



ศูนย์บริหารงานส่วน
สำนักงานตัวราชวิถี

PDPA

Personal Data Protection Act

ข้อกฎหมายครั้งที่ ๑ พ.ศ.๒๕๖๔

พระราชนิเวศน์สันติคุณครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๔

พิมพ์ครั้งที่ ๑ พ.ศ.๒๕๖๕





ข้อกฎหมายคาวรู้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ISBN

พิมพ์ครั้งที่ ๑ พ.ศ. ๒๕๖๕

จำนวน ๓,๐๐๐ เล่ม

จัดทำโดย ศูนย์บริหารงานสอบสวน สำนักงานตำรวจนครบาล

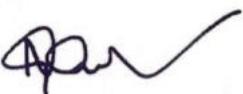
พิมพ์โดย โรงพิมพ์ตำรวจนครบาล

สงวนลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. ๒๕๓๗

คำปราารภ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เป็นกฎหมายที่กำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแล เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลอันเป็นการป้องกัน มิให้มีการล่วงละเมิดสิทธิความเป็นส่วนตัวของประชาชน โดยมีบัญญัติ ที่เป็นบทกำหนดโดยผู้ที่ฝ่าฝืนไม่ปฏิบัติตามกฎหมายฉบับนี้ ดังนั้น เจ้าหน้าที่ตำรวจ และผู้ที่เกี่ยวข้อง จึงจำเป็นต้องศึกษา ค้นคว้า ให้เกิด ความรู้ ความเข้าใจ และสามารถปฏิบัติงานได้อย่างถูกต้องเพื่อไม่ให้ เกิดข้อบกพร่องจนต้องรับผิดในทางปกครอง ทางแพ่ง และทางอาญา

สำนักงานตำรวจนครบาล จึงได้จัดทำหนังสือ “ข้อกฎหมาย ความรู้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒” เพื่อเผยแพร่ให้กับข้าราชการตำรวจ หรือผู้เกี่ยวข้อง ได้ใช้ในการปฏิบัติ หน้าที่ให้ถูกต้อง เป็นไปตามกฎหมาย และไม่ล่วงละเมิดสิทธิความเป็น ส่วนตัวของประชาชนที่กฎหมายให้ความคุ้มครองไว้

พลตำรวจนครบาล 
(สุวัฒน์ แจ้งยอดสุข)

ผู้บัญชาการตำรวจนครบาล

๙ กันยายน ๒๕๖๕

คำปราารภ

การคุ้มครองข้อมูลส่วนบุคคล ถือเป็นเรื่องที่สำคัญ
เนื่องจากเป็นสิทธิความเป็นส่วนตัวของประชาชนที่รัฐต้องให้ความ
คุ้มครองมิให้เกิดการล่วงละเมิด ดังนั้นจึงได้มีการตราพระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ขึ้นโดย เป็นกฎหมายที่บัญญัติ
เกี่ยวกับหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้
ความคุ้มครองข้อมูลส่วนบุคคล และมีบทกำหนดโทษสำหรับผู้ที่ฝ่าฝืน
ไม่ปฏิบัติตามกฎหมายฉบับนี้

สำนักงานตำรวจแห่งชาติ ได้ตระหนักรึงความสำคัญ
ของการคุ้มครองข้อมูลส่วนบุคคล จึงได้จัดทำหนังสือ “ข้อกฎหมาย
ควรรู้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒” ขึ้น
เพื่อเผยแพร่ให้กับข้าราชการตำรวจ หรือผู้เกี่ยวข้อง ได้ใช้ในการศึกษา
ค้นคว้าให้เกิดความรู้ ความเข้าใจ และสามารถนำไปใช้ในการปฏิบัติหน้าที่
ได้อย่างถูกต้อง เป็นไปตามกฎหมาย และคุ้มครองสิทธิความเป็นส่วนตัว
ของประชาชนมิให้ถูกล่วงละเมิด

ผลตำรวจนอก

(สุวนิ ทรัพย์พ่วง)

รองผู้บัญชาการตำรวจนครบาล

ผู้อำนวยการศูนย์บริหารงานสอบสวน

๙ กันยายน ๒๕๖๕

คำนำ

ปัจจุบันมีการล่วงละเมิดข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลส่วนตัว เป็นจำนวนมาก เป็นเหตุให้ประชาชนได้รับความเดือดร้อนรำคาญและ ความเสียหาย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ จึงมีเจตนาرمณ์ที่จะให้การคุ้มครองข้อมูลส่วนบุคคล และมีมาตรการ เยียวยาเจ้าของข้อมูลส่วนบุคคลจากการกระทำดังกล่าว และการที่จะ ดำเนินการให้เป็นไปตามเจตนาرمณ์ของกฎหมายพนักงานสอบสวน หรือเจ้าหน้าที่ตำรวจต้องมีความรู้ ความเข้าใจในกฎหมาย และต้อง ระมัดระวังในการบังคับใช้กฎหมายให้ถูกต้องด้วย มีฉะนั้นอาจส่งผล เสียหายและสร้างความเดือดร้อนให้กับประชาชนไม่เป็นไปตาม เจตนาرمณ์ของกฎหมายที่ต้องการให้ความคุ้มครอง

หนังสือเล่มนี้จัดทำขึ้น เพื่อให้พนักงานสอบสวน และเจ้าหน้าที่ ตำรวจเข้าใจในหลักของกฎหมายดังกล่าวซึ่งเป็นกฎหมายใหม่ และหวังว่า หากได้เข้าใจในหลักกฎหมายดังกล่าวแล้วจะทำให้การปฏิบัติหน้าที่ เป็นไปอย่างถูกต้อง และเกิดประโยชน์ต่อประชาชนสืบไป

ผลสำรวจโดย

ผู้ทรงคุณวุฒิพิเศษ สำนักงานตำรวจแห่งชาติ

(ชนาชัย ลิ้มประเสริฐ)

๙ กันยายน ๒๕๖๒

สารบัญ

Part I: PDPA ๑๐๑.....	๑
๑. หลักการสำคัญของ PDPA	๑
๑.๑ PDPA คืออะไร	๑
๑.๒ สำนักงานต่างประเทศ แลเจ้าหน้าที่ต่างๆทุกคน จะยังใช้ข้อมูลได้อยู่หรือไม่ ภายใต้ PDPA	๒
๑.๓ หลักการสำคัญง่าย ๆ ที่สำนักงานต่างประเทศต้องดำเนินการให้เป็นไปตาม PDPA ...	๒
๒. ขอบเขตของการบังคับใช้ PDPA.....	๓
๒.๑ PDPA ใช้อย่างไร กับใคร	๓
๒.๒ มีใครหรือกระบวนการใช้ข้อมูลไหนที่ได้รับการยกเว้นจาก PDPA หรือไม่	๔
๒.๓ PDPA มีผลบังคับโดยตรงกับเจ้าหน้าที่ต่างๆโดยไม่	๖
๓. คำศัพท์สำคัญ.....	๗
มาตรา ๖ ข้อมูลส่วนบุคคลคืออะไร	๗
มาตรา ๒๖ ข้อมูลส่วนบุคคลอ่อนไหวคืออะไร	๘
เจ้าของข้อมูลส่วนบุคคลหมายถึงใคร	๑๐

การประมวลผลข้อมูลส่วนบุคคลที่ต้องทำตาม PDPA หมายถึงกระบวนการใด	๑๑
ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล คือใคร	๑๓
๔. หน้าที่หลักของสำนักงานตรวจสอบแห่งชาติ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล	๑๖
๔.๑ ประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็น	๑๖
๔.๒ ข้อมูลส่วนบุคคล (Record of Processing)	๑๖
๔.๓ การแจ้งประมวลผลข้อมูลส่วนบุคคล	๑๘
๔.๔ การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล	๒๐
๔.๕ การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)	๒๑
๕. ความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลได้ใช้ได้ภายใต้ PDPA	๒๓
๕.๑ ฐานกฎหมาย (Legal Obligations)	๒๓
๕.๒ ฐานประโยชน์สาธารณะและการใช้อำนาจรัฐ (Public Tasks)	๒๔
๕.๓ ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)	๒๖
๕.๔ ฐานการวิจัยหรือทำสถิติ (Research / Archives)	๒๗
๕.๕ ฐานสัญญา (Contractual Performance)	๒๗
๕.๖ ฐานความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)	๒๙

๔.๗ ฐานความยินยอม (Consent) ต้องขอในกรณีใดบ้าง.....	๓๐
๔.๘ การประเมินฐานการประมวลผลข้อมูลอันชอบด้วยกฎหมาย (Lawful Basis).....	๓๑
๔.๙ สรุปเอกสารที่เจ้าหน้าที่สำรวจต้องทำและแจ้ง ภายใต้ PDPA.....	๓๒
๖. การรักษาความมั่นคงปลอดภัยต้องทำอย่างไรจึงจะเรียกว่า เพียงพอเหมาะสม ภายใต้ PDPA	๓๓
๗. กรณีมีการส่งต่อเปิดเผยข้อมูลส่วนบุคคลไปนอกองค์กร โดยเฉพาะส่งต่อให้แก่หน่วยงาน ที่ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล.....	๓๔
๘. สิทธิเจ้าของข้อมูลส่วนบุคคล มีอะไรบ้าง ภายใต้ PDPA	๓๗
๙. โทษของการไม่ปฏิบัติตาม PDPA มีอะไรบ้าง	๔๐
Part II: FAQ for PDPA Application.....	๔๑
คำถามที่ ๑. การค้นบุคคล	๔๑
๑.๑ ส่วนที่เกี่ยวข้องกับ PDPA	๔๑
๑.๒ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล	๔๒
๑.๓ สิ่งที่ต้องดำเนินการ	๔๒
คำถามที่ ๒. การจับกุมผู้ถูกจับ	๔๔
๒.๑ ส่วนที่เกี่ยวข้องกับ PDPA	๔๔

๒.๒ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล	๔๔
๒.๓ สิ่งที่ต้องดำเนินการ	๔๕
๒.๔ กระบวนการขอข้อมูลจากบุคคลภายนอก (ขอความร่วมมือ) เช่น กล้องวงจรปิด / ธนาคาร หรือบุคคลอื่น	๔๖
คำถามที่ ๓. การแฉลงข่าวจับกุม	๔๗
๓.๑ ส่วนที่เกี่ยวข้องกับ PDPA	๔๘
๓.๒ การแฉลงข่าวจับกุม	๔๙
๓.๓ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล	๔๙
๓.๔ หลักการสำคัญที่ต้องพิจารณา คือ	๕๐
๓.๕ สิ่งที่ต้องดำเนินการ	๕๐
๓.๖ กรณีในส่วนข้อมูลของผู้เสียหาย ต้องปิดบังไว้ตลอดเวลา	๕๑
คำถามที่ ๔. การจัดทำทะเบียน.....	๕๑
๔.๑ ส่วนที่เกี่ยวข้องกับ PDPA	๕๑
๔.๒ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล	๕๒
๔.๓ สิ่งที่ต้องดำเนินการ	๕๓
๔.๔ การส่งต่อไปด้วยรายชื่อบุคคลต้องห้าม	๕๓

๔.๕ การติดภาพของบุคคลต้องห้ามไว้ในพื้นที่ปฏิบัติงานที่ประชาชนอื่นอาจเห็นได้	๔๕
คำถามที่ ๕. การส่งต่อเปิดเผยข้อมูลไปให้แก่หน่วยงานหรือบุคคลภายนอก.....	๕๖
๕.๑ ส่วนที่เกี่ยวข้องกับ PDPA	๕๖
๕.๒ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล	๕๗
๕.๓ สิ่งที่ต้องดำเนินการ	๕๘
คำถามที่ ๖. การเปิดให้บุคคลตรวจสอบประวัติอาชญากรรม	๕๙
๖.๑ ส่วนที่เกี่ยวข้องกับ PDPA – ประวัติอาชญากรรมจากเจ้าหน้าที่ตำรวจ	๕๙
๖.๒ กรณีเจ้าของข้อมูลส่วนบุคคลขอตรวจสอบเอง	๖๐
๖.๓ กรณีนายจ้างขอตรวจข้อมูลของเจ้าของข้อมูลส่วนบุคคล	๖๐
คำถามที่ ๗. ระบบ CRIMES.....	๖๐
๗.๑ ส่วนที่เกี่ยวข้องกับ PDPA	๖๐
๗.๒ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล	๖๑
๗.๓ สิ่งที่ต้องดำเนินการ	๖๑
คำถามที่ ๘. ประเภทคดีเข้าข่ายและไม่เข้าข่ายที่เจ้าหน้าที่ตำรวจต้องดำเนินการ	๖๓
๘.๑ กรณีการใช้ประมวลผลข้อมูลส่วนบุคคล	๖๓
๘.๒ โทษอาญาภายใต้ PDPA	๖๓

๔.๓ ความผิดนอกเหนือจากความรับผิดทางอาญา.....	๖๕
บรรณานุกรม	๖๗
ประวัติผู้เรียบเรียง	๗๐
คณะผู้จัดทำ.....	๗๑
บันทึกช่วยจำ	๗๓

PDPA for Police Guideline

Part I: PDPA ๑๐๑

๑. หลักการสำคัญของ PDPA

๑.๑ PDPA คืออะไร?

- PDPA ย่อมาจาก Personal Data Protection Act หรือชื่อภาษาไทย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ประกาศใช้ในปี พ.ศ. ๒๕๖๒ และมีผลบังคับใช้สมบูรณ์ในวันที่ ๑ มิถุนายน พ.ศ. ๒๕๖๕
- จุดประสงค์หลักของ PDPA ต้องการป้องกันคุ้มครองสิทธิ “เจ้าของ ข้อมูลส่วนบุคคล” ซึ่งเป็นบุคคลธรรมดा โดยการกำหนด “กรอบ” การใช้ข้อมูลส่วนบุคคลที่บุคคลหรือนิติบุคคลได้จะใช้ข้อมูลของบุคคลนั้น ๆ ภายใต้หลักการที่ต้อง “ไม่ให้กระทบสิทธิ” เจ้าของ ข้อมูลส่วนบุคคลมากเกินความจำเป็น
- การคุ้มครองสิทธิเจ้าของข้อมูลส่วนบุคคล คือ เจ้าของข้อมูลมีสิทธิ ที่จะได้รับแจ้งและรับทราบการใช้ข้อมูล และมีสิทธิที่จะควบคุม การใช้ข้อมูลของตนเองได้มากขึ้น เช่น สิทธิในการขอเข้าถึง ขอรับ สำเนาคัดค้าน ระงับการใช้ข้อมูลส่วนบุคคล สิทธิขอลบข้อมูล รวมไปถึงสิทธิในการร้องเรียนหากมีการใช้ข้อมูลไม่ถูกต้อง

๑.๒ สำนักงานติดตามและเจ้าหน้าที่ติดตามทุกคน จะยังใช้ข้อมูลได้อよู่หรือไม่ ภายใต้ PDPA?

- PDPA ไม่ได้ห้ามเจ้าหน้าที่ติดตามใช้ข้อมูลส่วนบุคคล ดังนั้น สำนักงานติดตามและเจ้าหน้าที่ติดตามทุกคนจะยังคงใช้ข้อมูลส่วนบุคคล ของบุคคลธรรมดายกเว้น
- แต่ในการใช้ข้อมูลส่วนบุคคลนั้น สำนักงานติดตามและเจ้าหน้าที่เพิ่มเติม ดังนี้ (๑) ต้องคิดพิจารณาความจำเป็นในการใช้ข้อมูลให้มากขึ้น (๒) ต้องดำเนินการขั้นตอนบางอย่างเพิ่มเติม ก่อนและระหว่าง การใช้ข้อมูลส่วนบุคคล และ (๓) ต้องเคารพสิทธิของเจ้าของข้อมูลส่วนบุคคลที่อาจขอใช้เกียร์ข้อมูลกับเจ้าของข้อมูลของตนเองมากขึ้น

๑.๓ หลักการสำคัญง่าย ๆ ที่สำนักงานติดตามและเจ้าหน้าที่ต้องดำเนินการให้ เป็นไปตาม PDPA มีอะไรบ้าง?

