
- E. [Fees and funding](#)
- F. [Person](#)
- G. [Post award](#)
- H. [Research students](#)
- I. [Students on course](#)
- J. [Student support](#)
- K. [Higher doctorates](#)

Related documents and links

[Retention of staff records](#)

[Data Protection: Policy](#)

[Data Protection: Guidance](#)

Further information: Data Quality Team (dqt@admin.ox.ac.uk)

แนวทางการเก็บรักษาข้อมูลและรายการของนักเรียน/นักศึกษา

ID	Sub-category	Purpose	data example	Where processed	Retention Period	Retention Record Owner
Admissions						
A.1.1	Application details (central): successful candidates who enrol	Information to enable recruitment and funding panels to determine admissions outcomes	interview and admissions test scores, previous qualifications, previous education, supporting statements, references, personal data covered under Person (section F).	ADSS, SITS & eVision, paper copies in central teams, data warehouse, definitive dataset (including its processing files), other reporting Access databases	permanent in master system i.e. SITS/eVision; else: End of student relationship + 6 years UG Admissions data is held in ADSS for 12 months before being permanently stored on a dedicated reporting server.	GAR and UAO (with SDMA)
A.4.1	Application details (central): unsuccessful candidates; successful candidates who don't enrol	Information to enable recruitment and funding panels to determine admissions outcomes	interview and admissions test scores, previous qualifications, previous education, supporting statements, references, personal data covered under Person (section F).	ADSS, SITS & eVision, paper copies in central teams, data warehouse, definitive dataset (including its processing files), other reporting Access databases	End of the admissions cycle in which applied plus one year for full records. Permanent: anonymised skeleton records without supporting documentation. UG Admissions data is held in ADSS for 12 months before being permanently stored on a dedicated reporting server.	GAR and UAO (with SDMA)

University of Cambridge

<https://www.information-compliance.admin.cam.ac.uk/data-protection>



Study at Cambridge

About the University

Research at Cambridge

Quick links

Search



Information Compliance

Home

Data Protection

Freedom of Information

Records Management

Data Protection

Information Compliance

Data Protection

- > [Making a Subject Access Request](#)
- > [How we use your personal information \(general\)](#)
- > [How we use your personal information \(for applicants\)](#)
- > [How we use your personal information \(for students\)](#)
- > [How we use your personal information \(for alumni and supporters\)](#)
- > [How we use your personal information \(for job applicants and staff\)](#)
- > [How we use your personal information \(for research participants\)](#)
- > [How we use your personal information \(for third parties whose personal data is used for academic and research purposes\)](#)

This page provides an overview of the following areas of further information.

- [Legislation](#)
- [Principles](#)
- [Privacy notices](#)
- [Rights](#)
- [Accountability obligations](#)
- [Data breaches](#)
- [Policy](#)
- [Guidance and training](#)
- [Data protection and Brexit](#)

Data Protection

- > [Making a Subject Access Request](#)
- > [How we use your personal information \(general\)](#)
- > [How we use your personal information \(for applicants\)](#)
- > [How we use your personal information \(for students\)](#)
- > [How we use your personal information \(for alumni and supporters\)](#)
- > [How we use your personal information \(for job applicants and staff\)](#)
- > [How we use your personal information \(for research participants\)](#)
- > [How we use your personal information \(for third parties whose personal data is used for academic and research purposes\)](#)
- > [Data protection guidance](#)
- > [General Data Protection Regulation](#)

[Policy](#)

[Online Training](#)

[Quick Guide](#)

การฝึกอบรมให้ความรู้

ออนไลน์

UNIVERSITY OF CAMBRIDGE

Select training provider (PPD Personal and Professional Development) Courses

Training / PPD / Data Protection Training: Online Course

PPD Personal and Professional Development

You are not currently logged in [Log in](#)

Home Your bookings Timetable **Courses** Themes Venues

Self-taught course
Provided by: PPD Personal and Professional Development

Booking
This course is self taught (Online course).
This course is taking bookings
[Book a place >](#)

Data Protection Training: Online Course

Description

This online course offers a short introduction to data protection concepts, explains why they are important to the University, and signposts to further guidance materials. As nearly all University staff are likely to collect and handle personal information about living identifiable individuals in one way or another, it's important to have a basic understanding of the main issues.

All staff using personal data in some way in their role are encouraged to complete this online course once every two years, but the precise expectations about who should complete it (and how often) in different areas of the University should be set by Heads of Department (and equivalents).

