นโยบายความปลอดภัยสารสนเทศและแนวปฏิบัติการรักษาความปลอดภัย ในส่วนข้อมูลส่วนบุคคล บริษัทซินเน็ค (ประเทศไทย)จำกัด (มหาชน)

(IT policy and Personal Data Protection Policy.

---

1. บทนำ

เนื่องจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้บริษัทซินเน็ค (ประเทศไทย) จำกัด (มหาชน) ซึ่งต่อไปในนโยบายจะเรียกว่า “บริษัท” ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมในการป้องกันข้อมูลส่วนบุคคลของบุคคลต่างๆ ในความควบคุมของบริษัท เช่น ลูกค้า พนักงาน คู่ค้า ฯลฯ บริษัทจึงมีความจำเป็นต้องกำหนดแนวปฏิบัติและมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของบุคคลธรรมดาที่เกี่ยวข้องกับการประกอบธุรกิจของบริษัท เพื่อให้สอดคล้องกับกฎหมาย ภายใต้รายละเอียดตามนโยบายฉบับนี้

2. วัตถุประสงค์

นโยบายฉบับนี้มีวัตถุประสงค์เพื่อ

• เพื่อชี้แจงความรับผิดชอบและแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่บุคคลากร หน่วยงาน ฝ่ายงาน ของบริษัท รวมถึงผู้รับจ้าง ผู้รับเหมา คู่ค้า ของบริษัท เกี่ยวกับความรับผิดชอบในการคุ้มครองข้อมูลส่วนบุคคล

• เพื่อกำหนดมาตรฐานและแนวทางบริหารจัดการข้อมูลส่วนบุคคลเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยครอบคลุมถึงการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลทั้งหมดที่อยู่ในความควบคุมของบริษัท

3. ขอบเขตของนโยบาย

นโยบายฉบับนี้ใช้บังคับการจัดการและวางแนวปฏิบัติในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของบุคคลธรรมดาในสถานะต่างๆ ซึ่งบริษัทมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล โดยมีผลบังคับและกำหนดแนวปฏิบัติที่ครอบคลุมถึงบุคลากรทั้งหมด ได้แก่ พนักงานประจำ พนักงานชั่วคราว พนักงานสัญญาจ้าง รวมถึงสายงาน ฝ่ายงาน ทั้งหมดของบริษัท รวมถึงผู้รับจ้าง ผู้รับเหมา คู่ค้า ของบริษัท ซึ่งมีส่วนร่วมในการเข้าถึงหรือประมวลผลข้อมูลส่วนบุคคลของบุคคลทุกประเภทที่อยู่ในความควบคุมของบริษัท

เนื่องจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหน้าที่ให้บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยหลายด้าน เช่น มาตรการทางเทคนิค มาตรการ

ทางบริหารจัดการ มาตรการทางกายภาพ และข้อมูลส่วนบุคคลที่อยู่ภายใต้มาตรการดังกล่าวรวมถึงข้อมูลคอมพิวเตอร์และข้อมูลรูปแบบอื่นด้วย ทั้งนี้ในส่วนของการกำหนดมาตรการทางเทคนิคนั้น บริษัทได้จัดให้มี “IT Policy” (นโยบายความปลอดภัยระบบสารสนเทศ) ซึ่งมีขอบเขตกำหนดแนวปฏิบัติการรักษาความปลอดภัยในระบบ เครือข่าย อุปกรณ์สารสนเทศ สำหรับทรัพยากรคอมพิวเตอร์ทุกประเภทของบริษัท ไม่จำกัดเฉพาะข้อมูลส่วนบุคคล บริษัทจึงกำหนดนโยบายนี้เพิ่มเติมเฉพาะในส่วนการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ดังนั้น ในส่วนหลักการที่เกี่ยวกับการกำหนดมาตรการทางเทคนิคในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลส่วนใดที่ได้กำหนดไว้แล้วใน “IT Policy” ก็ให้ถือแนวปฏิบัติตามนโยบายดังกล่าว

นโยบายนี้เป็นแนวปฏิบัติภายในของบริษัทสำหรับการกำหนดมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล จึงเป็นคนละส่วนและแยกเป็นเอกสารคนละฉบับกับ นโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy policy) อันเป็นการแจ้งรายละเอียดและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบ

