ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ
ตามมาตรา ๒๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
พ.ศ. ๒๕๖๖

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และ (๕) ประกอบมาตรา ๒๙ วรรคสองและวรรคสาม แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ตามมาตรา ๒๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดเก้าสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“เครือกิจการหรือเครือธุรกิจเดียวกัน” หมายความว่า กิจการที่ผู้ประกอบกิจการมีอำนาจควบคุมหรือบริหารจัดการเหนือกิจการอื่น หรือกิจการที่ถูกควบคุมโดยผู้ประกอบกิจการที่มีอำนาจเหนือกิจการอื่นในรูปแบบบริษัทใหญ่ บริษัทย่อย หรือบริษัทร่วม รวมทั้งบุคคลธรรมดาหรือนิติบุคคลที่มีความเกี่ยวข้องกันทางกฎหมายหรือเกี่ยวข้องกันเนื่องจากประกอบกิจการหรือธุรกิจร่วมกัน โดยใช้หลักเกณฑ์การพิจารณาตามกฎหมายที่เกี่ยวข้องและมาตรฐานทางบัญชีอันเป็นที่ยอมรับโดยทั่วไป

“ผู้ส่งหรือโอนข้อมูลส่วนบุคคล” หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลส่วนบุคคลที่อยู่ต่างประเทศ

“ผู้รับข้อมูลส่วนบุคคล” หมายความว่า ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ต่างประเทศ ที่รับข้อมูลส่วนบุคคลจากผู้ส่งหรือโอนข้อมูลส่วนบุคคลเพื่อการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ให้บริการระบบคลาวด์ (cloud computing service provider)” หมายความว่า ผู้ให้บริการเก็บรักษาข้อมูลหรือเก็บพักข้อมูลแก่บุคคลอื่นในรูปแบบชั่วคราวหรือถาวร โดยมีระบบที่บริหารจัดการข้อมูลบนอินเทอร์เน็ต โดยอาจให้บริการในรูปแบบต่าง ๆ เช่น ผู้ให้บริการโครงสร้างพื้นฐานหลัก (Infrastructure as a Service : IaaS) ผู้ให้บริการแพลตฟอร์ม (Platform as a Service : PaaS) ผู้ให้บริการซอฟต์แวร์ (Software as a Service: SaaS) ผู้ให้บริการระบบจัดเก็บข้อมูล (Data Storage as a Service : DSaaS) และผู้ให้บริการระบบบริหารจัดการข้อมูลแบบ Serverless Computing หรือผู้ให้บริการฟังก์ชัน (Function as a Service : FaaS) เป็นต้น

“ส่งหรือโอนข้อมูลส่วนบุคคล” หมายความว่า ส่งหรือโอนข้อมูลส่วนบุคคลโดยผู้ส่งหรือโอนข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการส่งหรือโอนข้อมูลโดยทางกายภาพ หรือผ่านระบบคอมพิวเตอร์หรือระบบเครือข่าย ให้แก่ผู้รับข้อมูลส่วนบุคคล แต่มิให้หมายความรวมถึงการส่งและรับข้อมูลส่วนบุคคลในลักษณะที่เป็นเพียงสื่อกลาง (intermediary) ในการส่งผ่านข้อมูล (data transit) ระหว่างระบบคอมพิวเตอร์หรือระบบเครือข่ายหรือการเก็บพักข้อมูล (data storage) ในรูปแบบชั่วคราวหรือถาวรที่ไม่มีบุคคลภายนอกเข้าถึงข้อมูลส่วนบุคคลดังกล่าว นอกเหนือจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นผู้ส่งข้อมูลส่วนบุคคลนั้น หรือบุคลากร พนักงาน หรือลูกจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้น เช่น กรณีการส่งข้อมูลผ่านระบบเครือข่ายในต่างประเทศ หรือการส่งข้อมูลผ่านระบบของผู้ให้บริการระบบคลาวด์ (cloud computing service provider) ที่ไม่มีบุคคลใดนอกจากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นผู้ส่งข้อมูลส่วนบุคคลนั้น หรือบุคลากร พนักงาน หรือลูกจ้าง เข้าถึงข้อมูลส่วนบุคคล เนื่องจากมีมาตรการทางเทคนิคหรือเงื่อนไขทางกฎหมายรองรับ

“นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (binding corporate rules)” หมายความว่า นโยบายหรือข้อตกลงในการคุ้มครองข้อมูลส่วนบุคคลที่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลตกลงร่วมกันและมีผลผูกพัน เพื่อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมระหว่างเครือกิจการหรือเครือธุรกิจเดียวกัน

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๔ ให้ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้รักษาการตามประกาศนี้

หมวด ๑
นโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน

ข้อ ๕ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรอาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันได้ตามมาตรา ๒๙ วรรคหนึ่งแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หากผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลดังกล่าวได้มีการกำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (binding corporate rules) เพื่อการประกอบกิจการหรือธุรกิจร่วมกันที่ได้รับการตรวจสอบและรับรองจากสำนักงานแล้ว

ข้อ ๖ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่จะส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกัน สามารถเสนอนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (binding corporate rules) เพื่อการประกอบกิจการหรือธุรกิจร่วมกันตามข้อ ๕ เพื่อให้สำนักงานตรวจสอบและรับรองตามประกาศนี้ได้ โดยให้ยื่นนโยบายดังกล่าวโดยวิธีการใดวิธีการหนึ่ง ดังต่อไปนี้

(๑) ยื่นโดยตรงต่อสำนักงาน

(๒) ยื่นผ่านทางไปรษณีย์มายังสำนักงาน

(๓) ยื่นผ่านทางช่องทางอิเล็กทรอนิกส์หรือช่องทางอื่นใดตามที่สำนักงานกำหนด

ข้อ ๗ ให้สำนักงานตรวจสอบและรับรองนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (binding corporate rules) เพื่อการประกอบกิจการหรือธุรกิจร่วมกันที่ได้มีการยื่นตามข้อ ๖ ตามหลักเกณฑ์และมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ระบุไว้ในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายลำดับรองและประกาศที่เกี่ยวข้อง โดยให้ตรวจสอบเนื้อหาสาระของนโยบายในการคุ้มครองข้อมูลส่วนบุคคล ว่าต้องเป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

(๑) การมีผลและสภาพบังคับในทางกฎหมายของนโยบายในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวกับนิติบุคคลหรือบุคคลธรรมดาในเครือกิจการหรือเครือธุรกิจเดียวกัน ตลอดจนผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง ผู้ส่งหรือโอนข้อมูลส่วนบุคคล และผู้รับข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เสนอนโยบายให้สำนักงานตรวจสอบและรับรอง ทั้งนี้ นโยบายดังกล่าวต้องสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และต้องมีผลผูกพันต่อบุคลากร พนักงาน ลูกจ้าง หรือบุคคลที่เกี่ยวข้องกับผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคล และการส่งหรือโอนข้อมูลส่วนบุคคลและการรับข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันด้วย

(๒) ข้อกำหนดที่รับรองการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคลและการร้องเรียน สำหรับข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนไปยังต่างประเทศ

(๓) มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยมาตรการรักษาความมั่นคงปลอดภัยจะต้องเป็นไปตามมาตรฐานขั้นต่ำตามที่กฎหมายกำหนดด้วย

หมวด ๒
มาตรการคุ้มครองที่เหมาะสม (Appropriate Safeguards)

ข้อ ๘ ในกรณีที่ยังไม่มีคำวินิจฉัยเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลของคณะกรรมการตามมาตรา ๒๘ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือยังไม่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลตามข้อ ๕ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามมาตรา ๒๘ เมื่อได้จัดให้มีมาตรการคุ้มครองที่เหมาะสม (appropriate safeguards) ซึ่งสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ และมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ

มาตรการคุ้มครองที่เหมาะสมตามวรรคหนึ่ง อาจอยู่ในรูปแบบ ดังนี้

(๑) ข้อสัญญาที่เป็นไปตามข้อสัญญาในการส่งหรือโอนข้อมูลส่วนบุคคลที่เป็นที่ยอมรับซึ่งเป็นข้อสัญญาในการคุ้มครองข้อมูลส่วนบุคคล ในส่วนที่เกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดน หรือการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศ ที่คณะกรรมการกำหนดให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลใช้เพื่อกำหนดหน้าที่และเงื่อนไขของคู่สัญญา เพื่อให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