- จำเป็น / แจ้ง / รักษาความปลอดภัย / เคารพสิทธิ
- ตามมาตรา ๒๒ จำเป็น (Necessity) ต้องประเมินความจำเป็น ในการเก็บ รวบรวม ใช้ ประมวลผลข้อมูลส่วนบุคคลของบุคคลอื่น มากขึ้น โดยเฉพาะต้องสามารถอธิบายถึง วัตถุประสงค์ ในการเก็บ ใช้ข้อมูลส่วนบุคคลดังกล่าวให้ได้ในทุกรอบวนการ และ ต้องประเมินความจำเป็นภายใต้กรอบ ใจเขาใจเรา เพื่อไม่ให้ กระทบสิทธิเจ้าของข้อมูลส่วนบุคคลมากเกินความจำเป็น
- ตามมาตรา ๒๓ แจ้ง (No Surprise) ต้องแจ้งให้เจ้าของข้อมูลทราบ ก่อนหรือขณะที่จะมีการเก็บข้อมูลส่วนบุคคลว่า สำนักงานติดตามและเจ้าหน้าที่จะเก็บข้อมูลส่วนบุคคลใดบ้าง จุดประสงค์เพื่ออะไร

เก็บไว้นานเท่าใด ส่งต่อให้ครัวเรือน และในบางกรณีอาจจำเป็นต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน จึงจะสามารถใช้ข้อมูลส่วนบุคคลนั้นได้

สำหรับช่องทางการแจ้ง สามารถแจ้งฝ่ายเดียวสู่สาธารณะเป็นการทั่วไป เช่น การแจ้งประกาศผ่านเว็บไซต์ของตำรวจ หรือการติดประกาศไว้ในบริเวณพื้นที่ สำนักงานตำรวจนแห่งชาติ ไม่จำเป็นต้องแจ้งเป็นรายครั้ง

- ตามมาตรา ๓๗ รักษาความปลอดภัย (Keep it Safe) เมื่อเก็บรักษาข้อมูลส่วนบุคคลมาแล้ว สำนักงานตำรวจนแห่งชาติต้องรักษาความปลอดภัยของข้อมูล ซึ่งรวมถึง การรักษาความลับ การรักษาความถูกต้อง และรักษาความพร้อมในการใช้งานของข้อมูลนั้นอยู่เสมอ
- ตามหมวด ๓ เคารพสิทธิ (Respect the Right) ต้องเคารพและตอบสนองตามสิทธิที่เจ้าของข้อมูลส่วนบุคคลอาจขอใช้เกี่ยวข้องโดยตรงกับข้อมูลส่วนบุคคลของตนเอง ไม่ว่าจะยอมรับหรือปฏิเสธ ก็ต้องตอบรับ และบันทึกการขอใช้สิทธินั้นไว้

๒. ขอบเขตการบังคับใช้ของ PDPA

๒.๑ PDPA ใช้กับบุคคลดังนี้ต่อไปนี้

- ตามมาตรา ๕ ใช้กับการประมวลผลข้อมูลส่วนบุคคล โดยบุคคล ไม่ว่าจะเป็นบุคคลธรรมดा หรือนิติบุคคลที่จดทะเบียนตั้งบริษัทอยู่ในราชอาณาจักรหรือที่อยู่นอกราชอาณาจักร ซึ่งประมวลผลข้อมูลส่วนบุคคลของบุคคลที่อยู่ในราชอาณาจักร

ໃກຣຕ້ອງປົກປັດຕາມ PDPA ບ້າງ

PDPA ໄປສັບ “ບຸຄຄລທີ່ໃຊ້ຂອບໜຸລສ່ວນບຸຄຄລເຈັນ”
ກີ່ຈົກເປັນບຸຄຄລຮຽນບາຍເຮືອມືບຸຄຄລ ຮົບເຖິງ
ກັບຍົງນາງາຮາກາຮົກທີ່ຈະນົດທີ່ຈົດກະເບືອນເຖິງໃນ
ປະເກສໄກຍ ພິຈາລະນາຈົ່ງຢູ່ນອກປະເກສໄກຍແລ້ວ
ໃຊ້ຂອບໜຸລຂອງຄົນໃນປະເກສ

- 01** 
ບຸຄຄລຮຽນ
ກີ່ໃຊ້ຂອບໜຸລເຈັນໃນກາຮາຮົກ
- 02** 
ນີ້ບຸຄຄລຫອງຄົກທີ່ຈົດກະເບືອນ
ຈັດຕື່ອຳນັດໃນປະເກສໄກຍ
- 03** 
ກັບຍົງຈາບຮັງ
ແລ້ວກັບຍົງຈາບຮັງວິສາຫະກົດ
- 04** 
ບັນຫຼາດປະເກສ
ກີ່ໃຊ້ຂອບໜຸລນີ້ໃນປະເກສ

໢.໢ ກະບວນກາຮົກໃໝ່ຂໍ້ອມຸລໃດທີ່ໄດ້ຮັບກາຮົກເວັນບັງຄັບໃໝ່ຈາກ PDPA

- ກາຮົກໃໝ່ຂໍ້ອມຸລສ່ວນບຸຄຄລເພື່ອປະໂຍ່ນສ່ວນຕົວ ສ້າງຄວາມຮັກຮັກ
ຂອງເຈົ້າຂອງຂໍ້ອມຸລສ່ວນບຸຄຄລນີ້ເອງ ໄດ້ຮັບກາຮົກເວັນຈາກກາຮົກ
ປົກປັດຕາມ PDPA ດັ່ງນີ້ ບຸຄຄລທີ່ໄວ້ໄປສາມາດຄຳໄຍງ້ຮູບ Selfie ແລ້ວ
ລົງ Social Media ຕົວເອງໄດ້ ບຸຄຄລທີ່ໄວ້ໄປຢັ້ງສາມາດຕິດກັບລົງວິຈາ
ປິດ ໃນບັນຫຼາດປະເກສ ສ້າງຄວາມຮັກຮັກຂອງຕົວເອງໄດ້ ໂດຍໄມ່ມີ
ໜ້າທີ່ທຳມານ PDPA
- ກາຮົກປະມວລຜົລຂໍ້ອມຸລສ່ວນບຸຄຄລຂອງຕຳມະຈາກກະບວນກາຮົກ
ໄດ້ຮັບຂໍ້ອຍກເວັນ

- ◊ มาตรา ๔ (๒) การประมวลผลข้อมูลส่วนบุคคล โดยสำรวจ
ที่มีหน้าที่ดำเนินการเพื่อการรักษาความปลอดภัย
ของประชาชน
- ◊ มาตรา ๔ (๕) การประมวลผลข้อมูลส่วนบุคคลในระหว่าง
ขั้นตอนดำเนินกระบวนการยุติธรรมทางอาญา
- ◊ นอกจากทั้งสองกระบวนการนี้ไม่ได้รับการยกเว้น การประมวลผล
ข้อมูลส่วนบุคคลของสำนักงานตำรวจแห่งชาติในกระบวนการ
อื่นนอกเหนือจากที่กำหนดไว้ในมาตรา ๔ (๒) และ (๕)
เช่น การใช้ข้อมูลส่วนบุคคลในกระบวนการว่าจ้าง และ
บริหารจัดการทรัพยากรบุคคลภายนอกในสำนักงาน เป็นต้น
ไม่ได้รับการยกเว้น (เว้นแต่มีการประกาศพระราชบัญญัติฯ
ยกเว้นเป็นการเฉพาะเพิ่มเติม) ดังนั้น ในกระบวนการ
ประมวลผลข้อมูลส่วนบุคคลส่วนอื่นของสำนักงานตำรวจ
ยังคงมีหน้าที่ต้องปฏิบัติตาม PDPA
- ◊ การยกเว้นมาตรา ๔ ยกเว้นเพียงหน้าที่การแจ้ง มาตรา ๔
โดยยกเว้นเพียงหน้าที่ในการแจ้งการประมวลผลข้อมูล
ส่วนบุคคลหรือการขอความยินยอม (ในบางกรณี) แต่ มาตรา ๔
วรรคท้าย กำหนดว่า ตำรวจนายังคงมีหน้าที่ในการ (๑) รักษา
ความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Keep it Safe) และ
(๒) ต้องเคารพสิทธิเจ้าของข้อมูลส่วนบุคคล (Respect the
Right)

๒.๓ PDPA มีผลบังคับโดยตรงกับเจ้าหน้าที่สำรวจแต่ละนาย ดังนี้

- ภายใต้ PDPA มีเพียงสำนักงานสำรวจแห่งชาติ ซึ่งเป็นต้นสังกัดที่ทำ การตัดสินใจการประมวลผลข้อมูลส่วนบุคคลทั้งหมดขององค์กร เท่านั้นที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และมีหน้าที่โดยตรงต้องดำเนินการต่าง ๆ ตามที่กำหนดไว้ภายใต้ PDPA
- ผู้ที่ทำงานภายใต้สังกัดองค์กร ที่มีฐานะเป็นผู้ควบคุมข้อมูล ส่วนบุคคล เช่น เจ้าหน้าที่สำรวจแต่ละนาย หากดำเนินการตาม ขอบเขตหน้าที่ ตามกฎหมายและตามคำสั่งของต้นสังกัดของ สำนักงานสำรวจแห่งชาติแล้ว เจ้าหน้าที่แต่ละรายดังกล่าวจะไม่มี หน้าที่ความรับผิดโดยตรงภายใต้ PDPA อีก ถือว่าเป็นการ ดำเนินการในฐานะส่วนหนึ่งของสำนักงานสำรวจแห่งชาติเท่านั้น
- เมื่อสำนักงานสำรวจแห่งชาติเป็นผู้ควบคุมข้อมูลส่วนบุคคล การกระทำการของเจ้าพนักงาน จะถือเป็นการดำเนินการในนาม และแทนสำนักงานสำรวจแห่งชาติเท่านั้น ดังนั้นจะไม่มีการแต่งตั้ง เจ้าหน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูล ส่วนบุคคลโดยเจ้าหน้าที่สำรวจแต่ละนายถือเป็นการดำเนินการของ สำนักงานสำรวจแห่งชาติ

๓. คำศัพท์สำคัญ

มาตรา ๖ ข้อมูลส่วนบุคคล คืออะไรบ้าง

- ข้อมูล ไม่ว่าจะเป็นข้อมูลเดียว หรือชุดข้อมูลที่รวมกันแล้ว สามารถระบุเชื่อมโยงตัวตนบุคคลธรรมดานั่นคนได้ ไม่ว่าทางตรงหรือทางอ้อม ไม่รวมข้อมูลของผู้ถึงแก่กรรม
 - ◊ ข้อมูลนิติบุคคล (เข่น องค์กรหรือบริษัท) ไม่ถือเป็นข้อมูลส่วนบุคคล แต่ข้อมูลผู้ถือหุ้น หรือกรรมการของนิติบุคคลตั้งกล่าวถือเป็นข้อมูลส่วนบุคคล
 - ◊ เจ้าของข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองสิทธิภายใต้ PDPA รวมทั้งเจ้าของข้อมูลส่วนบุคคลที่เป็น บุคคลสัญชาติไทย หรือต่างประเทศ
 - ◊ การระบุตัวตน ไม่จำเป็นต้องรู้จักตัวตนบุคคลนั้น ดังนั้น ด้วยภาพถ่ายใบหน้าคน เร��สามารถนำข้อมูลดังกล่าวไปเชื่อมตัวคนหนึ่งคนได้ แม้มันได้รู้จักว่า คนนั้นชื่ออะไร ดังนั้น ภาพถ่ายใบหน้าจึงเป็นข้อมูลส่วนบุคคล (Personal Data)
 - ◊ ตัวอย่างข้อมูลส่วนบุคคล ได้แก่ ชื่อ นามสกุล เบอร์โทรศัพท์ อีเมล สำเนาบัตรประจำตัวประชาชน Social Media Account
- ปัจจัยการพิจารณาว่า ข้อมูลไหนเป็นข้อมูลส่วนบุคคล ให้ประเมินว่า ในขอบเขตการเข้าถึงข้อมูลของสำนักงานตรวจแห่งชาตินั้น

สำนักงานตำรวจแห่งชาติสามารถนำข้อมูลดังกล่าวกลับมาใช้เพื่อรับข้อมูลของสำนักงานตำรวจแห่งชาติที่มีอยู่ในระบบคนหนึ่งคนใดหรือไม่ เช่น

- ◊ กรณีเลขรหัสเจ้าหน้าที่ตำรวจ ซึ่งเป็นเลขที่ได้รับการบันทึกในฐานข้อมูลของสำนักงานตำรวจแห่งชาติถือเป็นข้อมูลส่วนบุคคล เพราะเมื่อนำเลขดังกล่าวกลับมาค้นในฐานข้อมูลจะสามารถระบุตัวตนได้ทันทีว่า รหัสดังกล่าวคือ เจ้าหน้าที่คนไหน
- ◊ หากตำรวจได้ข้อมูลรหัสพนักงานของบริษัทหนึ่งมาแล้ว ไม่สามารถตรวจสอบ หรือระบุย้อนกลับไปได้ว่ารหัสนั้นคือรหัสประจำตัวของพนักงานคนไหน กรณีรหัสพนักงานของบริษัทนั้นไม่ถือเป็นข้อมูลส่วนบุคคลสำหรับการประมวลผลของสำนักงานตำรวจนั้น

มาตรา ๒๖ ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Identifiable Information (SPII))

- ข้อมูลส่วนบุคคลอ่อนไหว หมายถึง ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน และสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติไม่ว่าผู้เก็บข้อมูลนั้นมาจากการเลือกปฏิบัติจริงหรือไม่ก็ตาม
- PDPA กำหนดรายละเอียดของข้อมูลส่วนบุคคลที่ถือว่าเป็นข้อมูลส่วนบุคคลอ่อนไหวไว้เป็นการเฉพาะ หากไม่อยู่ในรายการดังกล่าว ไม่ถือว่า เป็นข้อมูลส่วนบุคคลอ่อนไหว
- ข้อมูลส่วนบุคคลอ่อนไหว ได้แก่ ข้อมูลพันธุกรรม (ยีนส์ และ DNA) ข้อมูลชีวภาพ / ชีวามตร ที่ใช้เทคโนโลยีมาสร้างแบบจำลอง

เพื่อระบุตัวตน (ลายนิ้วมือ แบบจำลองใบหน้า รูป่านตา) ข้อมูลสุขภาพ
กายและใจ ข้อมูลความพิการ เข็อชาติ เพาพันธุ์ ความคิดเห็น
ทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทาง
เพศ (LGBTQ) ประวัติอาชญากรรม (ที่ควบคุมโดยสำนักงานตำรวจ
แห่งชาติ) ข้อมูลสุขภาพแรงงาน และอาจรวมข้อมูลอื่นที่คณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคลอาจกำหนด

- ด้วยความอ่อนไหวของข้อมูล หากจะมีการประมวลผลข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้ความระมัดระวัง
มากกว่าข้อมูลส่วนบุคคลอื่น ได้แก่
 - ◊ ต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล
(เว้นแต่เข้าข้อยกเว้นที่มาตรา ๒๖ กำหนดไว้) และต้องแจ้งให้
ชัดเจนเกี่ยวกับวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล
อ่อนไหวดังกล่าว หากดำเนินการไม่ถูกต้อง อาจนำไปสู่โทษ
ทางปกครองสูงสุด ๕,๐๐๐,๐๐๐ บาท
 - ◊ ต้องรักษาความปลอดภัยมากขึ้น โดยเฉพาะหากข้อมูลส่วน
บุคคลอ่อนไหวนั้นร่วมหลอกไป ทำให้เกิดความเสียหาย
สำนักงานตำรวจแห่งชาติ และผู้บัญชาการสำนักงานตำรวจ
แห่งชาติ ผู้เป็นหน้าที่รับผิดชอบในส่วนงานดังกล่าว อาจต้องรับ
โทษอาญา (รวมถึงปรับและจำคุก) ภายใต้ PDPA
- ข้อควรพิจารณา
 - ◊ หลีกเลี่ยงการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว
โดยไม่จำเป็น เช่น การประมวลผลข้อมูลเข็อชาติ ศาสนา

ในแบบฟอร์มต่าง ๆ หากไม่จำเป็นต้องเก็บข้อมูลส่วนบุคคล
ดังกล่าว

- ◊ เจ้าหน้าที่สำรวจเป็นผู้ประมวลผล เก็บรักษา และเผยแพร่
ข้อมูลส่วนบุคคลอ่อนไหวหลายส่วน โดยเฉพาะ ประวัติ
อาชญากรรม ดังนั้น ต้องใช้ความระมัดระวังอย่างมากในการ
เก็บรักษาความปลอดภัยข้อมูลดังกล่าวไม่ให้หลุดรั่วไหล
หรือถูกเข้าถึง แก้ไข ลบ หรือเปลี่ยนแปลง โดยไม่ได้รับ
อนุญาต
- ◊ ในกระบวนการดำเนินคดี เจ้าหน้าที่สำรวจอาจมีโอกาสเข้าถึง
และใช้ประมวลผลข้อมูลสุขภาพของผู้เสียหาย (เช่น ข้อมูล
ความบาดเจ็บหรือพิการทุพพลภาพ) และจำเป็นต้องประมวลผล
ข้อมูลส่วนบุคคลดังกล่าวในฐานะที่เป็นพยานหลักฐานเช่นกัน
และด้วยความอ่อนไหวของข้อมูลนั้น ต้องมีกระบวนการในการ
รักษาความปลอดภัยให้ได้เป็นพิเศษ
- ◊ ข้อมูลรายนี้มีผู้ต้องหาที่สำรวจเก็บเข้าฐานข้อมูล
โดยเชื่อมโยงระบุตัวตนบุคคลได้ เป็นอีกประเภทของข้อมูล
ชีวภาพ ที่ถือเป็นข้อมูลส่วนบุคคลอ่อนไหว ที่ต้องรักษาความ
ปลอดภัยพิเศษเพิ่มเติม

เจ้าของข้อมูลส่วนบุคคล หมายถึงใคร (Subject Information)

- เจ้าของข้อมูลส่วนบุคคล หมายถึง บุคคลธรรมดานั่วไปที่ข้อมูลส่วน
บุคคลเหล่านั้น เชื่อมโยงระบุถึงบุคคลเหล่านั้นได้ และเป็นผู้ที่ได้รับ¹
การปกป้องและคุ้มครองสิทธิสูงสุดภายใต้ PDPA

