รายงานการศึกษาส่วนบุคคล

(Individual Study)

เรื่อง แนวทางการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน

จัดทำโดย นางสาวมุทิตา ชูประดิษฐ์

รหัส 9970

รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม

หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 99

วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.

ประจำปี 2567

รายงานการศึกษาส่วนบุคคล

(Individual Study)

เรื่อง แนวทางการพัฒนาระบบติดตามและตรวจสอบ
การใช้ข้อมูลส่วนบุคคลของผู้ประกันตน

จัดทำโดย นางสาวมุทิตา ชูประดิษฐ์
รหัส 9970

หลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม รุ่นที่ 99
วิทยาลัยนักบริหาร สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.
ประจำปี 2567
รายงานนี้เป็นความคิดเห็นเฉพาะบุคคลของผู้ศึกษา

สำนักงาน ก.พ.

เอกสารรายงานการศึกษาส่วนบุคคลนี้ อนุมัติให้เป็นส่วนหนึ่งของการฝึกอบรมหลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรมสำนักงาน ก.พ.

นางสาวสุชาดา ไทยบรรเทา
อาจารย์ที่ปรึกษา

นางสาวบรรจงจิตต์ อังศุสิงห์
อาจารย์ที่ปรึกษา

นายจุฬา สุขมานพ
อาจารย์ที่ปรึกษา

บทสรุปสำหรับผู้บริหาร

รายงานการศึกษาส่วนบุคคล (Individual Study) เรื่อง “แนวทางการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน” มีวัตถุประสงค์เพื่อเสนอแนวทางพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อให้บริการแก่ผู้ประกันตน ต่อสำนักงานประกันสังคม ในประเด็นการจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกันตน เพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่กำหนดมาตรฐานให้หน่วยงานซึ่งมีหน้าที่จัดเก็บข้อมูลส่วนบุคคล จะต้องดำเนินการจัดการข้อมูลอย่างปลอดภัยเพื่อปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคล ทั้งยังกำหนดให้สิทธิแก่เจ้าของข้อมูลในการเข้าถึง แก้ไข ลบ หรือระงับข้อมูลตนเองได้ อย่างเป็นรูปธรรม

ในปัจจุบันมีข่าวภัยคุกคามจากการละเมิดข้อมูลส่วนบุคคลมากมาย กรณีการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ทางธุรกิจโดยไม่ได้รับอนุญาตอันเป็นการสร้างความเดือดร้อนรำคาญแก่เจ้าของข้อมูล หรือในบางกรณีเป็นเรื่องของมิจฉาชีพ ส่งผลร้ายแรงถึงขนาดทำให้เกิดการสูญเสียทรัพย์สิน เงินทอง ด้วยภารกิจของสำนักงานประกันสังคม ทำให้สำนักงานเป็นหน่วยงานหนึ่งในหลายหน่วยงานภาครัฐที่ได้จัดเก็บข้อมูลส่วนบุคคลไว้เป็นจำนวนมาก และข้อมูลดังกล่าวได้ถูกขอเชื่อมโยงเพื่อใช้ประโยชน์จากหน่วยงานภาครัฐภาคเอกชนอื่นๆหลายหน่วยงานด้วยกัน ในการปฏิบัติงานสำนักงานประกันสังคมมีการใช้งานระบบเทคโนโลยีสารสนเทศเป็นจำนวนมากเพื่อบริหารจัดการข้อมูล การรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศจึงถือเป็นหัวใจสำคัญ ในการดำเนินงานของสำนักงานประกันสังคม ที่จะละเลยไปไม่ได้ ด้วยความสำคัญของระบบสารสนเทศที่นับวันจะยิ่งเพิ่มสูงขึ้นและการโจมตีระบบสารสนเทศที่นับวันจะยิ่งซับซ้อนขึ้น ทำให้สำนักงานประกันสังคมมีความจำเป็นต้องใส่ใจทางด้านการรักษาความปลอดภัยสารสนเทศเพิ่มมากขึ้นตามไปด้วย เพื่อป้องกันไม่ให้ข้อมูลผู้ประกันตนของสำนักงานประกันสังคมถูกโจรกรรมโดยผู้ไม่ประสงค์ดี

ในปี พ.ศ.2565 ประเทศไทยได้มีการบังคับใช้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อันมีวัตถุประสงค์เพื่อปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยกฎหมายกำหนดหลักเกณฑ์กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อสร้างความมั่นใจให้แก่ประชาชนเรื่องข้อมูลส่วนบุคคลของที่มีผู้ได้รับไปนั้น ได้ทำการเก็บรักษา ใช้ เผยแพร่อย่างปลอดภัยและเหมาะสม รวมทั้งการแจ้งรายละเอียดของการเปิดเผยข้อมูลส่วนบุคคล ในภาคประชาชน และในส่วนของภาครัฐการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพและมีความทัดเทียมนานาอารยประเทศในด้านกฎหมาย อย่างชัดเจน นั้น แสดงให้เห็นถึงการมีธรรมาภิบาลในการด้านการคุ้มครองข้อมูลส่วนบุคคลที่โปร่งใสและตรวจสอบได้อีกด้วย

ดังนั้นนอกจากการที่สำนักงานประกันสังคมจะต้องปฏิบัติตามมาตรฐาน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ประกอบกับ สถิติการคุกคามทางไซเบอร์ ที่มีแนวโน้มเพิ่มขึ้น ในช่วงที่ผ่านมานับตั้งแต่ เดือนกันยายน ปี 2565 ถึงปัจจุบัน ศูนย์กลางเฝ้าระวัง และรับมือภัยคุกคามความปลอดภัยคอมพิวเตอร์ (SSO Security Operation Center) ได้ตรวจจับพบว่าสถิติภัยคุกคามความปลอดภัยมีแนวโน้มเพิ่มขึ้นเป็นลำดับ