4. นิยาม

การประมวลผล (Processing)	หมายถึง การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล
ข้อมูลส่วนบคล	หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ อาทิ ชื่อ นามสกุล อายุ วันเดือนปีเกิด หมายเลขโทรศัพท์ หมายเลขบัตรประจำตัวประชาชน และ/หรือข้อมูลอื่นใดตามที่กฎหมายกำหนด เป็นต้น
ข้อมูลส่วนบุคคลอ่อนไหวหรือละเอียดอ่อน	หมายถึง ข้อมูลที่ระบุตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อมและเป็นข้อมูลที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	หมายถึง บุคคลที่ข้อมูลส่วนบุคคลนั้นระบุถึง ไม่รวมถึง “นิติบุคคล” ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัท, สมาคม, มูลนิธิ หรือองค์กรอื่นใด

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในที่นี้คือบริษัท ซินเน็ค (ประเทศไทย) จำกัด (มหาชน) หรือ “บริษัท”
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัท

5. หลักการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

• นโยบายฉบับนี้ จัดให้มีการประกาศและสื่อสารไปยังพนักงานและหน่วยงานที่เกี่ยวข้อง และกำหนดให้มีการทบทวนและปรับปรุงนโยบายฉบับนี้ให้เป็นปัจจุบันอย่างสม่ำเสมอ

• การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล จะต้องเป็นไปตามวัตถุประสงค์ที่กำหนดในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy policy) ตามประเภทเจ้าของข้อมูลที่บริษัทจัดทำขึ้น

• โดยหลักแล้ว ข้อมูลส่วนบุคคลถือเป็นความลับและจะสามารถเปิดเผยต่อบุคลากรเฉพาะที่ได้รับอนุญาตตามข้อกำหนดทางกฎหมาย นโยบาย และ ระเบียบของบริษัท

• การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข และเปิดเผยข้อมูลส่วนบุคคล จะกระทำได้เฉพาะบุคคลที่มีอำนาจและได้รับมอบหมาย รวมทั้งสายงานที่เกี่ยวข้อ ซึ่งต้องร่วมดำเนินการให้มีการควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม เพื่อให้มั่นใจว่าบุคคลที่เกี่ยวข้องมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้รายละเอียดที่บริษัทกำหนดขึ้น

• บริษัทฯ อนุญาตให้จัดเก็บข้อมูลส่วนบุคคลภายในระยะเวลาที่บริษัทกำหนดเท่านั้น ซึ่งต้องพิจารณาเชื่อมโยงกับระยะเวลาจัดเก็บข้อมูลที่แจ้งให้เจ้าของข้อมูลส่วนบุคคลแต่ละประเภททราบใน “นโยบายคุ้มครองข้อมูลส่วนบุคคล” (Privacy policy) สำหรับ ข้อมูลส่วนบุคคลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด ผู้รับผิดชอบจะต้องมีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้

• บริษัทมีอำนาจในการกำหนดรายละเอียดในการจัดชั้นความลับของข้อมูลส่วนบุคคล ให้เหมาะสมกับประเภทและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้นๆ

• การจัดให้มีมาตรการทางเทคนิคในการป้องกันความปลอดภัยข้อมูลส่วนบุคคล ในส่วนโครงสร้างพื้นฐานสารสนเทศ (Infrastructure) เช่น การควบคุมการเข้าถึงเครือข่าย (Network) การรักษาความปลอดภัยในอุปกรณ์ฮาร์ดแวร์และซอฟท์แวร์ การป้องกันมัลแวร์ เป็นไปตามรายละเอียดที่กำหนดใน “IT Policy”

• การประมวลผลข้อมูลส่วนบุคคลจะต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ ตามที่ระบุใน “IT Policy” ซึ่งรวมถึงการป้องกันการประมวลผลข้อมูลส่วนบุคคลโดยผู้ที่ไม่มีสิทธิ การลบหรือทำลายข้อมูลทั้งโดยความตั้งใจและไม่ตั้งใจ การดำเนินการสำรองข้อมูล การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

6. การควบคุมการเข้าถึงและการกำหนดสิทธิเข้าถึงข้อมูลส่วนบุคคล

บริษัทกำหนดมาตรการป้องกันความปลอดภัยข้อมูลส่วนบุคคล 3 กลุ่มมาตรการหลักคือ

- มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)

- มาตรการป้องกันด้านเทคนิค (technical safeguard)

- มาตรการป้องกันทางกายภาพ (physical safeguard)

มาตรการทั้ง 3 กลุ่มข้างต้น ต้องประกอบด้วยการดำเนินการเพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access control) ดังนี้

(1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูล ส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(2) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

(3) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุม การเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

(4) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกัน การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูล ส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