- เจ้าของข้อมูลส่วนบุคคลมีหลากหลาย รวมถึง บุคคลภายนอกและบุคคลภายนอกในองค์กรตัววิจัย ซึ่งแต่ละกลุ่มเจ้าของข้อมูลส่วนบุคคลล้วนมีสิทธิและได้รับการคุ้มครองเท่าเทียมกัน
- กลุ่มเจ้าของข้อมูลที่เกี่ยวข้องซึ่งสำนักงานตัววิจัยแห่งชาติอาจมีความจำเป็นต้องประมวลผลข้อมูล ได้แก่
 - ◊ ประชาชนที่เข้ามาติดต่อ และ/หรือใช้บริการของสำนักงานตัววิจัยแห่งชาติ หน่วยงานภายใต้สังกัดสำนักงานตัววิจัยแห่งชาติ หรือโรงพยาบาลตัววิจัย
 - ◊ ผู้ต้องหา ผู้ต้องขัง หรือบุคคลที่อยู่ภายใต้การควบคุมของสำนักงานตัววิจัยแห่งชาติ
 - ◊ เจ้าหน้าที่ตัววิจัย เจ้าหน้าที่สำนักงานตัววิจัยแห่งชาติวิจัย ไม่ว่าจะเป็นพนักงานในตำแหน่งประจำ หรือชั่วคราวหรือรายวัน
 - ◊ คู่สัญญา ผู้ให้บริการภายนอก ผู้ที่เข้ามาให้บริการในกระบวนการจัดซื้อจัดจ้าง

การประมวลผลข้อมูลส่วนบุคคลที่ต้องทำตาม PDPA หมายรวมถึงกระบวนการใดบ้าง

- การประมวลผลข้อมูลส่วนบุคคล ภายใต้เงื่อนไขที่ระบุไว้ของ PDPA ครอบคลุมทุกรอบวนการใช้ข้อมูลส่วนบุคคล (Data Lifecycle) กล่าวคือ ตั้งแต่การเก็บ รวบรวม ประมวลผล ใช้ การเก็บรักษา

ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลนั้นยังอยู่ในความครอบครอง และการส่งต่อเปิดเผยออกไปภายนอกองค์กร

- การดำเนินการทุกกระบวนการประมวลผลข้อมูลส่วนบุคคลตามนิยาม ดังกล่าวโดยสำนักงานตำรวจแห่งชาติ ถือเป็นการประมวลผลข้อมูล ส่วนบุคคลที่สำนักงานตำรวจนายที่ต้องปฏิบัติตาม PDPA ทั้งหมด

การประมวลผลข้อมูลภายใต้ PDPA เริ่มต้นแต่ "เก็บ"

⌚ เก็บรวบรวม
(Collect)

ได้เอง หรือได้จากบุคคลอื่น

ใช้งาน
(Process)

🔒 เก็บรักษา
(Storage)

ก็งในรูปแบบที่เป็นกระดาษ
และเป็นระบบ Electronic

เปิดเผย/ส่งต่อ
(Disclose/Transfer)

ไปยังองค์กร

การประมวลผลข้อมูลเริ่มต้นแต่ "เก็บ" ต่อเนื่องตลอด
ระยะเวลาที่ข้อมูลยังอยู่ใน "ครอบครอง"

- ตัวอย่างการประมวลผลข้อมูลส่วนบุคคล รวมกระบวนการ ดังนี้
 - ◊ การเก็บ รวบรวม (Collect) ไม่ว่าจะเป็น กรณีที่ (๑) เจ้าของ ข้อมูลนำข้อมูลนั้นมาส่งให้ (๒) ระบบหรืออุปกรณ์ของตำรวจ อาจเก็บรวบรวมโดยอัตโนมัติ เช่น การเก็บข้อมูลจาก กล้องวงจรปิด หรือระบบ Logs หรือ (๓) จากการที่มีบุคคลภายนอก ส่งข้อมูลของบุคคลอื่นมาให้แก่ตำรวจเพื่อใช้ในการประมวลผล

- ◊ การใช้งาน (Use) ภายในสำนักงานติดตามและตรวจสอบ ไม่ว่าจะดำเนินการโดยหน่วยงานใด
 - ◊ การเก็บรักษาไว้จนกว่าจะนำไปสู่การทำลาย ไม่ว่าจะจัดเก็บในรูปแบบกระดาษ หรืออิเล็กทรอนิกส์
 - ◊ การเปิดเผย หรือส่งต่อออกไปที่หน่วยงานหรือบุคคลภายนอก สังกัดของสำนักงานติดตามและตรวจสอบ ซึ่งรวมถึงการใช้ระบบเทคโนโลยีสารสนเทศภายนอก (เช่น Cloud / Server) หรือการใช้บริการผู้ใช้ บริการภายนอก รวมถึงการส่งต่อเปิดเผยข้อมูลให้แก่ที่ปรึกษา หรือการส่งต่อให้แก่หน่วยงานราชการอื่น หรือการส่งข้อมูลเปิดเผยข้อมูลให้แก่บุคคลผู้ร้องขอที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคล
- ในทุกรอบวนการประมวลผลข้อมูลส่วนบุคคลที่สำนักงานติดตามและตรวจสอบ จะดำเนินการ สำนักงานติดตามและตรวจสอบ มีหน้าที่สำคัญภายใต้ PDPA ที่ต้องรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่อยู่ระหว่างการประมวลผลไม่ว่าในขั้นตอนใดก็ตาม

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller (DC)) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor (DP)) คือใคร

- ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล เป็นผู้ใช้ และประมวลผลข้อมูลส่วนบุคคลของบุคคลอื่นทั้งคู่

- ฐานะการเป็น ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล จะเกิดขึ้นเฉพาะกรณีที่มีการส่งต่อเปิดเผยข้อมูลส่วนบุคคลไปนอกองค์กรเท่านั้น
 - ◊ การประมวลผลข้อมูลส่วนบุคคล โดยบุคลากรหรือแม่กระแทก หน่วยงานที่อยู่ภายใต้สังกัดของสำนักงานตำรวจแห่งชาติ จะไม่เกิดความสัมพันธ์ที่เจ้าหน้าที่ตำรวจ หรือหน่วยงานภายในดังกล่าว จะมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ภายใต้ PDPA มีเพียง สำนักงานตำรวจนครบาลเท่านั้นที่มีฐานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล”
- มาตรา ๖ ระบุนิยาม ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ว่าหมายถึง องค์กรที่เป็นผู้ตัดสินใจ และกำหนดว่า จะมีการเก็บรวบรวม ใช้และประมวลผลข้อมูลส่วนบุคคลนั้นๆ อย่างไร
 - ◊ สำนักงานตำรวจนครบาล เป็นผู้ตัดสินใจเก็บข้อมูลเพื่อการบันทึกประจำวัน หรือแบบฟอร์มต่าง ๆ หรือการจัดทำระบบทะเบียน หรือระบบ CRIMES ดังนั้น สำนักงานตำรวจนครบาล จึงมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล สำหรับข้อมูลส่วนบุคคลที่ดำเนินการในกระบวนการดังกล่าว
 - ◊ สำนักงานตำรวจนครบาล ซึ่งเป็นผู้ตัดสินใจกำหนดกระบวนการในการรับสมัครพนักงานที่ จำกัด ทำงานภายใต้สังกัด ดังนั้น สำนักงานตำรวจนครบาล เป็นผู้ควบคุมข้อมูลส่วนบุคคล ของพนักงานทั้งหมด

- มาตรา ๖ ระบุนิยาม ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ว่าหมายถึง องค์กรที่ทำการประมวลผลข้อมูลส่วนบุคคล ตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล
 - ◊ ยกตัวอย่างเช่น ผู้ให้บริการแพตช์ระบบเทคโนโลยีสารสนเทศที่เก็บ รวบรวม ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ระบุไว้ในขอบเขตของการว่าจ้าง (TOR) ที่สำนักงานตำรวจแห่งชาติ เป็นผู้กำหนดออกคำสั่ง จะมีฐานะเป็น ผู้ประมวลผลข้อมูล ส่วนบุคคล
- โดยหลัก ทุกการประมวลผลข้อมูลส่วนบุคคลโดยสำนักงานตำรวจนแห่งชาติเป็นการประมวลผลข้อมูลส่วนบุคคลในฐานะ ผู้ควบคุม ข้อมูลส่วนบุคคลทั้งหมด ในทุกกลุ่มเจ้าของข้อมูลส่วนบุคคล ยกเว้นเป็นกรณีเฉพาะที่สำนักงานตำรวจนแห่งชาติเพียงดำเนินการตามคำสั่งบังคับกฎหมายของหน่วยงานอื่น ที่นอกเหนือจากการปฏิบัติหน้าที่ในฐานะเป็นเจ้าหน้าที่ตำรวจนโดยตรง

๔. หน้าที่หลักของสำนักงานติดตามและตรวจสอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ประกอบด้วย

๔.๑ ประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็น (มาตรา ๒๒)

- สำนักงานติดตามและตรวจสอบที่พิจารณาความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล ด้วยการกำหนด วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลให้ได้หากมีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคล สำนักงานติดตามและตรวจสอบย่อมสามารถประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้
- นอกจากกำหนดวัตถุประสงค์แล้ว ต้องมีการกำหนดระยะเวลาในการประมวลผลข้อมูลส่วนบุคคลให้ชัดเจนมากขึ้น ซึ่งการเก็บข้อมูลตลอดไปไม่สามารถทำได้ตามหลักการ PDPA
 - ◊ ต้องมีกรอบระยะเวลาให้เจ้าของข้อมูลส่วนบุคคลคาดหมายได้ว่า จะเก็บไว้ภายใต้กรอบระยะเวลาใด แต่ไม่จำเป็นระบุเป็นตัวเลขปี เช่น เก็บรวบรวมตามกรอบระยะเวลาที่กฎหมายกำหนดไว้ หรือเก็บรวบรวมไว้ตลอดระยะเวลาที่สำนักงานติดตามและตรวจสอบที่ต้องปฏิบัติ เพื่อประโยชน์ของเจ้าของข้อมูล (เช่น ตลอดระยะเวลาตามสัญญาจ้างงานของพนักงาน)

๔.๒ จัดทำรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) มาตรา ๓๙

ยกเว้น ในส่วนที่ได้รับการยกเว้นจากการปฏิบัติหน้าที่ตาม PDPA (มาตรา ๔) ได้แก่ การประมวลผลข้อมูลเพื่อรักษาความปลอดภัยของประชาชน หรือการประมวลผลในการดำเนินคดีโดยบันทึกรายการ

กิจกรรมการประเมินผลข้อมูลส่วนบุคคล (ROP) ต้องรวมการบันทึกข้อมูลส่วนบุคคล ตั้งแต่ สำนักงานตำรวจนแห่งชาติได้รับข้อมูล นำข้อมูลส่วนบุคคลนั้นมาประเมินผล และส่งต่อข้อมูลดังกล่าวออกไปภายนอก

- ROP เป็นเอกสารที่จัดทำและเก็บรักษาไว้เป็นเอกสารภายในองค์กร ไม่จำเป็นต้องมีการส่งให้แก่บุคคลภายนอก แต่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลสามารถขอตรวจสอบได้
- หากไม่จัดทำบันทึกรายการการประเมินผลข้อมูลส่วนบุคคล สำนักงานตำรวจนแห่งชาติ อาจอยู่ภายใต้บังคับการปรับใหม่โทษปาก戎ในอัตราสูงสุด ๓,๐๐๐,๐๐๐ บาท
- การจัดทำบันทึกรายการการประเมินผลข้อมูลส่วนบุคคลเป็นการจัดทำกรอบ (Framework) สำหรับการประเมินผลข้อมูลส่วนบุคคล โดยรวมของแต่ละกลุ่มเจ้าของข้อมูล และในแต่ละกระบวนการ ไม่ใช่การบันทึกรายการการประเมินผลข้อมูลของเจ้าของข้อมูล เป็นรายบุคคล

ช่องทางได้รับข้อมูล	ระยะเวลาการจัดเก็บ	การส่งต่อข้อมูลให้ผู้อื่น	มาตรการรักษาความปลอดภัย
ส่วนตัวที่ได้รับโดยไม่ทราบหรือเห็นชอบด้วย มิใช่ความต้องการที่จะได้รับโดยที่ต้องการ หมายความว่า	ระยะเวลาการจัดเก็บ	ส่วนตัวที่ได้รับโดยไม่ทราบหรือเห็นชอบด้วย มิใช่ความต้องการที่จะได้รับโดยที่ต้องการ หมายความว่า	ส่วนตัวที่ได้รับโดยไม่ทราบหรือเห็นชอบด้วย มิใช่ความต้องการที่จะได้รับโดยที่ต้องการ หมายความว่า
ส่วนตัวที่ได้รับโดยไม่ทราบหรือเห็นชอบด้วย มิใช่ความต้องการที่จะได้รับโดยที่ต้องการ หมายความว่า	ระยะเวลาการจัดเก็บ	ส่วนตัวที่ได้รับโดยไม่ทราบหรือเห็นชอบด้วย มิใช่ความต้องการที่จะได้รับโดยที่ต้องการ หมายความว่า	ส่วนตัวที่ได้รับโดยไม่ทราบหรือเห็นชอบด้วย มิใช่ความต้องการที่จะได้รับโดยที่ต้องการ หมายความว่า
ส่วนตัวที่ได้รับโดยไม่ทราบหรือเห็นชอบด้วย มิใช่ความต้องการที่จะได้รับโดยที่ต้องการ หมายความว่า	ระยะเวลาการจัดเก็บ	ส่วนตัวที่ได้รับโดยไม่ทราบหรือเห็นชอบด้วย มิใช่ความต้องการที่จะได้รับโดยที่ต้องการ หมายความว่า	ส่วนตัวที่ได้รับโดยไม่ทราบหรือเห็นชอบด้วย มิใช่ความต้องการที่จะได้รับโดยที่ต้องการ หมายความว่า

๔.๓ แจ้งการประมวลผลข้อมูลส่วนบุคคล (มาตรา ๒๓)

- สำนักงานตำรวจนครบาล ต้องแจ้งการประมวลผลข้อมูลส่วนบุคคล เสมอ ยกเว้นการประมวลผลเพื่อการรักษาความปลอดภัย ของประชาชน หรือการดำเนินกระบวนการดำเนินคดี หรือกรณีได้รับ การยกเว้นเพิ่มเติมตามพระราชบัญญัติ (มาตรา ๔)
- ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล สำนักงานตำรวจนครบาล โดยอ้างอิงจาก “ความจำเป็นและวัตถุ ประสงค์การประมวลผล ข้อมูลส่วนบุคคล และบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล” มีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลรับทราบก่อน หรือขณะที่จะมีการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล ส่วนบุคคลกลุ่มนี้

- สำนักงานตำรวจนครบาล ต้องจัดทำและประกาศเอกสาร “ประกาศ เรื่อง แนวโน้มการคุ้มครองข้อมูลส่วนบุคคล” (Privacy Statement / Privacy Notice) ซึ่งต้องระบุข้อความรายละเอียดดังนี้
 - ◊ ควรจัดทำเอกสารแจ้ง Privacy Statement / Privacy Notice แยกกัน สำหรับการประมวลผลข้อมูลส่วนบุคคลของแต่ละกลุ่มเจ้าของข้อมูล เนื่องจากการประมวลผลข้อมูลส่วนบุคคลของแต่ละกลุ่มเจ้าของข้อมูลย่อมมีความแตกต่างกัน
 - ◊ การแจ้ง Privacy Statement / Privacy Notice นี้สามารถดำเนินการได้เพียงฝ่ายเดียว ไม่จำเป็น ต้องเก็บลายมือชื่อ หรือหลักฐานการได้รับทราบประกาศดังกล่าว แต่ควรประกาศผ่านช่องทางที่ชัดเจนเพียงพอที่ควรเชื่อถ้วน เจ้าของข้อมูลส่วนบุคคลทั้งหมดสามารถรับทราบประกาศดังกล่าว เช่น ติดประกาศในสถานที่สามารถมองเห็นได้ชัดเจนก่อนเข้าพื้นที่ สำนักงานตำรวจนครบาล หน้าเว็บไซต์ เป็นต้น
- การประมวลผลข้อมูลส่วนบุคคลบางประเภทหรือบางวัตถุประสงค์ (โดยเฉพาะ ข้อมูลส่วนบุคคลอ่อนไหว) อาจจำเป็นต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน
 - ◊ กรณีการขอความยินยอม ต้องแยกการขอความยินยอมออกจาก การแจ้งการประมวลผลข้อมูลส่วนบุคคลใน Privacy Statement / Privacy Notice และต้องบันทึกการให้ความ

ยินยอม พร้อมหลักฐาน การให้ความยินยอมของเจ้าของ
ข้อมูลส่วนบุคคลเป็นรายบุคคล

๔.๔ รักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (มาตรา ๓๗ (๑))