(๒) การรับรอง (certification) เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในส่วนที่เกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดน หรือการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศ ว่ามีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม โดยเป็นไปตามมาตรฐานที่เป็นที่ยอมรับ

(๓) ข้อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลในตราสารหรือข้อตกลงที่มีผลผูกพันทางกฎหมายและสามารถใช้บังคับได้ระหว่างหน่วยงานของรัฐของประเทศไทยกับหน่วยงานของรัฐของประเทศอื่น ในกรณีการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างหน่วยงานของรัฐของประเทศไทยกับหน่วยงานของรัฐของประเทศอื่นนั้น

ข้อ ๙ มาตรการคุ้มครองที่เหมาะสมตามข้อ ๘ ต้องเป็นไปตามหลักเกณฑ์ ดังต่อไปนี้

(๑) การมีผลและสภาพบังคับในทางกฎหมายของมาตรการคุ้มครองข้อมูลส่วนบุคคลและมาตรการเยียวยาทางกฎหมายกับนิติบุคคลหรือบุคคลธรรมดาที่เป็นผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคล ตลอดจนผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง ไม่ว่าผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลนั้นจะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลก็ตาม ทั้งนี้ มาตรการคุ้มครองที่เหมาะสมดังกล่าวต้องสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และต้องมีผลผูกพันต่อบุคลากร พนักงาน ลูกจ้าง หรือบุคคลที่เกี่ยวข้องกับผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลด้วย

(๒) ข้อกำหนดที่รับรองการคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคลและการร้องเรียน สำหรับข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนไปยังต่างประเทศ

(๓) มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยมาตรการรักษาความมั่นคงปลอดภัยจะต้องเป็นไปตามมาตรฐานขั้นต่ำตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลด้วย

ข้อ ๑๐ ภายใต้บังคับข้อ ๙ ข้อสัญญาในเรื่องการส่งหรือโอนข้อมูลส่วนบุคคลตามข้อ ๘ วรรคสอง (๑) จะต้องมีลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้

(๑) ข้อสัญญาที่คู่สัญญาจัดทำขึ้นและมีผลผูกพันที่มีเนื้อหาและข้อกำหนดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

(ก) การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล รวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับข้อมูลส่วนบุคคล ต้องเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ข) ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย โดยต้องเป็นไปตามมาตรฐานขั้นต่ำตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(ค) กรณีผู้รับข้อมูลส่วนบุคคลเป็นผู้ประมวลผลข้อมูลส่วนบุคคล

๑) ผู้รับข้อมูลส่วนบุคคลต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ส่งหรือโอนข้อมูลส่วนบุคคล และตามวัตถุประสงค์ที่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลกำหนดไว้เท่านั้น

๒) ผู้รับข้อมูลส่วนบุคคลจะต้องติดต่อผู้ส่งหรือโอนข้อมูลส่วนบุคคลในโอกาสแรกที่ทำได้ หากเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เว้นแต่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลจะมอบหมายให้ผู้รับข้อมูลส่วนบุคคลดำเนินการตามคำขอใช้สิทธิดังกล่าวแทนผู้ส่งหรือโอนข้อมูลส่วนบุคคล

๓) ผู้รับข้อมูลส่วนบุคคลต้องส่งคืนข้อมูลส่วนบุคคลตามข้อสัญญาแก่ผู้ส่งหรือโอนข้อมูลส่วนบุคคล หรือลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ โดยวิธีการที่เหมาะสม ตามหลักเกณฑ์และเงื่อนไขที่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลกำหนด และผู้รับข้อมูลส่วนบุคคลจะต้องยืนยันเป็นลายลักษณ์อักษรต่อผู้ส่งหรือโอนข้อมูลส่วนบุคคลเมื่อมีการดำเนินการดังกล่าวแล้ว

๔) ผู้รับข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้

(ง) กรณีผู้รับข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคล ผู้รับข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลด้วยในกรณีที่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งต้องแจ้งโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(จ) ต้องมีมาตรการเยียวยาทางกฎหมายแก่เจ้าของข้อมูลส่วนบุคคลหรือสิทธิของเจ้าของข้อมูลส่วนบุคคลที่จะได้รับการเยียวยาตามกฎหมายที่มีประสิทธิภาพ (effective legal remedies)