การดำเนินการตามรายละเอียดของมาตรการทั้ง 3 กลุ่ม อย่างน้อยต้องปฏิบัติดังต่อไปนี้

• บริษัทกำหนดสิทธิให้พนักงานในฝ่าย IT เข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็นเพื่อการปฏิบัติงานตามตำแหน่งหน้าที่และที่ได้รับมอบหมายจากบริษัท ภายใต้เงื่อนไขและรายละเอียดที่กำหนดใน “IT Policy” เช่น ช่วงและระยะเวลาการเข้าออก การจำแนกตำแหน่งและระดับของพนักงานที่มีสิทธิเข้าถึง

• บริษัทกำหนดมาตรการทางกายภาพและทางเทคนิคเพื่อควบคุมการเข้าถึงห้องศูนย์คอมพิวเตอร์ของพนักงาน เช่น มาตรการตรวจสอบรายชื่อบุคคลเข้าและออก มาตรการติดตั้งอุปกรณ์ scan บุคคลเข้าและออก ตามรายละเอียดที่กำหนดใน “IT Policy”

• บริษัทกำหนดมาตรการทางกายภาพและทางเทคนิคเพื่อควบคุมการเข้าถึงห้องศูนย์คอมพิวเตอร์ของบุคคลภายนอก เช่น มาตรการกำหนดรหัสผ่านชั่วคราว มาตรการลงทะเบียนตรวจสอบบุคคลภายนอก ตามรายละเอียดที่กำหนดใน “IT Policy”

• บริษัทกำหนดมาตรการรักษาความปลอดภัยทางกายภาพของศูนย์คอมพิวเตอร์ เช่น การป้องกันอุบัติเหตุ ตามรายละเอียดที่กำหนดใน “IT Policy”

• หน่วยงานที่เกี่ยวข้องต้องทำการทบทวนสิทธิพนักงานที่มีหน้าที่เกี่ยวข้องเข้าถึงข้อมูลเท่าที่จำเป็นและควบคุมการเข้าถึงระบบงาน และบริหารจัดการสิทธิของพนักงานให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งหรือการจ้างงาน ตามรายละเอียดที่กำหนดใน “IT Policy”

• การเข้าถึงและการกำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคลของบริษัทในระบบ Synnex Domain, Synnex Application, Database ของบริษัท เป็นไปตามรายละเอียดและเงื่อนไขใน “IT Policy” รวมทั้งระเบียบที่เกี่ยวข้อง เช่น ระเบียบข้อบังคับการทำงาน คำสั่งและอำนาจบังคับบัญชาของบริษัทต่อพนักงานตามตำแหน่งงาน

• รายละเอียดของการเข้าถึงและการกำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคลที่ไม่ได้ระบุในนโยบายนี้ เป็นไปตาม “IT Policy” รวมทั้งระเบียบที่เกี่ยวข้อง เช่น ระเบียบข้อบังคับการทำงาน คำสั่งและอำนาจบังคับบัญชาของบริษัทต่อพนักงานตามตำแหน่งงาน

• ฝ่าย IT มีหน้าที่ติดตามตรวจสอบการเข้าถึงระบบงานอย่างสม่ำเสมอเพื่อตรวจสอบความผิดปกติของการเข้าถึงข้อมูลส่วนบุคคลและสามารถแก้ไขปัญหาได้ทันท่วงที และรายงานผลการตรวจสอบตามลำดับขั้น ในกรณีที่บริษัทมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จะต้องเข้ามามีส่วนร่วมกับฝ่าย IT ในการตรวจสอบและจัดทำรายงานด้วย

7.อุปกรณ์ในการทำงานที่เกี่ยวกับข้อมูลส่วนบุคคล

- การนำอุปกรณ์คอมพิวเตอร์ส่วนตัวมาใช้ในการปฏิบัติงาน และการติดตั้งโปรแกรม เป็นไปตามเงื่อนไขที่กำหนดใน “IT Policy”

- บริษัทไม่อนุญาตให้พนักงานใช้งานอุปกรณ์บันทึกข้อมูล ในการบันทึกข้อมูลส่วนบุคคลใดๆที่เกี่ยวข้องกับการปฏิบัติงาน เว้นแต่จะเป็นการปฏิบัติตามตำแหน่งหน้าที่ที่ได้รับมอบหมายหรือได้รับอนุญาตตามลำดับขั้น

- บริษัทไม่อนุญาตให้ใช้อุปกรณ์ส่วนตัวของพนักงานในการบันทึกข้อมูลส่วนบุคคล เช่น Hard disk, External drive, Thumb Drive ยกเว้นอุปกรณ์นั้นจะได้รับการตรวจสอบจากฝ่าย IT และได้รับอนุญาตตามลำดับขั้น โดยหากอุปกรณ์บันทึกข้อมูลนั้นจัดเก็บข้อมูลส่วนบุคคลจะต้องได้รับการเข้ารหัส

-ในกรณีเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล จะต้องได้รับอนุมัติตามลำดับขั้น และให้มีการบันทึกการรับ-ส่ง อุปกรณ์จัดเก็บข้อมูลดังกล่าวด้วย

- ในกรณีที่มีการจัดเก็บข้อมูลที่มีข้อมูลส่วนบุคคลในอุปกรณ์ชนิดพกพา จะต้องมีการบันทึกรายละเอียดของข้อมูลส่วนบุคคล

-การสั่งพิมพ์เอกสารใดๆ ที่มีข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบการใช้เอกสารดังกล่าวให้เป็นไปตามขั้นตอนการทำงานและสอดคล้องกับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล และข้อมูลเอกสารอันเกิดจากการสั่งพิมพ์ต้องไม่ถูกทิ้งไว้ที่เครื่อง Printer หลังจากทำการพิมพ์แล้ว

8. การทำงานเกี่ยวกับข้อมูลส่วนบุคคลนอกสถานที่

• การทำงานเกี่ยวกับข้อมูลส่วนบุคคลที่เกิดขึ้นจากภายนอกสถานที่ทำงาน หรือการทำงานที่บ้านเป็นทางเลือกหนึ่งในการบริหารจัดการ เฉพาะตามที่บริษัทอนุญาต สำหรับสิทธิในการเข้าถึงข้อมูลจาก

ภายนอกจะต้องได้รับการอนุมัติตามลำดับขั้น ก่อนที่พนักงานจะสามารถเริ่มการใช้งานข้อมูลจากภายนอกได้

• พนักงานจะต้องตรวจสอบว่าว่าสถานที่ ที่พนักงานทำงานอยู่ เช่นที่บ้าน มีความเหมาะสมในการปฏิบัติงาน โดยพิจารณาถึงสภาพแวดล้อมและความปลอดภัยจากการละเมิดข้อมูลส่วนบุคคลทางกายภาพทางเทคนิค

• ในการทำงานนอกสถานที่ พนักงานจะต้องใช้ความระมัดระวังเพื่อป้องกันทรัพย์สินต่างๆ ขององค์กรทั้ง Hardware และ Software จากการถูกขโมย การสูญหาย

• หากบริษัทกำหนดระเบียบปฏิบัติเกี่ยวกับการทำงานนอกสถานที่ ขึ้นเป็นการเฉพาะ จะต้องปฏิบัติตามรายละเอียดและเงื่อนไขของระเบียบดังกล่าวเพิ่มเติมด้วย

9. การละเมิดข้อมูลส่วนบุคคล (Personal Data Breaches)

• หากพนักงานหรือหน่วยงานหรือฝ่ายงานใดทราบถึงการละเมิดข้อมูลส่วนบุคคลของบริษัท จะต้องรายงานเหตุการณ์ที่เกิดขึ้นแก่ฝ่าย IT และ หัวหน้างานตามลำดับ โดยทันที ทั้งนี้ การรายงานดังกล่าวจะถูกเก็บเป็นความลับ

• เมื่อมีการแจ้งการละเมิดความปลอดภัย ฝ่ายงานที่เกี่ยวข้องจะดำเนินการตรวจสอบข้อเท็จจริง และดำเนินการขออนุมัติตามลำดับในการแจ้งเหตุละเมิดต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลตามเงื่อนไขที่กฎหมายกำหนด

• ในกรณีที่บริษัทมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ฝ่ายงานที่เกี่ยวข้องและฝ่าย IT ต้องแจ้งให้ DPO ทราบเพื่อเข้าร่วมการพิจารณาในการดำเนินการแจ้งเหตุละเมิดตามที่กฎหมายกำหนด

10. การปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Rights of data subject)

เนื่องจากเจ้าของข้อมูลส่วนบุคคลมีสิทธิดังที่บริษัทได้แจ้งให้เจ้าของข้อมูลรับทราบในนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy policy) เช่น

- สิทธิในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล
- สิทธิในการขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม
- สิทธิในการขอให้โอนย้ายข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น
- สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- สิทธิในการขอให้ลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

- สิทธิในการขอให้แก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์

ดังนั้น เมื่อปรากฏว่ามีเจ้าของข้อมูลร้องขอใช้สิทธิที่กฎหมายรับรองไว้ต่อบริษัท พนักงานหรือหน่วยงานหรือฝ่ายงานที่เกี่ยวข้อง ต้องบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล และรายละเอียดคำขอจากเจ้าของข้อมูล โดยต้องประกอบด้วยข้อมูลดังต่อไปนี้