- หน้าที่ในการรักษาความมั่นคงปลอดภัย เป็นหน้าที่สำนักงานตัวรวจ
แห่งชาติต้องดำเนินการอยู่เสมอ สำหรับทุกการประมวลผลข้อมูล
ส่วนบุคคล ไม่มีข้อยกเว้น แม้จะเป็นกรณีการประมวลผลข้อมูล
ส่วนบุคคลที่ได้รับการยกเว้นตามมาตรา ๔
- สำนักงานตัวรวจแห่งชาติต้องรักษาความมั่นคงปลอดภัย ตามมาตรฐาน
ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดขึ้น
 - ◊ ต้องประเมินความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคล
ทั้งหมด ทั้งในเรื่องของข้อมูลส่วนบุคคลที่มีการประมวลผล
และวัสดุอุปกรณ์เครื่องมือที่ใช้ในการเก็บรักษาความปลอดภัย
ข้อมูลนั้น
 - ◊ อ้างอิงจากการประเมินความเสี่ยง ต้องจัดให้มีมาตรการ
เชิงองค์กร เชิงกายภาพ และเทคนิคอย่างเหมาะสม เพื่อรักษา
ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity)
และความพร้อมใช้งาน (Availability)
 - ◊ ข้อมูลส่วนบุคคลทั้งหมด ทั้งที่เก็บในรูปแบบกระดาษ
หรืออิเล็กทรอนิกส์ต้องได้รับการรักษาปกป้องไม่ให้สูญหาย
ถูกเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยโดยปราศจาก
อำนาจหรือโดยมิชอบจากทั้ง บุคลากรภายในและภายนอก
ของสำนักงานตัวรวจแห่งชาติ

- ◊ ต้องทบทวนมาตรการการรักษาความมั่นคงปลอดภัย เมื่อมีความจำเป็น โดยเฉพาะเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล
- หากเกิดเหตุละเมิดข้อมูลส่วนบุคคลอ่อนไหว และเหตุดังกล่าวสร้างผลกระทบรุนแรง (มาตรา ๓๗ (๔))
 - ◊ สำนักงานตรวจแห่งชาติต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลนั้นต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุ และหากกระทบสิทธิเจ้าของข้อมูลส่วนบุคคล สำนักงานตรวจแห่งชาติต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบด้วยเช่นกัน

๔.๕ การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) มาตรา ๔๑

- ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นหน่วยงานรัฐ เช่น สำนักงานตรวจแห่งชาติ มีหน้าที่ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน
- สำนักงานตรวจแห่งชาติ ต้องดำเนินการ (๑) แจ้งรายชื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และ (๒) แจ้งช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ ในประกาศ
 - ◊ หากไม่ดำเนินการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจต้องโทษปรับทางปกครองสูงสุด ๑,๐๐๐,๐๐๐ บาท

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ (มาตรา ๔๗) ดังนี้
 - ◊ ให้คำแนะนำการปฏิบัติตาม PDPA แก่หน่วยงานและเจ้าหน้าที่ ตัวรวมทั้งหมวดของสำนักงานที่ตรวจสอบให้ดำเนินการ
 - ◊ ตรวจสอบการดำเนินงานของสำนักงานที่ตรวจสอบให้เป็นไปตาม PDPA และนโยบายที่กำหนดได้
 - ◊ ประสานงาน และให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ที่สอบถามข้อมูลกรณีมีการร้องเรียน หรือติดต่อกับเจ้าของข้อมูลส่วนบุคคลกรณีมีการขอใช้สิทธิ
 - ◊ รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องมาจากการปฏิบัติหน้าที่เป็น DPO
 - ◊ รายงานตรงไปยังผู้บังคับบัญชาสูงสุดของสำนักงานที่ตรวจสอบให้ดำเนินการ หากมีปัญหาในการปฏิบัติหน้าที่ ดังนั้นต้องทำงานได้อย่างเป็นอิสระ
- สำนักงานที่ตรวจสอบให้ดำเนินการ ต้องจัดทำเครื่องมือหรืออุปกรณ์ที่เพียงพอ และอำนวยความสะดวกในการทำหน้าที่ของ DPO ให้ครบถ้วน
- สำนักงานที่ตรวจสอบให้ดำเนินการ ต้องมีให้ DPO ออกจากงานหรือเลิกสัญญาจ้างด้วยเหตุที่ DPO ปฏิบัติหน้าที่ของตนภายใต้ PDPA

๕. “ความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล” ที่ใช้ได้ ภายใต้ PDPA

- การประมวลผลข้อมูลส่วนบุคคลของสำนักงานตรวจสอบแห่งชาติท้องเมือง “วัตถุประสงค์” ต้องประเมินความจำเป็นของวัตถุประสงค์ดังกล่าว ภายใต้ PDPA โดยอ้างอิงจาก ฐานการประมวลผลข้อมูลโดยชอบด้วยกฎหมาย (Lawful Basis)



๔.๑ กฎหมาย Legal Obligations (มาตรา ๒๔ (๖))

- การประมวลผลข้อมูลส่วนบุคคลด้วยฐานกฎหมาย หมายถึง การประมวลผลข้อมูลส่วนบุคคลที่สำนักงานตำรวจแห่งชาติ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ตามกฎหมายต้องปฏิบัติ และเพื่อการปฏิบัติหน้าที่ตามกฎหมายดังกล่าว สำนักงานตำรวจแห่งชาติ จึงจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลดังกล่าว

- ตัวอย่าง
 - ◊ การเก็บและใช้เลขบัตรประจำตัวประชาชนของบุคคลที่สำนักงานตำรวจแห่งชาติว่าจ้าง เพื่อทำเอกสารหักภาษีณ ที่จ่ายและเก็บเอกสารบัญชีไว้ ตามข้อกำหนดของประมวลรัษฎากร
 - ◊ กรณีที่สำนักงานตำรวจแห่งชาติเก็บข้อมูล WiFi Logs / Traffic Logs ภายใต้หน้าที่ของ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และที่แก้ไขเพิ่มเติม
- กรณีฐานกฎหมาย เจ้าของข้อมูลส่วนบุคคลไม่สามารถปฏิเสธการประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ โดยสำนักงานตำรวจแห่งชาติ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บ รวบรวม ใช้และรักษาข้อมูลส่วนบุคคลดังกล่าวไว้ได้ตลอดระยะเวลาที่กฎหมายกำหนด

๕.๒ ฐานประโยชน์สาธารณะและการใช้อำนาจรัฐ (Public Tasks) (มาตรา ๒๔ (๔))

- การประมวลผลข้อมูลส่วนบุคคลด้วยฐานนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องเป็นหน่วยงานราชการที่มีอำนาจตามกฎหมายเฉพาะ

และเพื่อการปฏิบัติหน้าที่ตามกฎหมายดังกล่าว หน่วยงานรัฐนั้น
จึงจำเป็นต้องประมวลผลข้อมูลส่วนบุคคล

- กรณีของสำนักงานตำรวจแห่งชาติ ซึ่งมีหน้าที่ตาม พ.ร.บ.ตำรวจ
แห่งชาติ พ.ศ.๒๕๔๗ หรือกฎหมายอื่น หากเป็นการประมวลผล
ข้อมูลส่วนบุคคลซึ่งสำนักงานตำรวจแห่งชาติต้องดำเนินการเพื่อให้
บรรลุอำนาจหน้าที่ตามที่ระบุไว้เพื่อประโยชน์สาธารณะการประมวลผล
ข้อมูลส่วนบุคคลดังกล่าวนั้นจะอยู่ภายใต้ขอบเขตการประมวลผล
ข้อมูลส่วนบุคคลด้วยฐาน Public Tasks
- ตัวอย่าง
 - ◊ กรณีที่สำนักงานตำรวจแห่งชาติเก็บและดูแลองค์กรปิด^๑
จับการขับรถเร็วเกินกำหนดหรือฝ่าไฟแดง
 - ◊ การใช้อำนาจของสำนักงานตำรวจแห่งชาติในการดำเนินการอื่น
เพื่อการป้องกันประโยชน์สาธารณะหรือป้องกันเหตุที่อาจ
เกิดขึ้นภายใต้กรอบกฎหมายที่เกี่ยวข้องกำหนด ตั้งแต่การค้น
การจับ หรือการเปรียบเทียบปรับต่าง ๆ ที่อยู่ภายใต้ขอบสิทธิ
ของอำนาจตามกฎหมายที่เป็นภารกิจของสำนักงานตำรวจ
แห่งชาติ
- สำหรับการประมวลผลข้อมูลส่วนบุคคลด้วยฐาน Public Task นี้
เจ้าของข้อมูลส่วนบุคคลไม่สามารถปฏิเสธการประมวลผลข้อมูล
ส่วนบุคคลดังกล่าวได้ แต่การประมวลผลข้อมูลส่วนบุคคลดังกล่าว
ต้องอยู่ภายใต้ขอบเขตอำนาจที่ชอบด้วยกฎหมายของสำนักงานตำรวจ
แห่งชาติด้วย

- ในการประมวลผลข้อมูลส่วนบุคคลด้วย Public Task สำนักงานติดตามและรายงานแก่เจ้าหน้าที่ รวมไปถึงรักษาข้อมูลส่วนบุคคลดังกล่าวไว้ได้ตลอดระยะเวลาที่กฎหมายกำหนด หรือระยะเวลาที่อาจมีความจำเป็นเพื่อจุดประสงค์การปฏิบัติหน้าที่ตามกรอบกฎหมายที่เกี่ยวข้องดังกล่าว

๕.๓ ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุภาพของส่วนบุคคล (Vital Interest) (มาตรา ๒๔ (๒))

- ผู้ควบคุมข้อมูลส่วนบุคคลที่จะสามารถใช้ฐานตามกฎหมาย Vital Interest ได้ ต้องไม่มีทางเลือกอื่นในการระงับอันตรายเฉพาะหน้าต่อชีวิต ร่างกาย ของเจ้าของข้อมูลส่วนบุคคลจึงจำเป็นต้องใช้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลเพื่อป้องกันหรือระงับอันตรายต่อบุคคลนั้น
- ตัวอย่างที่สำนักงานติดตามและรายงานแก่เจ้าหน้าที่ใช้ฐาน Vital Interest ได้ เช่น กรณีเจ้าหน้าที่ติดตามพบรหินอุบัติเหตุมีผู้ได้รับบาดเจ็บสาหัสและหมดสติ เจ้าหน้าที่ติดตามสามารถใช้ข้อมูลบัตรประจำประชาชนของผู้ประสบเหตุดังกล่าว เพื่อดำเนินการค้นหาข้อมูลส่วนบุคคลของผู้ได้รับบาดเจ็บ เพื่อแจ้งข้อมูลไปยังโรงพยาบาลก่อนการส่งตัวไปรักษา ด้วยจุดประสงค์การระงับอันตรายป้องกันรักษาชีวิตของผู้ประสบเหตุดังกล่าวได้
- การประมวลผลข้อมูลภายใต้ฐานนี้ค่อนข้างจำกัด ต้องเป็นกรณีเฉพาะหน้าที่ไม่มีทางเลือกอื่น เป็นหลัก

๕.๔ ฐานการวิจัยหรือทำสถิติ (Research / Archives) (มาตรา ๒๔ (๑))

- การประมวลผลข้อมูลส่วนบุคคลด้วยฐานนี้ ต้องเป็นการจัดทำเอกสารประวัติศาสตร์ หมายเหตุ หรือการศึกษาวิจัยหรือสถิติ เพื่อประโยชน์สาธารณะ ซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลนั้น แล้วเท่านั้น
- ตัวอย่างเช่น การทำวิจัยโดย สำนักงานตำรวจแห่งชาติ หากเป็น การทำ Modeling เพื่อการป้องกันและปราบปรามเหตุหรือการ ป้องกัน Fraud Detection ซึ่งเป็นการดำเนินการเพื่อประโยชน์สาธารณะ ส่วนนี้ สามารถถือว่าใช้ฐานนี้ได้
- ข้อสังเกต หากการทำสถิติหรือวิจัยได้ดำเนินการ โดยข้อมูล ที่ไม่สามารถระบุตัวตนได้ ในลักษณะของข้อมูลนิรนาม หรือข้อมูล สถิติ ไม่ได้นำข้อมูลส่วนบุคคลเข้ามาเกี่ยวข้องในกระบวนการวิจัย กรณีนี้ ข้อมูลที่นำมาใช้ในการวิจัยอาจไม่ถือเป็น ข้อมูลส่วนบุคคล และไม่ต้องดำเนินการได้ภายใต้ PDPA ทั้งสิ้น

๕.๕ ฐานสัญญา (Contractual Performance) (มาตรา ๒๔ (๓))

- กรณีการย้างใช้ฐาน Contractual Performance ต้องมีการทดลอง ระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคล แม้จะไม่เป็นลายลักษณ์อักษร ในลักษณะที่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องมีหน้าที่ดำเนินการบางอย่างให้แก่ เจ้าของข้อมูลส่วนบุคคล และเพื่อการทำหน้าที่นั้นผู้ควบคุมข้อมูลส่วนบุคคลจึงมีความจำเป็น ต้องประมวลผลข้อมูลส่วนบุคคล

- ตัวอย่างเช่น
 - ◊ ในการให้บริการแก่ประชาชน หากอยู่ภายใต้วิสัยการคาดหมายได้ว่า เจ้าของข้อมูลส่วนบุคคลต้องการให้เจ้าหน้าที่สำรวจดำเนินการได้ให้ เช่น โทรกลับมาแจ้งความคืบหน้าเรื่องที่ร้องเรียนหรือขอใช้บริการ ทางเจ้าหน้าที่สามารถใช้ข้อมูลการติดต่อ เพื่อติดต่อกลับไปแจ้งตามที่คาดหมายดังกล่าวได้
 - ◊ การจ้างงานระหว่างสำนักงานสำรวจแห่งชาติ หรือการจ้างคู่ค้าต่างๆ สำนักงานสำรวจแห่งชาติ ย่อมมีหน้าที่ต้องชำระค่าตอบแทนให้แก่บุคคลดังกล่าว จึงมีความจำเป็นต้องใช้ข้อมูลบัญชีธนาคารเพื่อการชำระเงินให้แก่บุคคลนั้น ภายใต้ข้อตกลงที่เกี่ยวข้อง
- กรณี การประมวลผลข้อมูลส่วนบุคคลด้วยฐาน Contractual Performance นี้เจ้าของข้อมูลส่วนบุคคลไม่สามารถปฏิเสธการใช้ข้อมูลนั้นได้ หากยังต้องการใช้บริการหรือใช้สิทธิตามข้อตกลงนั้น
- ทั้งนี้ สำนักงานสำรวจแห่งชาติในฐานะผู้ควบคุมข้อมูล ส่วนบุคคล จะสามารถใช้ข้อมูลเพื่อประโยชน์ดังกล่าวได้เฉพาะตลอดระยะเวลาที่ยังจำเป็นสำหรับการปฏิบัติหน้าที่ตามข้อตกลงหรือสัญญานั้น เท่านั้น

๕.๖ ฐานความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) (มาตรา ๒๔ (๕))

- การประมวลผลข้อมูลส่วนบุคคลด้วยฐาน Legitimate Interest ต้องเป็นกรณีการประมวลผลข้อมูลส่วนบุคคลที่มีความจำเป็น เพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (คือ สำนักงานตำรวจแห่งชาติ หรือของเจ้าหน้าที่ตำรวจเอง) หรือ ของบุคคลอื่น แต่ในการประมวลผลข้อมูลส่วนบุคคลนั้นต้องไม่ กระทบ รบกวนสิทธิเจ้าของข้อมูลส่วนบุคคลมากเกินสมควร
- ตัวอย่าง
 - ◊ การติดกล้องวงจรปิดภายในพื้นที่สำนักงานหรือหน่วยงานใน สำนักงานตำรวจแห่งชาติ เพื่อประโยชน์ในการรักษาความ ปลอดภัยภายในพื้นที่
 - ◊ การบันทึกภาพและเสียงในการจับหรือการค้น ซึ่งไม่ใช่หน้าที่ โดยตรงตามกฎหมายที่บังคับให้สำนักงานตำรวจแห่งชาติต้อง ดำเนินการดังกล่าวแต่เป็นการดำเนินการเพื่อสร้างหลักฐานใน การต่อสู้คดีในภายหลัง
 - ◊ การถ่ายภาพการจัดกิจกรรมต่าง ๆ ของสำนักงานตำรวจ แห่งชาติ ซึ่งเป็นการถ่ายภาพในลักษณะของภาพบรรยายรวม และใช้ภาพดังกล่าวในการจัดทำสื่อประชาสัมพันธ์ หรือ รายงานของสำนักงานตำรวจแห่งชาติ ไม่ว่าจะเป็นเอกสาร รายงานภายใน หรือเผยแพร่สู่ภายนอก

- การใช้ Legitimate Interest ต้องประเมินความสมดุลระหว่างประโยชน์อันชอบด้วยกฎหมายซึ่งอาจรวมถึงประโยชน์ของบุคคลโดยรวม และความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลหนึ่งคน
- หมายเหตุ เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้หากรู้สึกว่า ถูกกระทบความเป็นส่วนตัวมากเกินสมควร

๕.๗ ฐานความยินยอม (Consent)

- การขอความยินยอมไม่ใช่ฐานอันชอบด้วยกฎหมายหลักสำหรับการประมวลผลข้อมูลส่วนบุคคล ดังนั้นหากเป็นการประมวลผลตามฐานที่กำหนดไว้ข้างต้นทั้ง ๖ ฐานแล้วไม่ต้องขอความยินยอมเลย
- การทำงานของเจ้าหน้าที่ต้องสามารถดำเนินการได้โดยใช้ฐานกฎหมาย ฐานการใช้งานจริงหรือฐานประโยชน์อันชอบด้วยกฎหมายอยู่แล้วโดยหลัก โดยจะมีกรณีต้องขอความยินยอมใน ๒ กรณี เท่านั้น
 - ◊ เป็นการประมวลผลข้อมูลส่วนบุคคลที่ไม่เข้าฐานกฎหมายอื่นแล้ว (มาตรา ๑๙) ยกตัวอย่างเช่น การขอความยินยอมในการใช้คุกกี้ (Cookies) ซึ่งเป็นพักร์ชั้นในการใช้อินเทอร์เน็ต บริวารเซอร์บางประเภทบนหน้าเว็บไซต์ หรือการขอความยินยอมในการถ่ายภาพ หรือสัมภาษณ์รายบุคคลเพื่อการจัดทำสื่อประชาสัมพันธ์ ซึ่งมีความเฉพาะเจาะจง