The content of this course reflects the provisions of the General Data Protection Regulation as well as related data protection law.

Target audience
University staff

พบหน้า

UNIVERSITY OF CAMBRIDGE

Select training provider (PPD Personal and Professional Development) Courses

Training / PPD / Data Protection and FOI: An Introduction

PPD Personal and Professional Development

You are not currently logged in [Log in](#)

Home Your bookings Timetable **Courses** Themes Venues

Instructor-led course
Provided by: PPD Personal and Professional Development

This course is not scheduled to run.

Register interest
Register your interest - if you would be interested in additional dates being scheduled.

Data Protection and FOI: An Introduction

Description

The rights and responsibilities outlined in data protection and freedom of information legislation impact upon the University's academic and administrative work. This course explores the key concepts in data protection law and illustrates how the 'data protection principles' affect various day-to-day working scenarios. It introduces the fundamental aspects of the Freedom of Information Act 2000 and details the ways in which the University handles responses to individual requests. Finally, it outlines various records management and information security measures that can aid compliance with the legislation and lead to a more efficient working environment.

Target audience

- University staff
- Further details regarding PPD's eligibility criteria are available

Imperial College London

<https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/>

Imperial College
London



Coronavirus (COVID-19) updates: Safety information for academic year 2020-21

Latest information for current students and staff

Imperial
ALERT

[Study](#) [Research & Innovation](#) [Be Inspired](#) [About](#)

[News](#) [What's on](#) [Give](#) [A-z](#) [Information for](#)

[Search](#)



Data protection

[Our policy](#) [GDPR](#) [Processing personal data](#) [Internal guidance](#) [External guidance](#) [Training](#) [Brexit](#) [Contact us](#)



GDPR is here!

There are new laws governing data protection. It is important that you understand your personal responsibilities so please familiarise yourself with the [guidance](#).

[Report a data breach](#)



[Make a subject access request](#)



The College is a centre of knowledge and training. Next to its people, information is its most important asset. Because of this, the College

ประกาศการคุ้มครองข้อมูลส่วนบุคคลอื่นๆ เพิ่มเติม : ประกาศฯ ของบริการห้องสมุด

Library Services

[Getting started](#) | [Use the library](#) | [Find books, articles and more](#) | [Subject support](#) | [Learning support](#) | [Research support](#) | [NHS](#) | [About us](#)

About us

- Your librarian
- Staff structure
- Library regulations
- Library policies
 - Room bookings
 - Student PC software policy
 - Collections policy
 - Conditions of use of IT resources
 - Online resources conditions of use
 - Privacy notice**
 - Library placements
 - Filming and photography
- Our strategy
- Projects

[Home](#) / [Administration and support services](#) / [Library Services](#) / [About us](#) / [Library policies](#) / [Privacy notice](#)

Privacy notice

Library Services Privacy Notice

This notice sets out the basis on which Library Services at Imperial College London collects and uses the personal data of our users.

Our users include, and accordingly this privacy policy applies to:

- Imperial College London students
- Imperial College London staff
- Imperial Alumni
- Retired Imperial staff
- NHS Trust staff
- Members of Imperial Incubator companies
- Francis Crick Institute staff
- Medical Research Council (MRC) Staff
- Thrombosis Research Institute staff

ประกาศการคุ้มครองข้อมูลส่วนบุคคลอื่นๆ เพิ่มเติม ประกาศฯ ของบริการห้องสมุด

ประเด็น	เนื้อหา
กลุ่มผู้ใช้	ระบุกกลุ่มผู้ใช้ เช่น นศ. พนง. ศิษย์เก่า และ พนง.เกษียณของ ม., นศ. และ พนง. ในชุมชนและเครือข่ายฯ
คำนิยาม	“เรา”และ“ของเรา” หมายถึง ห้องสมุด , “คุณ”และ“ของคุณ” หมายถึงผู้ใช้
ประเภทข้อมูลส่วนบุคคลที่เก็บ	ระบุประเภทข้อมูลส่วนบุคคลที่เก็บ เช่น ชื่อ-นามสกุล, รายละเอียดการติดต่อ, ว/ด/ป เกิด, หมายเลขสมาชิก, คณะและสาขา, วันที่จบหลักสูตร, ประวัติการใช้ห้องสมุด, ความเห็น/ข้อเสนอแนะจากการสำรวจและการศึกษาผู้ใช้
วิธีเก็บรวบรวมข้อมูล	ระบุวิธีเก็บรวบรวมข้อมูลส่วนบุคคล เช่น ผ่านพีดีข้อมูลอัตโนมัติจากระบบของ ม., แบบฟอร์มออนไลน์ของห้องสมุด, ในระหว่างการให้บริการ
วัตถุประสงค์การใช้ข้อมูล	ระบุวัตถุประสงค์การใช้ข้อมูลส่วนบุคคลและฐานการประมวลผล เช่น เพื่อเข้าอาคาร เพื่อจัดหาและดูแลบริการห้องสมุด เพื่อให้สามารถเข้าถึงทรัพยากรสารสนเทศ เพื่อตอบคำถาม เพื่อรวบรวมสถิติการใช้งาน เพื่อการปรับปรุงบริการอย่างต่อเนื่อง โดยใช้ฐานสัญญาและประโยชน์โดยชอบด้วยกฎหมาย