- รายละเอียดของเจ้าของข้อมูลส่วนบุคคล
- รายละเอียดการขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- รายละเอียดของการดำเนินการ ซึ่งรวมถึงเหตุผลในกรณีที่มีการปฏิเสธการขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

เมื่อมีการขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคล พนักงานหรือหน่วยงานหรือฝ่ายงานจะต้องปฏิบัติตามกระบวนการการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดภายใต้ระเบียบและการพิจารณาอนุมัติตามขั้นตอนการบริหารจัดการของบริษัท หากการปฏิบัติตามคำขอจะต้องมีการประมวลผลหรือเข้าถึงข้อมูลส่วนบุคคล จะกระทำได้ภายใต้สิทธิการเข้าถึงตามตำแหน่งหน้าที่ซึ่งบริษัทกำหนดไว้ใน “IT policy” และต้องมีการขออนุมัติตามลำดับ

ในกรณีที่บริษัทมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หน่วยงานหรือฝ่ายงานที่ได้รับคำร้องขอใช้สิทธิจากเจ้าของข้อมูลต้องส่งเรื่องให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการ

11. การควบคุมหน่วยงานภายนอกที่มีการประมวลผลข้อมูลส่วนบุคคล (Controlling other parties involving the processing of personal data)

ในกรณีที่บริษัทส่งหรือโอนข้อมูลส่วนบุคคลในความควบคุมของบริษัทให้กับบุคคลหรือหน่วยงานภายนอกที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล หน่วยงาน ฝ่ายงาน ที่เกี่ยวข้องจะต้องมีการระบุรายละเอียดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในสัญญาระหว่างบริษัท และผู้ประมวลผลข้อมูลส่วนบุคคล โดยอย่างน้อยจะต้องครอบคลุมเนื้อหาดังต่อไปนี้

- ข้อตกลงการไม่เปิดเผยความลับของข้อมูล
- รายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
- คำสั่ง (Instruction) ของบริษัทในการประมวลผลข้อมูลส่วนบุคคล
- สิทธิของบริษัทฯ ในการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานภายนอก
- มาตรการการลบ ทำลาย หรือส่งคืนข้อมูลเมื่อสิ้นสุดระยะเวลาการประมวลผลข้อมูล
- การแจ้งต่อบริษัทเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

บริษัทอาจกำหนดรายละเอียดและเนื้อหาสัญญาที่แตกต่างกันไปให้เหมาะสมกับสภาพข้อเท็จจริงและการประมวลผลข้อมูลส่วนบุคคลเป็นรายกรณี

12. การวิเคราะห์ผลกระทบของข้อมูลส่วนบุคคล (Data Protection Impact Assessment)

- ในกรณีที่กฎหมายหรือประกาศคณะกรรมการกำหนดให้บริษัทต้องมีหน้าที่จัดทำการวิเคราะห์ผลกระทบของข้อมูลส่วนบุคคล (Data Protection Impact Assessment) บริษัทจะมอบหมายให้ฝ่าย IT และฝ่ายงานที่เกี่ยวข้องจัดทำขั้นตอนปฏิบัติในการวิเคราะห์ผลกระทบของข้อมูลส่วนบุคคล รวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหากมีการแต่งตั้ง โดยต้องมีการทบทวนขั้นตอนปฏิบัติอย่างสม่ำเสมอ
- ในกรณีที่มีการจัดทำการวิเคราะห์ผลกระทบของข้อมูลส่วนบุคคลแล้ว บริษัทจะทำการประเมินผลกระทบของข้อมูลส่วนบุคคล (Data Protection Impact Assessment) ร่วมกับสายงานกำกับดูแลกิจการ/DPO ก่อนริเริ่มดำเนินกิจกรรมทางธุรกิจ โครงการ หรือการกระทำอื่น ๆ ที่อาจก่อให้เกิดผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลของบริษัทภายใต้เงื่อนไขที่กฎหมายกำหนด

นโยบายนี้ประกาศใช้ควบคู่ไปกับ “IT Policy” โดยมุ่งเน้นการรักษาความปลอดภัยเฉพาะในส่วนของข้อมูลส่วนบุคคล สำหรับการรักษาความปลอดภัยของข้อมูลส่วนบุคคลในระบบสารสนเทศของบริษัทนอกเหนือจากที่ระบุในนโยบายนี้เป็นไปตาม “IT Policy”

นโยบายฉบับนี้มีผลบังคับใช้ในวันที่ 31 พฤษภาคม พ.ศ. 2565