- ◊ เป็นการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว ยกเว้นกรณี การใช้ข้อมูลส่วนบุคคลอ่อนไหวนี้ได้รับการประมวลผล เพื่อการก่อตั้งสิทธิเรียกร้องตามกระบวนการทางกฎหมาย หรือเก็บเพื่อประโยชน์ส่วนรวมสาธารณะ ทั้งนี้ การประมวลผล ข้อมูลส่วนบุคคลอ่อนไหวหากเป็นการดำเนินการเพื่อประโยชน์ ในการรักษาความปลอดภัยของประชาชน หรือนิติวิทยาศาสตร์ จะได้รับการยกเว้นจากการปฏิบัติตาม PDPA จึงไม่มีหน้าที่ การขอความยินยอม
- การขอความยินยอม มีหลักการที่ PDPA กำหนด ดังนี้
 - ◊ ต้องแยกขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเป็น รายบุคคล แยกวัดถูประสงค์
 - ◊ เจ้าของข้อมูลมีสิทธิเลือกที่จะให้หรือไม่ให้ความยินยอม และต้องสามารถถอนความยินยอมได้เสมอ

๕.๔ การประเมินฐานการประมวลผลข้อมูลอันชอบด้วยกฎหมาย (Lawful Basis)

การพิจารณาการประมวลผลข้อมูลส่วนบุคคลโดยยุ่งยากให้ Lawful Basis ได้นั้น สำนักงานตำรวจแห่งชาติต้องแยกแต่ละกิจกรรมการประมวลผล เนื่องจาก กิจกรรมและวัตถุประสงค์การใช้ข้อมูลที่ต่างกันอาจนำไปสู่ฐานการประมวลผล ที่อ้างอิงได้ที่ต่างกัน เช่น

- การถ่ายภาพระหว่างการจับกุม เพื่อเป็นหลักฐานในการฟ้องร้อง สามารถดำเนินได้ด้วยฐานประโยชน์อันชอบด้วยกฎหมาย Legitimate Interest

- แต่หากมีการนำข้อมูลภาพถ่ายนั้นไปเผยแพร่ให้แก่สื่อมวลชน เช่น การแกลงข่าวการจับกุม ซึ่งเป็นกิจกรรมใหม่ ต้องประเมินความจำเป็นและวัตถุประสงค์แยกต่างหาก
 - ◊ กรณีนี้เป็นการส่งต่อเปิดเผยข้อมูลส่วนบุคคล ซึ่งอาจถือว่า เป็นข้อมูลส่วนบุคคลอ่อนไหว (เพราะเป็นลักษณะของประวัติอาชญากรรมเนื่องจากเป็นการดำเนินการของสำนักงานตำรวจแห่งชาติ) ซึ่งไม่สามารถอ้างฐานการใช้อำนาจรัฐ (Public Task) ได้เนื่องจากไม่ได้เป็นหน้าที่โดยตรงของเจ้าหน้าที่ตำรวจต้องเปิดเผยข้อมูลดังกล่าวแก่สื่อมวลชน
 - ◊ ในกรณีดังกล่าว จึงต้องเป็นกรณีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นกรณีที่ควรหลีกเลี่ยงการดำเนินการดังกล่าว

๕.๙ สรุปเอกสารที่สำนักงานตำรวจแห่งชาติต้องทำและแจ้ง ภายใต้ PDPA

- เอกสารที่ สำนักงานตำรวจแห่งชาติต้องจัดทำและประกาศ ได้แก่ “ประกาศเรื่อง แนวโน้มภายในการคุ้มครองข้อมูลส่วนบุคคล” (Privacy Statement / Privacy Notice) ซึ่งแจ้งรวมการประมวลผลข้อมูลส่วนบุคคลทั้งหมดในทุกวัตถุประสงค์ ทุกฐานการประมวลผล ข้อมูลส่วนบุคคลไว้ในเอกสารฉบับเดียวกัน
 - ◊ จัดทำและแจ้งประกาศดังกล่าวเป็นเอกสารแจ้งฝ่ายเดียว ประกาศในที่ที่สามารถศึกษาได้เป็นการทั่วไป เช่น ผ่านทางเว็บไซต์ของสำนักงานตำรวจนแห่งชาติ หรือติดประกาศไว้ที่

บอร์ดประชาสัมพันธ์ของแต่ละหน่วยงาน หรือผ่านช่องทาง การติดต่อสื่อสารอื่นที่สำนักงานตำรวจแห่งชาติอาจมีกับ เจ้าของข้อมูลแต่ละกลุ่ม

- กรณีจำเป็นต้องขอความยินยอม สำนักงานตำรวจแห่งชาติต้อง ดำเนินการจัดทำแบบฟอร์มการขอความยินยอม และเก็บรวบรวม การให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลแต่ละท่าน

๖. การรักษาความมั่นคงปลอดภัยที่เพียงพอเหมาะสม ภายใต้ PDPA

- PDPA ไม่ได้กำหนดระดับความปลอดภัยไว้ชัดเจน แต่ละองค์กร ต้องประเมินความเสี่ยงของข้อมูลส่วนบุคคลที่ตนเก็บ โดยต้องจัดให้มีมาตรการที่เหมาะสมตามความเสี่ยงที่ประเมินไว้ดังกล่าว
- มาตรการรักษาความมั่นคงปลอดภัย ตามมาตรฐานขั้นต่ำที่สำนักงาน ตำรวจแห่งชาติต้องดำเนินการ โดยอ้างอิงจากประกาศคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล ได้แก่
 - การสร้างความเข้าใจและตระหนักรู้ (Awareness) ภายในองค์กร ให้บุคลากรที่เกี่ยวข้องทั้งหมดเข้าใจถึงความสำคัญของ PDPA และ การใช้ข้อมูลส่วนบุคคลที่ถูกต้อง
 - การจำกัดสิทธิในการเข้าถึงข้อมูล (Access Control) โดยต้องมี การประเมินการเปิดเผยส่งต่อ ให้สิทธิเข้าถึงข้อมูลให้เหมาะสมกับ ความจำเป็น (Need-to-Know Basis) และต้องมีการบริหารจัดการ สิทธิ์ดังกล่าวให้เป็นปัจจุบันตลอด
 - การเก็บบันทึกการเข้าถึงหรือใช้ข้อมูลส่วนบุคคล (Logs) เพื่อ การตรวจสอบย้อนหลังการประมวลผลข้อมูลส่วนบุคคลให้ถูกต้อง

หมายเหตุ ชี้งหากเป็นการประมวลผลข้อมูลด้วยระบบ
อิเล็กทรอนิกส์ การบันทึกการเข้าใช้งานด้วยระบบ (System Logs)
ถือว่าหมายเหตุและเพียงพอ

- การรักษาความปลอดภัยเพิ่มเติมตามความเสี่ยง (IT Security) เช่น การติดตั้ง Anti-virus, Firewall, การเข้ารหัสข้อมูล (Encryption) การติดตั้งระบบเพื่อป้องกันการเจาะระบบ
- จากรัฐติจากต่างประเทศ ส่วนมากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ที่เกิดขึ้น จะเกิดจากการดำเนินการโดยไม่ระมัดระวังของบุคลากรภายใน (Internal Breach) มากกว่าเกิดจากการโจมตีหรือขโมยข้อมูลจากภายนอก (External Breach)
 - การติดต่อสื่อสารผ่านทาง Application LINE ระหว่างบุคลากร ไม่ใช่สิ่งต้องห้าม ภายใต้ PDPA แต่ต้องมีการควบคุมมากขึ้น ดังนี้
 - ◊ ควรตรวจสอบและจำกัดการส่งข้อมูล โดยหลีกเลี่ยงการส่งต่อ ข้อมูลส่วนบุคคลอ่อนไหว (เช่น ข้อมูลหมายเลขอาญาต่าง ๆ หรือ ข้อมูลแจ้งความผิดอาญาของผู้ต้องหา) หรือข้อมูลที่มีความ สุ่มเสี่ยงที่หากหลุดรั่วไปจะสร้างความเสียหาย (เช่น รูปภาพ สำเนาประชาชน) ผ่านทาง LINE
 - ◊ หากจำเป็นต้องมีการส่งข้อมูลส่วนบุคคลที่อ่อนไหวหรือ สุ่มเสี่ยง เพื่อความสะดวก ควรส่งในวง LINE Group ที่จำกัด หรือการส่งสื่อสารส่วนบุคคล (Private Chat) แทนเพื่อให้ สามารถตรวจสอบย้อนหลังได้ว่า มีการส่งต่อเปิดเผยข้อมูลไป ให้แก่บุคคลใดบ้าง

- ◊ กรณีมีการตั้ง LINE Group ต้องมีการตรวจสอบยืนยันตัวตน และความเกี่ยวข้องของบุคคลที่เข้าร่วมในกลุ่มดังกล่าว โดยควร เลี่ยงการส่งข้อมูลส่วนบุคคลที่อ่อนไหวหรือมีความเสี่ยงทั้งหมด ผ่าน Line Group และควรเป็น Admin ของ LINE Group ทำหน้าที่ในการตรวจสอบยืนยันสิทธิและความเกี่ยวข้องของผู้ที่อยู่ใน LINE Group อญี่ปุ่นโดยเฉพาะผู้ที่พ้นจากการปฏิบัติหน้าที่ รับผิดชอบในส่วนที่ดำเนินการเกี่ยวกับคดี หรือออกจากงานไปแล้ว
- ◊ ควรมีการกำหนดกฎหมายสำหรับการใช้ LINE และการสร้าง ความตระหนักรู้กันภายในสำนักงานต่อว่า “ไม่ควร นำข้อมูลที่ได้รับจากการส่งต่อไปทำการอื่นที่นอกเหนือจาก วัตถุประสงค์ในการดำเนินการปฏิบัติหน้าที่ที่ตนเองมีหน้าที่ เท่านั้น”
 - ประเด็นที่ต้องใช้ความระมัดระวังเพิ่มเติมคือ การดำเนินการภายใต้ สำนักงานต่อว่า “ไม่ควร นำข้อมูลส่วนบุคคลอ่อนไหวมาใช้เดิม (Recycle) ควรทำลาย ด้วยวิธีการที่เหมาะสม”

๗. กรณีมีการส่งต่อเปิดเผยข้อมูลส่วนบุคคลไปออกองค์กร โดยเฉพาะส่งต่อ ให้แก่หน่วยงานที่ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผล ข้อมูลส่วนบุคคล

- ต้องตรวจสอบความจำเป็นในการส่งต่อเปิดเผยข้อมูลส่วนบุคคลไปยัง หน่วยงานภายนอกดังกล่าว โดยต้องประเมินจากฐานความจำเป็นอันชอบ ด้วยกฎหมาย เนื่องจากมาตรา ๒๗ กำหนดว่า ห้ามไม่ให้มีการเปิดเผย

เงื่อนแต่เข้ากรณีตามมาตรา ๒๔ หรือได้รับความยินยอมจากเจ้าของข้อมูล
ส่วนบุคคลก่อน

- หากเป็นการส่งต่อให้แก่ผู้ประมวลผลข้อมูลส่วนบุคคล สำนักงานตรวจ
แห่งชาติในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำ “ข้อตกลงการ
ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)” กับผู้รับ
ข้อมูลเพื่อกำหนดหน้าที่และความรับผิดชอบของผู้ได้รับข้อมูลในการ
ประมวลผลข้อมูลส่วนบุคคลตามคำสั่ง และกำหนดหน้าที่การรักษาความ
มั่นคงปลอดภัยให้ชัดเจน
- หากเป็นการส่งต่อไปให้แก่หน่วยงานอื่น แม้จะมีฐานะเป็นผู้ควบคุมข้อมูล
ส่วนบุคคลเช่นกัน การจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลจะช่วย
สร้างความชัดเจน เกี่ยวกับสิทธิและหน้าที่ได้มากขึ้น จึงควรต้องมีการจัดทำเสมอ
ไม่ว่าจะเป็นการจัดทำแยกเป็นสัญญาแยกหรือกำหนดเป็นข้อสัญญา
หนึ่งในสัญญาความร่วมมือระหว่างองค์กร

๔. สิทธิเจ้าของข้อมูลส่วนบุคคลภายใต้ PDPA

- สำนักงานตำรวจแห่งชาติ มีหน้าที่หลักอีกประการหนึ่งภายใต้ PDPA คือ “การเเครฟสิทธิเจ้าของข้อมูลส่วนบุคคล”
 - สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน (มาตรา ๓๐)
 - สำนักงานตำรวจแห่งชาติต้องปฏิบัติตามคำขอดังกล่าวเสมอ เว้นแต่ เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล หรือการเข้าถึงข้อมูลนั้น จะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพ ของบุคคลอื่น
 - สิทธิถอนความยินยอม (มาตรา ๑๙)
 - ถ้าเป็นการประมวลผลข้อมูลส่วนบุคคลโดยอ้างฐานความยินยอม สำนักงานตำรวจแห่งชาติต้องให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคล ถอนความยินยอมได้โดยง่าย เช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดตามกฎหมาย
 - สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลที่เก็บใน รูปแบบที่สามารถอ่าน หรือใช้งานได้โดย ทั่วไปด้วยเครื่องมือหรืออุปกรณ์ ที่รองรับการทำงานได้โดยอัตโนมัติไปให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลอื่น ได้ด้วยวิธีการอัตโนมัติ (Data Portability) (มาตรา ๓๑)
 - สำนักงานตำรวจแห่งชาติอาจปฏิเสธการใช้สิทธินี้ได้ หากเป็นการ ประมวลผลข้อมูลส่วนบุคคลตามหน้าที่ตามกฎหมาย หรือการใช้สิทธินี้ จะละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น

- สำนักงานติดตามตรวจสอบการดำเนินการดังกล่าวได้หากมีข้อจำกัดทางด้านเทคนิค และความเป็นไปได้ในการเชื่อมโยงและส่งต่อข้อมูลด้วยวิธีอัตโนมัติดังกล่าว
- สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล ในกรณีเป็นการประมวลผลข้อมูลส่วนบุคคลโดยอ้างประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest) และเจ้าของข้อมูลรู้สึกว่ากระทบสิทธิของตนมากเกินสมควร (มาตรา ๓๒)
 - สำนักงานติดตามจะได้แจ้งว่า สิทธิประโยชน์อันชอบด้วยกฎหมายนั้นมีความสำคัญกว่า สิทธิของเจ้าของข้อมูลส่วนบุคคลรายดังกล่าวเพียงคนเดียว หรือสำนักงานติดตามจะได้จัดให้มีกระบวนการในการป้องกันการกระทบสิทธิเจ้าของข้อมูลส่วนบุคคลแล้ว
 - หากการคัดค้านไม่สำเร็จ สำนักงานติดตามจะต้องหยุดการประมวลผลข้อมูลส่วนบุคคล
- สิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคล (มาตรา ๓๓) ในกรณีการประมวลผลข้อมูลส่วนบุคคลนั้นหมดความจำเป็น หรือกรณีเกิดการประมวลผลข้อมูลส่วนบุคคลที่ไม่ชอบด้วยกฎหมาย
 - สำนักงานติดตามจะต้องลบ ทำลาย หรือทำให้ระบุตัวตนไม่ได้ เมื่อหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลนั้นจริง
 - หากสำนักงานติดตามจะต้องเปิดเผยข้อมูลที่ถูกขอให้ลบทำลายไปต่อสาธารณะแล้ว ต้องดำเนินการทางเทคโนโลยีและค่าใช้จ่ายในการแจ้งบุคคลอื่นให้ทราบด้วยเช่นกัน

- สิทธิขอให้ระงับการประมวลผลข้อมูลส่วนบุคคล (มาตรา ๓๔) โดยให้
 ระงับการใช้ชั่วคราว
 - สำนักงานตำรวจแห่งชาติต้องดำเนินการให้ตามคำขอ โดยถือเป็น
 สิทธิ์ต่อเนื่องจากสิทธิ มาตรา ๓๒ หรือมาตรา ๓๓
- สิทธิในการขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องเป็นปัจจุบัน สมบูรณ์ และ
 ไม่ก่อให้เกิดความเข้าใจผิด (มาตรา ๓๕)
 - สำนักงานตำรวจแห่งชาติต้องดำเนินการให้ตามคำขอของเจ้าของ
 ข้อมูลส่วนบุคคล
- สิทธิร้องเรียนต่อหน่วยงานที่เกี่ยวข้อง เพื่อเรียกร้องให้ผู้ควบคุมข้อมูล
 ส่วนบุคคลที่ไม่ดำเนินการให้ถูกต้องต้องรับโทษตาม PDPA