ประกาศการคุ้มครองข้อมูลส่วนบุคคลอื่นๆ เพิ่มเติม ประกาศฯ ของบริการห้องสมุด

ประเด็น	เนื้อหา
การแบ่งปันข้อมูล	<ul style="list-style-type: none"> • ระบุว่า จะแชร์ข้อมูลส่วนบุคคลให้แก่ใคร เช่น คณะที่สังกัดและฝ่ายการเงินของ ม. (แจ้งหนี้หนังสือหาย) • ห้องสมุดจะไม่ส่งต่อข้อมูลผู้ใช้ไปยังผู้ให้บริการ e-book e-journal ฐานข้อมูล ซอฟต์แวร์การจัดการรายการอ้างอิง ซึ่งเป็นบุคคลที่ 3 กรณีที่ผู้ให้บริการบุคคลที่ 3 ต้องการให้ผู้ใช้สร้างบัญชี สัญญาของผู้ใช้จะอยู่กับผู้ให้บริการและข้อมูลของผู้ใช้จะถูกจัดเก็บโดยผู้ให้บริการ ไม่ใช่ ม. • ในกรณีการเข้าถึง e-book e-journal ฐานข้อมูล ผ่านชื่อผู้ใช้และรหัสผ่านของ ม. ข้อมูลของผู้ใช้จะถูกปิดบังชื่อ/นิรนาม (anonymous) ณ จุดที่ใช้บริการของบุคคลที่สาม
ความปลอดภัยของข้อมูล	<p>ระบุแนวทางการรักษาความปลอดภัยของข้อมูล</p> <ul style="list-style-type: none"> • มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลสูญหายโดยไม่ตั้งใจ ถูกใช้หรือเข้าถึงในลักษณะที่ไม่ได้รับอนุญาต เปลี่ยนแปลงหรือเปิดเผย จำกัดการเข้าถึงข้อมูลส่วนบุคคลของกับบุคคลภายนอกที่มีความจำเป็นทางธุรกิจที่จะต้องทราบ โดยจะประมวลผลข้อมูลส่วนบุคคลตามคำแนะนำของห้องสมุดเท่านั้นและอยู่ภายใต้หน้าที่ในการรักษาความลับ • กำหนดขั้นตอนเพื่อจัดการกับการละเมิดความปลอดภัยของข้อมูลที่น่าสงสัย และจะแจ้งให้ผู้ใช้และผู้ควบคุมข้อมูลที่เกี่ยวข้องทราบถึงการละเมิดที่น่าสงสัยตามกฎหมาย

ประกาศการคุ้มครองข้อมูลส่วนบุคคลอื่นๆ เพิ่มเติม ประกาศฯ ของบริการห้องสมุด

ประเด็น	เนื้อหา
สิทธิ์ของเจ้าของข้อมูล	ระบุให้ผู้ใช้ทราบสิทธิ์ของเจ้าของข้อมูล ขออนุญาตยินยอม ขอเข้าถึงข้อมูล ขอแก้ไขข้อมูล ขอให้ลบ/ทำลายข้อมูล ขอจำกัด/ระงับการประมวลผลข้อมูล ขอสำเนาข้อมูลของคุณในรูปแบบอิเล็กทรอนิกส์ที่ใช้กันทั่วไป ขอคัดค้านการประมวลผลข้อมูล
ระยะเวลาการเก็บข้อมูล	ระบุระยะเวลาในการเก็บข้อมูล โดยโยงไปที่ แนวทางการเก็บรักษาและทำลายข้อมูลของห้องสมุด / ม.
DPO	ข้อมูลสำหรับติดต่อสื่อสารกับเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer : DPO) ทั้งที่อยู่ และ อีเมล
การอัปเดตประกาศฯ	แจ้งผู้ใช้ว่าห้องสมุดขอสงวนสิทธิ์ในการอัปเดตประกาศฯ ได้ตลอดเวลาและจะแจ้งประกาศฯ ตัวใหม่ให้ผู้ใช้ เมื่อทำการอัปเดตที่สำคัญ นอกจากนี้อาจแจ้งให้ผู้ใช้ทราบเป็นระยะๆ เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของคุณ

แนวทางการเก็บรักษาและทำลายข้อมูล

Record Type	Initiating Department(s)	Retention period	Send to ACRU upon creation?	Compliance and Regulatory information	Additional Notes
Information Systems					
Information System Policies and Codes of Practice	ICT	Permanent			
Specification of functional and technical requirements for IT hardware, software and networks	ICT	Permanent			
Records of testing and operation of hardware, software and	ICT	Permanent			
Backup schedules	ICT	Retain while current + 1			
Archiving schedules	ICT	Permanent			
Design, development and implementation of IT systems	ICT	Retain while current - major documentation (including manuals) to be transferred to ACRU after system decommissioning			
Libraries					
Library user data	Library Services	End of study/employment + 3			
Membership and day visitor registrations	Library Services	Current + 1			
Enquiries	Library Services	Current + 5			
Entry gate data	Library Services	Current + 1 term			
Room bookings	Library Services	Current + 1			
Workshop evaluations and bookings	Library Services	Until superseded			

Templates



A [Article 30 - Records of Processing template \[Word\]](#)

C [Consent checklists \(Word\)](#)

[Contracts checklists \(Word\)](#)

D [Data Controller - Data Processor Checklists \(Word\)](#)

[Data processing agreement \[Word\]](#)

[Data protection impact assessment guidance \[Word\]](#)

[Data protection impact assessment template \[Word\]](#)

[Data sharing agreement \[Word\]](#)

[Direct Marketing checklist \(Word\)](#)

Browse the templates below

#	A	B	C	D	E	F	G	I
W	X	Y	Z					

Toolkit 1 - for office printing



A6 leaflet

8 page A6 leaflet suitable for office printing



A3 poster set

Posters optimised for A3 and suitable for office printing



A5 poster set

Posters optimised for A5 and suitable for office printing

Training

General GDPR training session
[\[PDF\]](#)



Marketing and GDPR training session
[\[PDF\]](#)



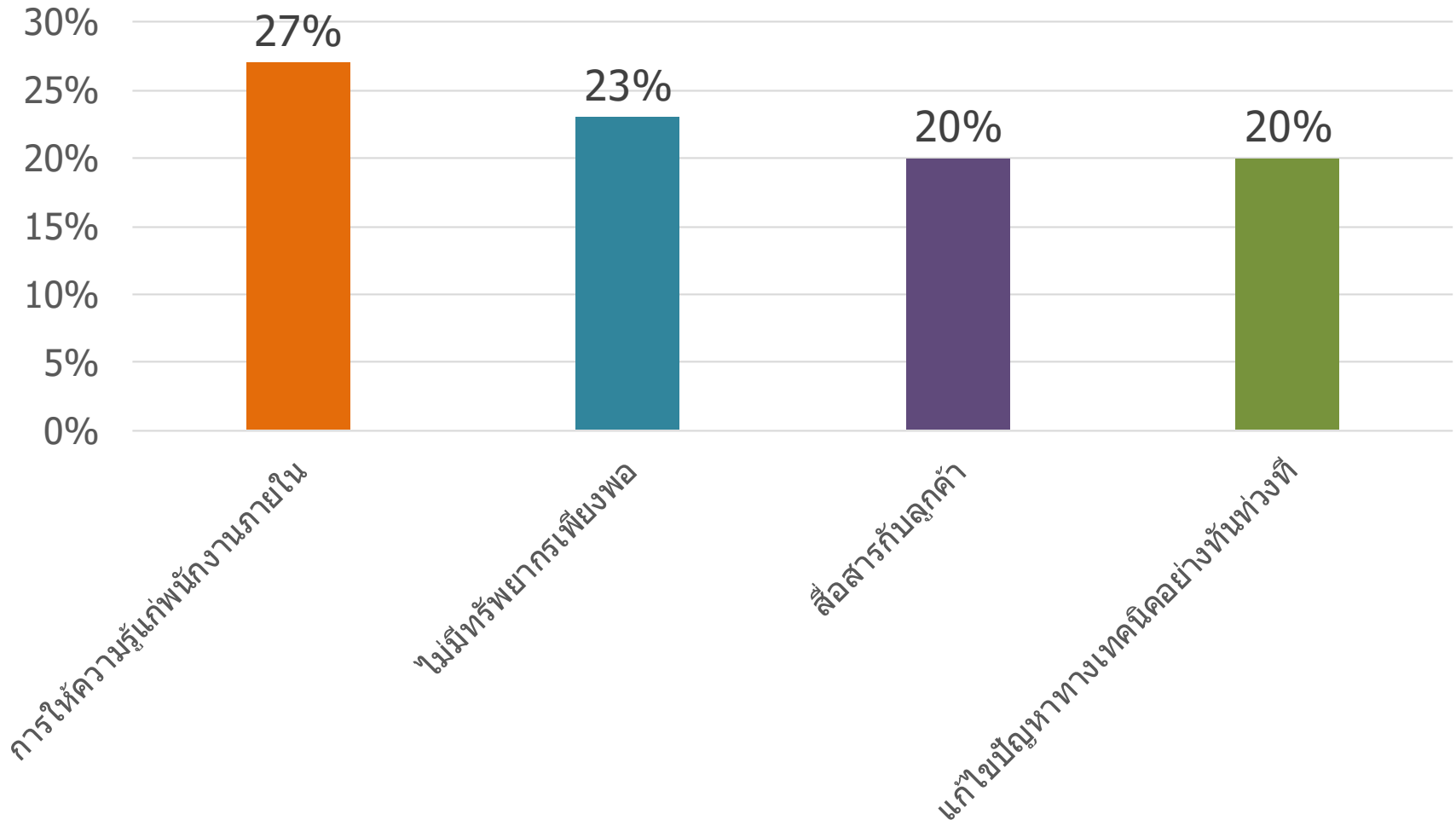
Research and GDPR training session
[\[PDF\]](#)