(๒) ข้อสัญญาที่คู่สัญญาจัดทำขึ้นตามกฎหมายของต่างประเทศ หรือจัดทำโดยองค์การระหว่างประเทศ และมีเนื้อหาและข้อกำหนดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล โดยใช้ข้อสัญญาต้นแบบอย่างใดอย่างหนึ่ง ดังนี้

(ก) ข้อสัญญาต้นแบบของอาเซียนสำหรับการไหลเวียนข้อมูลข้ามพรมแดน (ASEAN Model Contractual Clauses for Cross Border Data Flows)

(ข) ข้อสัญญามาตรฐานสำหรับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (Standard Contractual Clauses for the Transfer of Personal Data to Third Countries) ที่ออกตามความใน Article 46 (1) ประกอบ Article 46 (2) (c) และ Article 28 (7) ของกฎหมาย Regulation (EU) 2016/679 ของสหภาพยุโรป (European Union) หรือ General Data Protection Regulation (GDPR)

(ค) ข้อสัญญามาตรฐานสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศของหน่วยงาน หรือองค์การระหว่างประเทศอื่นตามที่คณะกรรมการประกาศกำหนด

ข้อ ๑๑ ข้อสัญญาตามข้อ ๑๐ (๒) ต้องมีเนื้อหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเรื่องดังต่อไปนี้

(๑) มาตรการแจ้งการส่งหรือโอนข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ

(๒) มาตรการจำกัดการส่งหรือโอนข้อมูลส่วนบุคคลให้เป็นไปเท่าที่จำเป็นและเกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเท่านั้น

(๓) มาตรการทางเลือกแก่เจ้าของข้อมูลส่วนบุคคล ในการใช้สิทธิยกเลิกการส่งหรือโอนข้อมูลส่วนบุคคลไปยังบุคคลภายนอกหรือยกเลิกการใช้ข้อมูลส่วนบุคคลนอกขอบเขตวัตถุประสงค์

(๔) มาตรการกำหนดความรับผิดชอบในการส่งหรือโอนข้อมูลส่วนบุคคลไว้ในสัญญาเพื่อกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม รวมถึงการคุ้มครองการส่งหรือโอนข้อมูลส่วนบุคคลไปยังบุคคลภายนอก

(๕) มาตรการรักษาความมั่นคงปลอดภัยในการส่งหรือโอนข้อมูลส่วนบุคคลเพื่อมิให้เกิดการละเมิดข้อมูลส่วนบุคคล

(๖) มาตรการในการกำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคล การดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด และการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

(๗) มาตรการเยียวยาความเสียหายในทางกฎหมายที่มีประสิทธิภาพ การบังคับใช้กฎหมายและการกำหนดความรับผิด อันเกิดจากการส่งหรือโอนข้อมูลส่วนบุคคลโดยมิชอบ

ข้อ ๑๒ ในกรณีที่มีการใช้ข้อสัญญาตามข้อ ๑๐ (๒) หากมีการอ้างอิงกฎหมายที่ใช้บังคับการแก้ไขเพิ่มเติมเนื้อหาเรื่องอื่นในข้อสัญญา หรือเพิ่มเติมมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม หรือการแก้ไขเพิ่มเติมเนื้อหาในส่วนที่ไม่ใช่สาระสำคัญ ซึ่งไม่ขัดต่อหลักการตามข้อ ๑๑ และไม่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ให้สามารถกระทำได้

ข้อ ๑๓ ให้สำนักงานเผยแพร่ข้อมูลและรายละเอียดของข้อสัญญาต้นแบบตามข้อ ๑๐ (๒) ผ่านเว็บไซต์ของสำนักงานด้วย

ข้อ ๑๔ การรับรอง (certification) เกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ในส่วนที่เกี่ยวกับการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดน หรือการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศ ว่ามีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม (appropriate safeguards) โดยเป็นไปตามมาตรฐานที่เป็นที่ยอมรับ ตามข้อ ๘ วรรคสอง (๒) ให้เป็นไปตามที่คณะกรรมการประกาศกำหนด ซึ่งจะต้องมีเนื้อหาตามข้อ ๑๑ ด้วย

ประกาศ ณ วันที่ ๑๒ ธันวาคม พ.ศ. ๒๕๖๖
เธียรชัย ณ นคร
ประธานกรรมการคุ้มครองข้อมูลส่วนบุคคล