๙. โทษของการไม่ปฏิบัติตาม PDPA มีอะไรบ้าง

ฟ้องคดีแพ่งต่อศาล	ฟ้องคดีอาญาต่อศาล	ร้องเรียนไปที่คณะกรรมการ
<ul style="list-style-type: none"> - หน้าที่ในการพิสูจน์ว่า ตนเอง ไม่ผิดเป็นของผู้ควบคุมหรือผู้ประมวลผลข้อมูล - ศาลสามารถเพิ่มค่าเสียหาย เชิงลงโทษได้ 2 เท่าเพิ่มเติม ขึ้นจากค่าเสียหายตามจริงได้ - ผู้เสียหายที่ได้รับผลกระทบ เช่นเดียวกับสามารถร่วมกัน ดำเนินคดีแบบกลุ่ม (Class Action) ได้ 	<ul style="list-style-type: none"> - เป็นกรณีที่ผู้ควบคุมข้อมูล ส่วนบุคคลใจหรือประมาท เลินเล่ออย่างร้ายแรงเบ็ดเตล็ด ข้อมูลส่วนบุคคลอ่อนไหว และทำให้เกิดความเสียหาย หรือ - เป็นกรณีที่ผู้ล่วงรู้ข้อมูล ส่วนบุคคลจากการปฏิบัติ หน้าที่และเบิดเผยข้อมูล ส่วนบุคคลนั้นออกไป หากนิติบุคคลกระทำ ความผิด และการกระทำ ผิดนั้นเกิดจากการสั่งการ หรือการกระทำของ กรรมการหรือผู้จัดการ PDPA กำหนดให้กรรมการ หรือผู้จัดการผู้นั้นต้องรับ โทษตามที่บัญญัติไว้ด้วย 	<ul style="list-style-type: none"> - ปรับเงินเข้ารัฐบาล กรณีผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล ไม่ปฏิบัติตาม พ.ร.บ. แม้จะไม่ได้เกิดความเสียหาย - มีโทษปรับสูงสุด จำนวนหนึ่งล้านบาท หรือสามล้านบาท หรือห้าล้านบาท แล้วแต่กรณี

Part II: FAQ for PDPA Application

คำถามที่ ๑. การค้นตัวบุคคล

๑.๑ ส่วนที่เกี่ยวข้องกับ PDPA

- PDPA ใช้สำหรับการประมวลผลข้อมูลส่วนบุคคลเท่านั้น ไม่ใช่สิทธิหนึ่อตัวบุคคลโดยตรง
 - ◊ สิทธิในการขัดขืนหรือไม่ให้ตรวจสอบในส่วนที่ไม่ได้เกี่ยวข้องกับการใช้ “ข้อมูลส่วนบุคคล” ไม่อุ่ยภายในได้ PDPA ต้องปฏิบัติตามกฎหมายและหลักการของกฎหมายอื่น
 - ◊ การตรวจค้นอาคารหรือสถานที่ ไม่อุ่ยภายในได้บังคับ PDPA
- PDPA เกี่ยวข้องกับการเก็บและใช้ข้อมูลของบุคคลที่ถูกเรียกค้นได้แก่
 - ◊ การขอตรวจสอบข้อมูลส่วนบุคคลผู้ถูกค้น เช่น บัตรประจำตัวประชาชนของบุคคลนั้น
 - ◊ การบันทึกภาพและเสียงของบุคคลผู้ถูกค้น ระหว่างการค้นตัวบุคคล

๑.๒ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

- เนื่องจากในระหว่างการค้นด้วยบุคคล อาจยังไม่ถึงขั้นการประมวลผลข้อมูลส่วนบุคคล เพื่อการรักษาความปลอดภัยของประชาชน (ตามมาตรา ๔) ได้โดยตรง เนื่องจากเป็นการดำเนินยุทธวิธีในลักษณะ “ป้องกัน” มากกว่า สำนักงานติดตามฯจึงยังมีหน้าที่ต้องปฏิบัติตาม PDPA
- ฐานกฎหมายที่สามารถอ้างอิงสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคล โดยเฉพาะการเรียกเก็บหลักฐานของผู้ถูกเรียกค้น โดยเฉพาะบัตรประจำตัวประชาชน ถือว่า เป็นการปฏิบัติหน้าที่ในฐานะองค์กรรัฐ (Public Task) ได้โดยถือว่า การตรวจค้นและตรวจสอบเอกสารแสดงตนนั้น เป็นกระบวนการทำหน้าที่ตามกฎหมายที่เจ้าหน้าที่ติดตามฯมีสิทธิอำนาจในการดำเนินการได้ แต่ก็ต้องประเมินตามหลักการความจำเป็นและความชอบธรรม
- ฐานกฎหมายที่สามารถอ้างอิงสำหรับการบันทึกภาพและเสียง สำนักงานติดตามฯสามารถอ้างการดำเนินการเพื่อประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest) โดยถือเป็นประโยชน์ อันชอบด้วยกฎหมายของเจ้าหน้าที่ ติดตามฯ ในกรณีการติดตามฯ ใช้ข้อมูลดังกล่าวเพื่อประกอบ เป็นพยานหลักฐาน

๑.๓ สิ่งที่ต้องดำเนินการ

- ปฏิบัติตามยุทธวิธีติดตามฯเป็นพื้นฐาน

- ◊ แสดงตนเป็นเจ้าหน้าที่ตัวรัว เพื่อยืนยันการใช้อำนาจของหน่วยงาน
 - ◊ แจ้งเหตุและวัตถุประสงค์การค้น โดยต้องแจ้งข้อมูลว่าทางเจ้าพนักงานตัวรัวจะเก็บข้อมูลส่วนบุคคลใดบ้าง (เช่น ข้อมูลเอกสารแสดงตน ภาพถ่ายหรือเสียง) และวัตถุประสงค์ในการเก็บประมวลผล (เช่น ใช้เพื่อเป็นหลักฐานในการปฏิบัติหน้าที่ และการดำเนินกระบวนการพิจารณาคดีในอนาคต)
- ข้อมูลการบันทึกการค้นต้องถูกบันทึก และใช้เพื่อประโยชน์ในการทำหน้าที่ของเจ้าหน้าที่ตัวรัวเท่านั้น ไม่นำไปใช้ส่งต่อเปิดเผยให้แก่บุคคลภายนอก เว้นเฉพาะกรณีการเปิดเผยในกระบวนการพิจารณาคดีเท่านั้น
 - ต้องเก็บรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทั้งหมดที่เก็บรวบรวมมา โดยการจำกัดสิทธิผู้เข้าถึง และการจัดทำบันทึกการเบิกใช้งานข้อมูลส่วนบุคคลที่ดำเนินการทั้งหมด
 - ต้องมีการทำหนังระยะเวลาที่เหมาะสมในการลบหรือทำลายข้อมูลส่วนบุคคล กรณีไม่จำเป็น โดยเฉพาะหากในท้ายที่สุด ไม่มีเหตุเพิ่มเติมในการค้นหรือดำเนินการในกระบวนการพิจารณาคดีได้ต่อไป

คำถามที่ ๒. การจับกุมผู้ถูกจับ

๒.๑ ส่วนที่เกี่ยวข้องกับ PDPA

- PDPA ใช้สำหรับการประมวลผลข้อมูลส่วนบุคคล ไม่ใช่สิทธิเห็นอัตัวบุคคลโดยตรง
 - ◊ กระบวนการยุทธวิธี เช่น การใช้อาวุธหรือท่าทางในการจับกุม ไม่ได้อยู่ภายใต้ PDPA
- PDPA เกี่ยวข้องกับการใช้ข้อมูลของบุคคลที่ถูกจับกุม ได้แก่
 - ◊ การขอตรวจสอบข้อมูลส่วนบุคคลผู้ถูกจับ เช่น บัตรประจำตัวประชาชนของบุคคลนั้น
 - ◊ การบันทึกภาพและเสียงของผู้ถูกจับ ระหว่างการค้นตัวบุคคล
 - ◊ การใช้ข้อมูลเพื่อการตามจับ ทั้งจากข้อมูลที่เก็บโดยเจ้าหน้าที่ ตำรวจนายโดยตรงและที่ขอความร่วมมือจากหน่วยงานหรือบุคคลอื่น เช่น การตรวจสอบเลขทะเบียนรถยนต์ และเส้นทางหลวงหนึ่งตามภาพกล้องวงจรปิด

๒.๒ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

- การดำเนินกระบวนการประมวลผลข้อมูลส่วนบุคคลของผู้ถูกจับ อาจถือว่า อยู่ภายใต้เงื่อนไขการประมวลผลข้อมูลส่วนบุคคล ในการดำเนินกระบวนการยุติธรรมทางอาญา ซึ่งได้รับการยกเว้นจาก

หน้าที่ในการแจ้งการประมวลผลข้อมูลส่วนบุคคล แต่ย่างไรก็ตาม ยังต้องรอการตีความที่ชัดเจนจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- การประมวลผลข้อมูลส่วนบุคคลเพื่อขอตรวจสอบข้อมูลและการตามข้อมูลการจับ สามารถอ้างฐานการปฏิบัติหน้าที่ในฐานะองค์กรรัฐ (Public Task) ได้ และกรณีการถ่ายบันทึกภาพและเสียง สามารถอ้างฐานการดำเนินการเพื่อประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest) กล่าวคือการเก็บเพื่อวัตถุประสงค์การป้องกันในกรณีการโட္เต้ยังในชั้นการดำเนินในกระบวนการดำเนินคดี หรือใช้ข้อมูลดังกล่าวเพื่อประกอบเป็นพยานหลักฐานได้

๒.๓ สิ่งที่ต้องดำเนินการ

- **ปฏิบัติตามยุทธวิธีที่มีการดำเนินการ**
 - ◊ แสดงตนว่าเป็นเจ้าหน้าที่ที่มีอำนาจ เพื่อยืนยันการใช้อำนาจของหน่วยงาน
 - ◊ แจ้งการประมวลผลข้อมูลส่วนบุคคลว่า ทางเจ้าหน้าที่ที่มีอำนาจจะเก็บข้อมูลส่วนบุคคลใดบ้างของบุคคลดังกล่าว (เช่น ข้อมูลเอกสารแสดงตน ภาพถ่ายหรือเสียง) และวัตถุประสงค์ในการเก็บประมวลผล (เช่น เพื่อเป็นหลักฐานในการปฏิบัติหน้าที่ และการดำเนินกระบวนการพิจารณาคดีในอนาคต)
- ข้อมูลการบันทึกการจับต้องถูกบันทึก และใช้เพื่อประโยชน์ในการทำหน้าที่ของเจ้าหน้าที่ที่มีอำนาจเท่านั้น ไม่นำไปใช้ส่งต่อเปิดเผยให้แก่

บุคคลภายนอก เว็บเฉพาะกรณีการเปิดเผยในกระบวนการพิจารณา คดีเท่านั้น

- ◊ การเปิดเผยข้อมูลดังกล่าวต่อสื่อมวลชน หรือบุคคลที่ไม่ใช่การประมวลผลข้อมูลส่วนบุคคลที่มีฐานอันชอบด้วยกฎหมายรับ อาจต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และการเปิดเผยดังกล่าวอาจนำไปสู่ความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล หรือการสร้างความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ซึ่งถือเป็นความเสี่ยงของเจ้าหน้าที่ตำรวจในการดำเนินการดังกล่าว จึงต้องใช้ความระมัดระวังอย่างมากในการดำเนินการนั้น และอาจควรหลีกเลี่ยง
- การเก็บรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทั้งหมดที่เก็บรวบรวมมาแล้ว ต้องมีการจำกัดสิทธิผู้เข้าถึง และการจัดทำ Log ในส่วนของการดำเนินการเกี่ยวนี้อย่างกับข้อมูลส่วนบุคคลนั้น
- ต้องมีการทำหนังสือระยะเวลาที่เหมาะสมในการลบหรือทำลายข้อมูลส่วนบุคคล กรณีไม่จำเป็น โดยเฉพาะหากในท้ายที่สุดไม่มีเหตุเพิ่มเติมในการจับ หรือการดำเนินในกระบวนการการดำเนินคดีได้ต่อบุคคลดังกล่าว

๒.๔ กระบวนการขอความร่วมมือขอข้อมูลจากบุคคลภายนอก เช่น การขอข้อมูลกล้องวงจรปิด เป็นต้น

- กรณีบุคคลภายนอกติดตั้งกล้องวงจรปิด บุคคลนั้นจะมีฐานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ในส่วนของการเก็บภาพกล้องวงจรปิดทั้งหมด เนื่องจากเป็นผู้ตัดสินใจในการเก็บรวบรวม และกรณีการที่

บุคคลนั้นจะส่งต่อข้อมูลให้แก่เจ้าหน้าที่ตำรวจ เจ้าของกล้องวงจรปิดต้องประเมินความจำเป็นในการส่งต่อเปิดเผยข้อมูลให้แก่เจ้าหน้าที่ตำรวจ

- การขอข้อมูลล้อง (ที่จะมีภาพถ่ายใบหน้าของบุคคล) ดังกล่าวเจ้าหน้าที่ตำรวจไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในภาพนั้น ด้วยถือเป็นการประมวลผลในฐานะองค์กรรัฐ จึงเป็นฐานกฎหมาย Public Task แต่เพื่อให้ได้รับความร่วมมือเจ้าหน้าที่ตรวจควรอธิบาย เพื่อขอความร่วมมือจากบุคคลภายนอก ดังนี้
 - ◊ กรณีมีการออกหมายอาญาหรือเป็นคำสั่งของเจ้าพนักงานตามกฎหมายโดยตรงแล้ว การที่บุคคลภายนอกนั้นจะส่งข้อมูลให้แก่เจ้าหน้าที่ตำรวจ สามารถอธิบายได้ว่า การส่งต่อข้อมูลส่วนบุคคลจากเจ้าของกล้องวงจรปิด ให้แก่เจ้าหน้าที่ตรวจ สามารถทำได้ตามกรอบฐานกฎหมาย (Legal Obligations)
 - ◊ หากยังไม่มีหมายอาญา แต่เป็นการขอความร่วมมือ เจ้าหน้าที่ตรวจสามารถอธิบายแก่บุคคลภายนอกได้ว่า กรณีที่บุคคลนั้นจะเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าหน้าที่ตำรวจ อาจถือเป็นการดำเนินการเพื่อประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest) ของเจ้าหน้าที่ตรวจซึ่งดำเนินการเพื่อประโยชน์สาธารณะ และของผู้อื่น ซึ่งสามารถดำเนินการได้เช่นกัน

- หากได้รับความร่วมมือจากเจ้าของกล้องวงจรปิด เจ้าหน้าที่ตำรวจ ต้องให้ข้อมูลและให้ความร่วมมือต่อบุคคลผู้ควบคุมข้อมูล ในการบันทึกรายละเอียดข้อมูลส่วนบุคคลของเจ้าหน้าที่ตำรวจ (เช่น ชื่อ นามสกุล ตำแหน่ง หรือบัตรเจ้าหน้าที่ตำรวจน) โดยถือเป็นกรณีที่เจ้าของกล้องวงจรปิดเองก็จะเรียกร้องอ้างสิทธิในการเก็บข้อมูลส่วนบุคคลดังกล่าว ด้วยฐานประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest) ของบุคคลดังกล่าว เช่น กัน เพื่อป้องกันการได้แย้งหรือข้อพิพาทในอนาคต

คำถามที่ ๓. การแสดงข่าวจับกุม

๓.๑ ส่วนที่เกี่ยวข้องกับ PDPA คือ การเปิดเผยภาพใบหน้า ชื่อ นามสกุล และรายละเอียดการจับกุม

๓.๒ การแสดงข่าวจับกุม อาจแบ่งออกเป็น ๓ ลักษณะ ได้แก่
(๑) การแสดงความคืบหน้าของคดี (๒) การแสดง การจับกุม และ
(๓) การแสดงเตือนแผนอาชญากรรมของคนร้ายต่างๆ ซึ่งสามารถจะ
ต้องใช้ความระมัดระวัง

๓.๓ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

- การดำเนินกระบวนการแสดงข่าวนี้ หากเป็นกรณีเกี่ยวข้องกับความมั่นคงของรัฐ หรือเพื่อการรักษาความปลอดภัยของประชาชน อาจถือว่าอยู่ภายใต้เงื่อนไขการประมวลผลข้อมูลส่วนบุคคล ซึ่งได้รับการยกเว้นจากหน้าที่ในการแจ้งการประมวลผลข้อมูลส่วนบุคคล

ตาม มาตรา ๔ แต่อย่างไรก็ตามยังต้องรอการตีความที่ขัดเจนจาก
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- การแกลงข่าว หากเป็นการแกลงข่าวเพื่อประโยชน์สาธารณะ
สามารถอ้างอิงฐานประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interest) ได้ โดยเฉพาะเพื่อประโยชน์ของสังคมโดยรวม เพื่อให้
ทราบความคืบหน้าของคดี หรือได้รับการแจ้งเตือนข้อมูล
อาชญากรรมต่าง ๆ เพื่อให้บุคคลทั่วไปจะได้ระมัดระวังตัว แต่ใน
การแกลงข่าวดังกล่าว สำนักงานต้องตรวจสอบแห่งชาติควรต้องประเมิน
หลักการความจำเป็นและความชอบธรรมในการเปิดเผยข้อมูล
โดยเฉพาะต้องจำกัดการเปิดเผยข้อมูลส่วนบุคคลเฉพาะเท่าที่
จำเป็นเท่านั้น