จากกรณีศึกษา

- จัดทำประกาศ นโยบาย แนวทาง/หลักปฏิบัติ เทมเพลตและข้อมูลการคุ้มครองข้อมูลส่วนบุคคล ทั้งแบบภาพรวมและแยกกลุ่มหรือแยกกิจกรรม ที่ชัดเจน สำหรับภายใน (พนักงานและนักศึกษา) และ ภายนอก (เจ้าของข้อมูลส่วนบุคคล แบ่งตามกลุ่ม เช่น ผู้สมัครเป็นนักศึกษาและบุคลากร นักศึกษาและพนักงาน ศิษย์เก่า ผู้เข้าชมและใช้งานเว็บไซต์ ผู้เข้าร่วมการวิจัย)
- สามารถเข้าถึงประกาศ นโยบาย แนวทาง/หลักปฏิบัติ เทมเพลตและข้อมูลการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวโดยสะดวก ผ่านเว็บไซต์ซึ่งจัดทำขึ้นเฉพาะ
- จัดทำแผนที่ข้อมูลส่วนบุคคลของมหาวิทยาลัยเพื่อการบริหารจัดการ โดยเสนอ ประเภท/รายการข้อมูล จุดประสงค์ของข้อมูล ตัวอย่างข้อมูล หน่วยงานที่ประมวลผลข้อมูล ระยะเวลาเก็บรักษาและทำลายข้อมูล
- มีกลไกการให้ความรู้ การสร้างความตระหนัก และการมีส่วนร่วม เช่น การอบรม การผลิตสื่อความรู้ การกำหนดนโยบายให้ร่วมมือและกำกับและติดตาม การกำหนดให้เป็นส่วนหนึ่งของการบริหารความเสี่ยงของ ม. และส่วนงาน การสอบถามและพูดคุยกับเจ้าหน้าที่ทั่วทั้ง ม. เพื่อให้ได้ภาพกิจกรรมการประมวลผลของที่สมบูรณ์ยิ่งขึ้น

ความท้าทายสูงสุดในปัจจุบัน



**กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
เป็น โอกาส มากกว่า อุปสรรค**

**เพื่อสร้างความไว้วางใจและเชื่อมั่นทางดิจิทัลที่
ลึกซึ้งยิ่งขึ้นกับเจ้าของข้อมูลส่วนบุคคล**



ฐิติมา ธรรมบำรุง, PhD

เจ้าหน้าที่สารสนเทศอาวุโส

ฝ่ายบริการความรู้ทางวิทยาศาสตร์และเทคโนโลยี (STKS)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

titima@nstda.or.th

<http://facebook.com/titima.thumbumrung>