๓.๔ หลักการสำคัญที่ต้องพิจารณา คือ

- สำนักงานต้องตรวจสอบแห่งชาติต้องประเมินความจำเป็นในการเปิดเผย
ข้อมูลในการแกลงข่าวแต่ละครั้ง โดยเฉพาะต้องประเมินเทียบความ
เหมาะสมสมในเรื่องประโยชน์ส่วนรวม เปรียบเทียบกับสิทธิความเป็น
ส่วนตัวของผู้ถูกจับกุม
- สำนักงานต้องตรวจสอบแห่งชาติควรพิจารณาความจำเป็นอย่างละเอียด
ด้วยความระมัดระวังเพิ่มเติม กรณีผู้ต้องหาเป็นผู้เยาว์ เนื่องจาก
ผู้เยาว์เป็นผู้ประสบภัยและอาจได้รับความเสียหายอย่างสูงในการถูก
เปิดเผยข้อมูลส่วนบุคคลต่อสื่อสาธารณะ
- สำนักงานต้องตรวจสอบแห่งชาติควรพิจารณาถึงระดับความผิดของผู้ที่จะ
ดำเนินการแกลงข่าวว่า อยู่ในสถานะเป็นผู้ถูกกล่าวหา ผู้ต้องหา

หรือผู้ต้องรับผิด เนื่องจากการเปิดเผยข้อมูลส่วนบุคคลที่ถือว่า เป็นข้อมูลส่วนบุคคลอ่อนไหวดังกล่าวในระยะเวลาที่ไม่เหมาะสม อาจนำไปสู่ผลเสียมากกว่าผลดี และจะมีผลต่อเนื่องเป็นการ ดำเนินการผิดหลักการข้อสันนิษฐานตามกฎหมายอาญาว่า “บริสุทธิ์จนกว่าจะพิสูจน์ตามกฎหมายได้ว่ามีความผิด” ซึ่งภายใต้ PDPA อาจนำไปสู่ความเสี่ยงด้านโทษอาญา ทั้งในแง่ขององค์กร สำนักงานตำรวจนครบาล และผู้บังคับบัญชาสูงสุดของสำนักงาน ตำรวจแห่งชาติ

๓.๕ สิ่งที่ต้องดำเนินการ

- รวมการประมวลผลข้อมูลส่วนบุคคลเพื่อการแต่งช่าวไว้ใน “ประกาศเรื่อง แนวโน้มโดยainenการคุ้มครองข้อมูลส่วนบุคคล” (Privacy Statement / Privacy Notice) ซึ่งควรต้องมีการประกาศให้ทราบเป็นการทั่วไป พร้อมกับการประกาศสิทธิ์ตามกฎหมายของ ผู้ถูกกล่าวหา ผู้ต้องหา หรือผู้ต้องรับผิด
- ภายหลังผ่านกระบวนการในการประเมินความจำเป็นแล้ว หากไม่ จำเป็นหรือมีความสูงเสี่ยงในการเปิดเผยข้อมูลส่วนบุคคลของ บุคคลใดเป็นการสาหารณะ ต้องปิดบังตัวตนของผู้ต้องหาดังกล่าวไว้ ด้วยการปกปิดใบหน้า หรือการใช้นามสมมติ

๓.๖ กรณีในส่วนข้อมูลของผู้เสียหาย ต้องปิดบังข้อมูลอันเป็นข้อมูลส่วนบุคคลของผู้เสียหายไว้ตลอดเวลา และจะเปิดเผยได้เฉพาะแต่ในกรณี ดังนี้

- ผู้เสียหายแสดงเจตนาโดยชัดแจ้งที่จะให้มีการเปิดเผยข้อมูลส่วนบุคคลของตน หรือ
- เป็นการเปิดเผยข้อมูลของผู้เสียหายในกระบวนการดำเนินคดีซึ่งเป็นส่วนที่ได้รับการยกเว้นจากการดำเนิน การตามมาตรา ๔ ของ PDPA

คำถามที่ ๔. การจัดทำทะเบียน

๔.๑ ส่วนที่เกี่ยวข้องกับ PDPA

- หากเป็นการทำทะเบียนสถิติแบบไม่ระบุตัวตนของเจ้าของข้อมูล ข้อมูลในทะเบียนดังกล่าวไม่เป็นข้อมูลส่วนบุคคล จึงไม่อยู่ภายใต้เงื่อนไขบังคับของ PDPA
- หากจัดทำเป็นทะเบียนที่ระบุชื่อ และข้อมูลส่วนบุคคลของบุคคลโดยเฉพาะ เช่น การจัดทำรายชื่อบุคคลต้องห้าม หรือบุคคล被列入 (Blacklisted / Stop-Listed) ถือว่า เป็นการประมวลผล ข้อมูลส่วนบุคคลและต้องอยู่ภายใต้บังคับการปฏิบัติหน้าที่ภายใต้ PDPA

- ข้อมูลส่วนบุคคลที่รวมอยู่ในทะเบียนดังกล่าว เนื่องจากเป็นสถิติทางการของสำนักงานตัวรวจแห่งชาติ อาจตีความได้ว่า เป็นข้อมูลส่วนบุคคลอ่อนไหว ซึ่งต้องใช้ความระมัดระวังอย่างมากในกระบวนการประมวลผล โดยเฉพาะ (๑) การรักษาความมั่นคงปลอดภัย และ (๒) การประเมินความจำเป็นในการส่งต่อเปิดเผยออกไปให้แก่บุคคลภายนอก

๔.๒ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

- การจัดทำรายชื่อบุคคลต้องห้ามหรือต้องเฝ้าระวัง (Blacklisted / Stop-Listed) อาจถือเป็นการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับหน้าที่ในการรักษาความมั่นคงของรัฐโดยตรง ซึ่งจะได้รับการยกเว้นจากหน้าที่บางส่วน ภายใต้ PDPA (มาตรา ๔) แต่อย่างไรก็ตาม ต้องรองรับตีความขัดเจน โดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอีกครั้งก่อน
- การจัดทำทะเบียนบุคคลต้องห้ามหรือต้องเฝ้าระวัง สำนักงานตัวรวจแห่งชาติอาจอ้างฐานการปฏิบัติหน้าที่และการใช้งานจรัญ (Public Task) ได้ โดยถือว่ากระบวนการจัดทำทะเบียนดังกล่าวเป็นกระบวนการทำหน้าที่ตามกฎหมายของเจ้าหน้าที่ตัวรวจซึ่งมีหน้าที่และสิทธิอำนาจในการดำเนินการได้โดยตรงในฐานสำนักงานตัวรวจแห่งชาติ

๔.๓ สิ่งที่ต้องดำเนินการ

- สำนักงานตรวจสอบแห่งชาติต้องเก็บรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทั้งหมดที่เก็บรวบรวมมา โดยการจำกัดสิทธิผู้เข้าถึงและการจัดทำบันทึก (Log) ในส่วนของการดำเนินการเกี่ยวนี้องกับข้อมูลส่วนบุคคลนั้นอย่างดีที่สุด
- สำนักงานตรวจสอบแห่งชาติต้องแจ้งการประมวลผลข้อมูลส่วนบุคคลเพื่อการจัดทำทะเบียนไว้ใน “ประกาศเรื่อง แนวโน้มบายในการคุ้มครองข้อมูลส่วนบุคคล” (Privacy Statement / Privacy Notice) ซึ่งต้องมีการประกาศเป็นการทั่วไปให้สาธารณะทราบ
- สำนักงานตรวจสอบแห่งชาติต้องกำหนดระยะเวลาที่เหมาะสมในการลบทำลาย หรือปรับปรุงข้อมูลส่วนบุคคล กรณีไม่จำเป็นอย่างสมำเสมอ

๔.๔ การส่งต่อเปิดเผยรายชื่อบุคคลต้องห้าม

- สำนักงานตรวจสอบแห่งชาติ ต้องประเมินความจำเป็น และวัตถุประสงค์ในการขอเข้าถึงข้อมูลทะเบียนบุคคลต้องห้าม รวมถึงตรวจสอบสถานะความเกี่ยวข้องของหน่วยงานที่จะมีการขอเข้าถึงข้อมูลดังกล่าว โดยต้องใช้ความระมัดระวังอย่างมากในการเปิดเผย เนื่องจากข้อมูลนี้อาจถือเป็น ข้อมูลส่วนบุคคลอ่อนไหว
 - ◊ กรณีส่งต่อเพื่อความต่อเนื่องในกระบวนการดำเนินคดีอาญา สามารถดำเนินการได้ โดยได้รับการยกเว้นจากการปฏิบัติหน้าที่แจ้ง หรือขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลภายใต้ PDPA (มาตรา ๔)

- ◊ กรณีส่งต่อเพื่อเปิดเผยให้แก่หน่วยงานราชการอื่น สำนักงานตำราจะแห่งชาติต้องพิจารณาอำนาจและหน้าที่ของหน่วยงานผู้รับข้อมูลว่า มีความจำเป็นเกี่ยวข้องหรือไม่ และประเมินว่า การเปิดเผยข้อมูลส่วนบุคคลนั้นมีความจำเป็นเพื่อประโยชน์สาธารณะ โดยได้จัดให้มีมาตรการที่เหมาะสม เพื่อคุ้มครองสิทธิขั้นพื้นฐาน และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล แล้วหรือไม่ หากครบองค์ประกอบดังกล่าว สำนักงานตำราจะแห่งชาติยื่นสามารถส่งต่อเปิดเผยข้อมูลส่วนบุคคลดังกล่าวได้
 - ◊ สำนักงานตำราจะแห่งชาติควรหลีกเลี่ยงการเปิดเผยข้อมูลส่วนบุคคลในกรณีดังกล่าวให้แก่ หน่วยงานที่ไม่เกี่ยวข้องหรือบุคคลอื่น หรืออาจต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้นก่อน เว้นแต่มีกรณีกฎหมายหรือคำสั่งของหน่วยราชการอื่นมาอ้างอิง เช่น มีหมายหรือคำสั่งเพื่อการบังคับอื่นมาเพิ่มเติม
- สำนักงานตำราจะแห่งชาติควรต้องประเมินรูปแบบในการส่งต่อเปิดเผยข้อมูลส่วนบุคคลให้เหมาะสมอีกครั้ง
- ◊ กรณีเป็นการส่งผ่านในรูปแบบอิเล็กทรอนิกส์ ควรมีการเข้ารหัส (Encrypted) หรือกำหนดรูปแบบการส่งที่สามารถติดตามผู้มีสิทธิเข้าถึงได้ เพื่อป้องกันการได้รับหรือส่งต่อข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต และต้องบันทึกการทำเนินการที่เกี่ยวกับข้อมูลส่วนบุคคลของผู้รับและผู้ส่งข้อมูลดังกล่าวด้วย

- ◊ ควรเลี่ยงการส่งข้อมูลส่วนบุคคลในรูปแบบกระดาษ แต่หากจำเป็น ต้องปิดผนึกของ พร้อมข้อความ “ลับที่สุด” พร้อมกับมีการลงบันทึกการส่งต่อการเปิดเผยข้อมูลดังกล่าวไว้อย่างชัดเจน

๔.๕ การติดภาพของบุคคลต้องห้ามไว้ในพื้นที่ปฏิบัติงานที่ประชาชนอื่นอาจเห็นได้

- ด้วยเหตุที่ข้อมูลในทะเบียนดังกล่าว อาจได้รับการตีความเป็นข้อมูลส่วนบุคคลอ่อนไหว สำนักงานตำรวจแห่งชาติต้องใช้ความระมัดระวังสูงสุดในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลนั้น ไม่ว่าจะเป็นการประมวลผลข้อมูลส่วนบุคคลในขั้นตอนใด ซึ่งหลักการรักษาความมั่นคงปลอดภัยอันดับแรก คือ ไม่เปิดเผยให้แก่บุคคลที่ไม่มีความจำเป็น และ ต้องมีการจำกัดสิทธิในการเข้าถึงข้อมูลนั้น
- ◊ หากสำนักงานตำรวจแห่งชาตินำข้อมูลส่วนบุคคลความอ่อนไหวไปติดไว้ในบริเวณพื้นที่ปฏิบัติงานที่ประชาชนทั่วไปอาจเห็นได้ ควรต้องประเมินความจำเป็น เปรียบเทียบผลประโยชน์ที่จะได้รับกับความเสี่ยงที่ข้อมูลนั้นอาจถูกเปิดเผยหรือเผยแพร่ไปยังบุคคลที่ไม่เกี่ยวข้อง และสร้างความเสียหายแก่บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลอีกครั้ง
- ◊ ด้วยเหตุที่โอกาสที่บุคคลทั่วไปจะมีส่วนช่วยในการติดตามบุคคลในทะเบียนต้องห้าม Blacklisted / Stop-Listed อาจมีน้อยเกินกว่าที่จะเปิดเผยข้อมูลนั้นเป็นการสาธารณะ ซึ่งอาจ

สร้างความเสียหายได้มากกว่า สำนักงานตรวจแห่งชาติ จังควรหลีกเลี่ยงการเปิดเผยข้อมูลส่วนบุคคลเป็นการสาธารณะดังกล่าว

- ◊ กรณีต้องการความสะดวก อาจแจกภาพหรือรายชื่อภายในหน่วยงานที่เกี่ยวข้องของสำนักงานตรวจแห่งชาติได้ แต่ต้องกำหนดมาตรการจำกัดสิทธิ์เข้าถึงข้อมูลนั้นอีกด้วย

คำถามที่ ๕. การส่งต่อเปิดเผยข้อมูลไปให้แก่หน่วยงานหรือบุคคลภายนอก

๕.๑ ส่วนที่เกี่ยวข้องกับ PDPA

- การส่งต่อเปิดเผยข้อมูลในกระบวนการดำเนินคดีอาญาของบุคคลโดยสำนักงานตรวจแห่งชาติให้แก่ หน่วยงานราชการอื่นที่เกี่ยวข้องในกระบวนการพิจารณาคดี เช่น ศาล อัยการ ราชทัณฑ์ ทำได้และได้รับการยกเว้นจาก PDPA ภายใต้มาตรา ๔
- กรณีการส่งต่อเปิดเผยให้แก่ หน่วยงานราชการ แม้จะเป็นศาล อัยการ ราชทัณฑ์ ในส่วนขั้นตอนอื่นที่ไม่เกี่ยวข้องโดยตรงกับการดำเนินการในกระบวนการดำเนินคดี เช่น การทำโครงการความร่วมมือร่วมกัน หรือการทำการวิจัยร่วมกัน หรือการส่งต่อไปให้แก่ หน่วยงานอื่น ถือเป็นการประมวลผลข้อมูลส่วนบุคคลที่ต้องดำเนินการภายใต้ PDPA ทั้งหมด

๕.๒ ฐานกฎหมายในการประเมินผลข้อมูลส่วนบุคคล

- ข้อมูลทั้งหมดในกระบวนการดำเนินคดี และการคุ้มครองของสำนักงานตำรวจแห่งชาติ อาจถือเป็นข้อมูลส่วนบุคคลอ่อนไหว แต่หากเป็นการเปิดเผยข้อมูลให้แก่หน่วยงานอื่น เพื่อ “ประโยชน์สาธารณะที่สำคัญ” ถือว่าได้รับข้อยกเว้นจากการขอความยินยอมจากเจ้าของข้อมูล (มาตรา ๒๖ (จ))
- กรณีการเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวนั้นให้แก่ บุคคลอื่น (เช่น ญาติ หรือบุคคลที่เกี่ยวข้อง)
 - ◊ สำนักงานตำรวจแห่งชาติมิได้มีหน้าที่ตามกฎหมายโดยตรง ใน การเปิดเผยข้อมูลส่วนบุคคลอ่อนไหวให้แก่บุคคลผู้ไม่เกี่ยวข้อง เนื่องจากไม่ถือเป็นการดำเนินการเพื่อประโยชน์สาธารณะ ควรหลีกเลี่ยงการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลที่ไม่มีสิทธิเข้าถึงข้อมูลดังกล่าวอาจนำไปสู่การละเมิดข้อมูลส่วนบุคคล
 - ◊ การเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนเท่านั้น โดยต้องผ่านกระบวนการยืนยันตัวตนทั้งเจ้าของข้อมูลส่วนบุคคล และบุคคลที่ได้รับการอนุญาตให้มารับข้อมูลส่วนบุคคลตั้งกล่าวอย่างเหมาะสมก่อนการเปิดเผย
- กรณีเจ้าของข้อมูลส่วนบุคคล เป็นผู้ขอข้อมูลส่วนบุคคลนั้นเอง จะถือเป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิในการเข้าถึง หรือขอสำเนาข้อมูล ซึ่งเป็นสิทธิที่เจ้าของข้อมูลส่วนบุคคลมีภายใต้

PDPA โดยตรง แต่ในการเปิดเผยข้อมูลของสำนักงานสำรวจ แห่งชาติในกรณีดังกล่าวต้องดำเนินกระบวนการเพื่อยืนยันตัวตนของเจ้าของข้อมูลอย่างละเอียด นอกจากนี้ สำนักงานสำรวจ แห่งชาติต้องดำเนินการเพิ่มเติม ดังนี้

- ◊ ต้องตรวจสอบกฎหมายความมั่นคง หรือกฎหมายเฉพาะ อีกรอบด้วย ว่ามีข้อจำกัดข้อห้ามการเปิดเผยหรือไม่ หากมีข้อห้ามไว้ สามารถปฏิเสธการใช้สิทธิขอเข้าถึงข้อมูลของเจ้าของข้อมูลส่วนบุคคลนั้นได้
- ◊ ต้องมีการจัดทำบันทึกการใช้สิทธิเจ้าของข้อมูลไว้ให้ครบถ้วน เพื่อการตรวจสอบโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลในอนาคต

๕.๓ สิ่งที่ต้องดำเนินการ

- ในกรณีสำนักงานสำรวจแห่งชาติมีฐานกฎหมายรองรับในการส่งต่อ เปิดเผยข้อมูลส่วนบุคคลอ่อนไหว สำนักงานสำรวจแห่งชาติต้อง พิจารณารูปแบบในการส่งต่อเปิดเผยข้อมูล ซึ่งต้องรักษาความปลอดภัยให้ดีเป็นพิเศษ เนื่องจากเป็นข้อมูลส่วนบุคคลอ่อนไหว

คำถามที่ ๖. การเปิดให้บุคคลตรวจสอบประวัติอาชญากรรม

๖.๑ ส่วนที่เกี่ยวข้องกับ PDPA

- ประวัติอาชญากรรมจากการเก็บรวบรวมของสำนักงานตำรวจแห่งชาติ ได้รับการระบุชัดเจนภายใต้ PDPA ว่าถือเป็นข้อมูลส่วนบุคคลอ่อนไหว

๖.๒ กรณีเจ้าของข้อมูลส่วนบุคคลขอตรวจสอบเอง

- หากเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิในการเข้าถึง หรือขอสำเนาข้อมูล ซึ่งสำนักงานตำรวจแห่งชาติสามารถดำเนินการดังกล่าวได้ภายหลังจากดำเนินกระบวนการยืนยันตัวตนของเจ้าของข้อมูลอย่างครบถ้วนแล้ว
- สำนักงานตำรวจแห่งชาติต้องจัดทำบันทึกการใช้สิทธิเจ้าของข้อมูลไว้ให้ครบถ้วน ทั้งนี้เพื่อการตรวจสอบโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลในอนาคต
- เมื่อเปิดเผยข้อมูลส่วนบุคคลตั้งกล่าวไปให้แก่เจ้าของข้อมูลแล้ว เป็นสิทธิแต่เพียงฝ่ายเดียวของเจ้าของข้อมูลส่วนบุคคลในการนำข้อมูลนั้นไปใช้ประโยชน์ ทางสำนักงานตำรวจแห่งชาติ ไม่มีหน้าที่ต้องรับผิดชอบใดเพิ่มเติมอีก

๖.๓ กรณีนายจ้างขอตรวจข้อมูลของเจ้าของข้อมูลส่วนบุคคล

- นายจ้างต้องขอความยินยอมเฉพาะจากเจ้าของข้อมูลส่วนบุคคล พร้อมข้อความชัดเจนว่า ยินยอมให้บุคคลใดดำเนินการตรวจสอบ ประวัติดังกล่าว เพื่อจุดประสงค์ใด
- ต้องมีการตรวจสอบเอกสารหลักฐานในการแสดงตน และการให้ความยินยอมจากเจ้าของข้อมูลส่วนบุคคลให้ชัดเจน
- จำกัดขอบเขตข้อมูลส่วนบุคคลที่จะมีการเปิดเผยไปเพียงเท่าที่จำเป็นเท่านั้น และต้องมีการจัดทำระบบเพื่อบันทึกการขอสำเนา ข้อมูลของนายจ้างดังกล่าว เพื่อประโยชน์ในการตรวจสอบในอนาคต

คำถามที่ ๗. ระบบ CRIMES

๗.๑ ส่วนที่เกี่ยวข้องกับ PDPA

- ประวัติอาชญากรรม ภายใต้การคุ้มครองและบริหารจัดการของ สำนักงานตำรวจแห่งชาติ ได้รับการระบุชัดเจน ภายใต้ PDPA ว่าถือเป็นข้อมูลส่วนบุคคลอ่อนไหว ดังนั้นต้องใช้ความระมัดระวัง สูงสุดในการประมวลผล โดยเฉพาะการรักษาความมั่นคงปลอดภัย

๗.๒ ฐานกฏหมายในการประมวลผลข้อมูลส่วนบุคคล

- สำนักงานตำรวจแห่งชาติ สามารถเก็บรวบรวม และจัดทำระบบ CRIMES ได้ โดยอ้างอิงความจำเป็นภายใต้ฐานการปฏิบัติหน้าที่ และอำนาจ รัฐ (Public Tasks) ซึ่งดำเนินการเพื่อประโยชน์สาธารณะ ด้วยเหตุที่ระบบดังกล่าวจะช่วยในการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานทำได้สมบูรณ์มากขึ้น

๗.๓ สิ่งที่ต้องดำเนินการ

- ข้อมูลทั้งหมดที่บันทึกในระบบถือว่า เป็นข้อมูลส่วนบุคคล อ่อนไหว ดังนั้นการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ดังกล่าวทั้งหมดจำเป็นและสำคัญมาก เพื่อหลีกเลี่ยงโ途ปกรอง สรงสุด ๕,๐๐๐,๐๐๐ บาท และโทษทางอาญา
- สำนักงานตำรวจแห่งชาติต้องกำหนดสิทธิในการเข้าถึง และดำเนินกระบวนการประมวลผลข้อมูลส่วนบุคคลโดยของแต่ละบุคคล แต่ละผู้ใช้งาน (User Account) อย่างเหมาะสม ควบคุมให้มีการเข้าถึง และใช้ข้อมูลตามความจำเป็นและตามหน้าที่ (Role-Based Assessment) และต้องมีการตรวจสอบยืนยันตัวตนผู้มีสิทธิดังกล่าว อย่างเหมาะสม รวมถึงต้องทบทวนความจำเป็นในการเข้าถึงข้อมูลอย่างสม่ำเสมอ
- สำนักงานตำรวจแห่งชาติต้องกำหนดระยะเวลาในการลบ ทำลาย หรือเก็บบันทึก (archives) ข้อมูลส่วนบุคคลดังกล่าว ตามรอบ

ระยะเวลา เพื่อจำกัดจำนวน และปริมาณของข้อมูลส่วนบุคคลที่อาจมีการเปิดเผยและเข้าถึงได้

- สำนักงานตำรวจแห่งชาติต้องมีการจัดให้มีการรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ อย่างละเอียดด้วยมาตรฐานสูงสุด โดยเฉพาะกรณีมีการว่าจ้างผู้ให้บริการภายนอก ซึ่งบุคคลดังกล่าวอาจมีส่วนเข้าถึงข้อมูลส่วนบุคคลที่บันทึกในระบบ CRIMES สำนักงานตำรวจนแห่งชาติ ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องจัดทำ “สัญญาการประมวลผลข้อมูลส่วนบุคคล” (Data Processing Agreement) เพื่อเป็นหลักฐาน
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสำนักงานตำรวจนแห่งชาติ เป็นผู้มีหน้าที่หลักในการติดตามและตรวจสอบการทำงานโดยเฉพาะการรักษาความมั่นคงปลอดภัยของข้อมูลในระบบ CRIMES และต้องเตรียมกระบวนการรับภัยรับมือปัญหาที่เกิดจากการละเมิดข้อมูลส่วนบุคคลไว้อย่างเหมาะสม

คำถามที่ ๘. ประเภทคดี เข้า และ ไม่เข้าข่ายที่ ต้องดำเนินการ

๘.๑ การใช้ประมวลผลข้อมูลส่วนบุคคล ที่เป็นการดำเนินการเพื่อประโยชน์ส่วนตัวหรือครอบครัว ได้รับการยกเว้นทั้งหมดจาก การปฏิบัติตาม PDPA

- การฟ้องร้องที่เกิดจากการใช้ข้อมูลเพื่อประโยชน์ส่วนตัว (เช่น การ Post ใน Social Media ของเจ้าของข้อมูลส่วนบุคคลโดยตรง) ไม่ถือเป็นความรับผิดภารຍใต้ PDPA ทั้งสิ้น

๘.๒ โทษอาญาภายใต้ PDPA มี ๒ กรณี กล่าวคือ

- ความรับผิด มาตรา ๗๙
 - ◊ ผู้กระทำผิด คือ ผู้ควบคุมข้อมูลส่วนบุคคล (ได้แก่ องค์กรหรือ หน่วยงานต้นสังกัด หรือบุคคลธรรมดายี่ไม่ได้ดำเนินเพื่อประโยชน์ส่วนตัว)
 - เนพาผู้ควบคุมข้อมูลส่วนบุคคล ไม่ร่วมผู้ประมวลผล ข้อมูลส่วนบุคคล
 - ◊ องค์ประกอบความผิด
 - ฝ่าฝืนหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล เนพากรณีข้อมูลส่วนบุคคลอ่อนไหว และการฝ่าฝืน นัยเป็นเหตุที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย ได้ยึดเสีย ได้รับความอับอาย

- ฝ่ายนักกฎหมายที่ในการประมวลผลข้อมูลส่วนบุคคล
เฉพาะกรณีข้อมูลส่วนบุคคลอ่อนไหว เพื่อแสดงให้
ผลประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับ
ตนเอง หรือผู้อื่น
 - ผู้เสียหายยังคงต้องพิสูจน์เจตนาการกระทำการความผิด
- ◊ โทษ จำคุกไม่เกิน ๖ เดือน หรือปรับไม่เกิน ๕๐๐,๐๐๐ บาท
หรือทั้งจำทั้งปรับ (หากเกิดความเสียหายอับอาย) หรือ จำคุก
ไม่เกิน ๑ ปีหรือปรับไม่เกิน ๑,๐๐๐,๐๐๐ บาท หรือทั้งจำ
ทั้งปรับ (หากเป็นการแสวงหาผลประโยชน์มิชอบ)
- หมายเหตุ ความผิดมาตราเรานี้เป็นความผิดอันยอมความได้
 - ◊ โทษที่ลงต่อผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นนิติบุคคล หากการ
กระทำการ เกิดจากการสั่งการ หรือลงทะเบียนไม่สั่งการ ของกรรมการ
หรือผู้จัดการ หรือบุคคลที่มีหน้าที่รับผิดชอบ ผู้นั้นต้องรับโทษ
ซึ่งรวมถึงโทษจำคุก ทั้งนี้ผู้เสียหายต้องพิสูจน์ว่า กรรมการ
ผู้จัดการ หรือบุคคลที่มีหน้าที่รับผิดชอบ เป็นผู้สั่งการ หรือ
ควรอยู่ในสัยที่จะต้องสั่งการ แต่ละเว้นการปฏิบัติหน้าที่
- ความรับผิด มาตรา ๔๐
 - ◊ ผู้กระทำความผิด หมายถึง บุคคลใดก็ตามที่มีหน้าที่ตาม
PDPA ได้แก่ พนักงานภายในองค์กร (โดยเฉพาะ เจ้าหน้าที่
คุ้มครองข้อมูลส่วนบุคคล) หรือเจ้าพนักงานของสำนักงาน
คณะกรรมการ หรือบุคคลใดก็ตามที่มีหน้าที่

◊ องค์ประกอบความผิด

- ผู้นั้นต้องล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่น เนื่องจากการปฏิบัติหน้าที่ และต้องเปิดเผยข้อมูลส่วนบุคคลนั้นให้แก่ผู้อื่นโดยไม่ชอบด้วยกฎหมาย ไม่เข้าตามข้อยกเว้นการเปิดเผย เช่น การทำตามหน้าที่ตามกฎหมาย หรือการเปิดเผยโดยอ้างความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- ผู้เสียหายยังคงต้องพิสูจน์เจตนาการกระทำความผิด

◊ โทษ ผู้ที่กระทำผิดระหว่างโทษจำคุกไม่เกิน ๖ เดือนหรือปรับไม่เกิน ๕๐๐,๐๐๐ บาทหรือทั้งจำทั้งปรับ

- ไม่ได้กำหนดเป็นคดีที่ยอมความได้
- หากผู้กระทำความผิดเป็น นิติบุคคล และการกระทำผิดเกิดจากการสั่งการ หรือละเว้นไม่สั่งการ ของกรรมการ หรือผู้จัดการ หรือบุคคลที่มีหน้าที่รับผิดชอบของนิติบุคคลนั้นต้องรับโทษซึ่งรวมถึงโทษจำคุก

๙.๓ นอกเหนือจากความรับผิดทางอาญาทั้ง ๒ มาตรานี้แล้ว ไม่มีเหตุอันนำมาสู่โทษทางอาญาภายใต้ความรับผิดชอบดำเนินคดี โดยเจ้าหน้าที่ตำรวจอีก

- อาจเป็นส่วนที่แยกเป็น โทษทางแพ่ง ซึ่งเป็นเขตอำนาจของศาลแพ่ง หรือ

- อาจเป็นโทษทางปกครอง เช่น การตักเตือน การออกคำสั่งทางปกครอง หรือการปรับเงิน ซึ่งเป็นเขตอำนาจของคณะกรรมการผู้เชี่ยวชาญ ซึ่งมีอำนาจในการตัดสินเป็นที่สุด

บรรณานุกรม

กฎหมาย กฎกระทรวง และระเบียบ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึก
รายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. ๒๕๖๕

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการใน
การจัดทำและเก็บรักษาบันทึกรายการ

ของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูล
ส่วนบุคคล พ.ศ. ๒๕๖๕

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษา
ความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึก
รายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. ๒๕๖๕

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง คุณสมบัติและลักษณะ
ต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่งและการดำเนินงานอื่น
ของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. ๒๕๖๕

บรรณานุกรม (ต่อ)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ

ระเบียบคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยการยื่น การไม่รับเรื่องการยุติเรื่อง การพิจารณา และระยะเวลา เวลาในการพิจารณาคำร้องเรียน พ.ศ. ๒๕๖๕

ระเบียบว่าด้วยหลักเกณฑ์และวิธีการสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๓

ระเบียบว่าด้วยหลักเกณฑ์และวิธีการสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ฉบับที่ ๒) พ.ศ. ๒๕๖๔

บรรณานุกรม (ต่อ)

อื่นๆ

แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

แนวทางการดำเนินการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บ
รวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ประวัติผู้เรียบเรียง

ชื่อ	รับขวัญ ชลธรรมคุณ
วุฒิ	LL.M. (Banking & Financial Regulations), UCL, UK Certified Information Privacy Manager, IAPP
ตำแหน่ง	ประธานเจ้าหน้าที่ฝ่ายกฎหมาย, EasyPDPA Founder

คณะผู้จัดทำ

ผลสำรวจโภ ชนะชัย ลิ้มประเสริฐ

ผู้ทรงคุณวุฒิพิเศษ สำนักงานตำรวจแห่งชาติ

พันตำรวจเอก วีรพล ไหญ่อรุณ

รองผู้บังคับการ กองคดีอาญา

สำนักงานกฎหมายและคดี

พันตำรวจนอกหญิง วรวรรณ หวานานพ

ผู้กำกับการ ฝ่ายอำนวยการ

สำนักงานกฎหมายและคดี

พันตำรวจนอกหญิง ประพร เติมเกา

ผู้กำกับการ กลุ่มงานพัฒนากฎหมาย

สำนักงานกฎหมายและคดี

ว่าที่ร้อยตำรวจเอกหญิง จารุวรรณ บำรุงรักษ์ อาจารย์ (สบ ๑) กศ.นต.รร.นรต.

จำเลยตำรวจหญิง วิจิตร ชาติวงศ์

ผู้บังคับหมู่ ตรวจคนเข้าเมือง จังหวัดขอนแก่น

นักเรียนนายร้อยตำรวจ วันรัฐ์ จันยารมณ์

รองผู้บังคับหมู่ โรงเรียนนายร้อยตำรวจ

นักเรียนนายร้อยตำรวจ ณพพลวัฒน์ ศรีกระจาง

รองผู้บังคับหมู่ โรงเรียนนายร้อยตำรวจ

นักเรียนนายร้อยตำรวจ วิรติกร ปิดพัด

รองผู้บังคับหมู่ โรงเรียนนายร้อยตำรวจ

นักเรียนนายร้อยตำรวจ รักษาพงศ์ ปัญญา

รองผู้บังคับหมู่ โรงเรียนนายร้อยตำรวจ

นักเรียนนายร้อยตำรวจ ราชัน ชัยนนกี

รองผู้บังคับหมู่ โรงเรียนนายร้อยตำรวจ

คณะผู้จัดทำ (ต่อ)

- | | |
|--|---------------------------------------|
| นักเรียนนายร้อยตำรวจ มนځګاټه วารรณ์ประดิษฐ์ | รองผู้บังคับหมู่ โรงเรียนนายร้อยตำรวจ |
| นักเรียนนายร้อยตำรวจ ชีรพัฒน์ บุษารัมย์ | รองผู้บังคับหมู่ โรงเรียนนายร้อยตำรวจ |
| นักเรียนนายร้อยตำรวจ วีระภัทร สุวนวัฒนาเจริญ | รองผู้บังคับหมู่ โรงเรียนนายร้อยตำรวจ |
| นักเรียนนายร้อยตำรวจ วุฒินันท์ ตาตะ | รองผู้บังคับหมู่ โรงเรียนนายร้อยตำรวจ |

 บันทึกช่วยจำ 

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

፩፪