ดังนั้น การพัฒนา “ระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน” เพื่อเป็นช่องทางให้บริการแก่ผู้ประกันตนซึ่งเป็นเจ้าของข้อมูลสามารถตรวจสอบการส่งหรือการเปิดเผยข้อมูลส่วนบุคคลของตน เห็นภาพรวมของการใช้ข้อมูลส่วนบุคคลของตนเอง และที่สำคัญสามารถบริหารจัดการข้อมูลของตนเองได้ในการให้ความยินยอมหรือไม่ให้ความยินยอมแก่สำนักงานประกันสังคมในการส่งข้อมูลให้แก่บุคคลที่ 3 ที่สำนักงานประกันสังคมได้เชื่อมโยงไปยังหน่วยงานภายนอกได้ ประโยชน์ที่ผู้ประกันตนจะได้รับจากแนวทางการพัฒนานี้ คือ ได้รับสิทธิการจัดการข้อมูลส่วนบุคคลอย่างสมบูรณ์ตามที่กฎหมายกำหนด และในระยะยาวเพื่อประโยชน์สูงสุดในการรับบริการของผู้ประกันตนภายใต้ความยินยอมของเจ้าของข้อมูล สำนักงานประกันสังคมสามารถพัฒนาระบบเชื่อมโยงข้อมูลให้เชื่อมโยงกับภาคธุรกิจที่มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคล เช่น การยื่นขอกู้เงินต่อสถาบันทางการเงิน ของสถาบันทางการเงินหากมีความจำเป็นต้องใช้หลักฐานข้อมูลความมั่งคงทางการเงิน ทางด้านสุขภาพ ทางครอบครัว ก็จะสามารถตรวจสอบได้ภายใต้ความยินยอมของเจ้าของข้อมูล ลดระยะเวลาการรอคอยการอนุมัติเงินกู้เช่นในปัจจุบัน ตลอดจนเชื่อมั่นว่า สถิติการคุกคามทางไซเบอร์น่าจะลดลงเนื่องจากธุรกิจเอกชนสามารถเชื่อมโยงข้อมูลได้โดยตรงกับหน่วยงานที่มีข้อมูลภายใต้ความยินยอมของเจ้าของข้อมูล ก็จะลดความเดือดร้อนรำคาญจากการได้รับโทรศัพท์เสนอขายสินค้าจากภาคเอกชน และสุดท้ายสำนักงานประกันสังคมก็จะเป็นหน่วยงานอันมีธรรมาภิบาลที่ดี มีภาพลักษณ์ที่โปร่งใสเป็นที่น่าเชื่อถือของผู้ประกันตนผู้รับบริการ

เพื่อให้บรรลุข้อเสนอ แนวทางการพัฒนา “ระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน” จึงกำหนดรูปแบบของระบบหลักดังกล่าวให้ประกอบไปด้วยระบบย่อย ในเรื่อง ระบบการจัดเก็บข้อมูล ระบบประมวลผลข้อมูล ระบบเซิร์ฟเวอร์ ระบบแสดงผล ระบบบันทึกการกระทำ (Audit Logging) ระบบการตรวจจับการละเมิด ระบบรักษาความปลอดภัย ระบบการตรวจสอบการเข้าถึงข้อมูล และระบบการยืนยันตัวตน เพื่อแสดงผลการให้บริการแก่ผู้ประกันตน ในการเข้าถึงข้อมูลส่วนบุคคล สามารถทำการเปลี่ยนแปลงข้อมูล และตรวจสอบการนำใช้ข้อมูลส่วนบุคคลไปใช้ รวมทั้งสามารถใช้สิทธิ์อนุญาตหรือไม่อนุญาตให้ใช้ข้อมูลแก่บุคคลภายนอกได้ และผู้ศึกษาคาดว่า สำนักงานประกันสังคมสามารถนำไปใช้เป็นแนวทางการดำเนินงานและบรรลุเป้าหมายในการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกันตนได้อย่างมีประสิทธิภาพ

กิตติกรรมประกาศ

รายงานการศึกษาส่วนบุคคล (Individual Study) เรื่อง “แนวทางการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน” มีวัตถุประสงค์เพื่อเสนอแนวทางพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อให้บริการแก่ผู้ประกันตนของสำนักงานประกันสังคม ในประเด็นการจัดการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกันตนให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่กำหนดมาตรฐานให้หน่วยงานซึ่งมีหน้าที่จัดเก็บข้อมูลส่วนบุคคล จะต้องดำเนินการจัดการข้อมูลอย่างปลอดภัยเพื่อปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคล ทั้งยังกำหนดให้สิทธิแก่เจ้าของข้อมูลในการเข้าถึง แก้ไข ลบ หรือระงับข้อมูลตนเองได้ ซึ่งเป็นส่วนหนึ่งของการอบรมหลักสูตรนักบริหารระดับสูง : ผู้นำที่มีวิสัยทัศน์และคุณธรรม (นบส.1) รุ่นที่ 99 รายงานการศึกษาส่วนบุคคลฉบับนี้สำเร็จลุล่วงได้ด้วยความอนุเคราะห์จากท่านอาจารย์สุชาดา ไทยบรรเทา อาจารย์ที่ปรึกษาหลัก ท่านอาจารย์บรรจงจิตต์ อังศุสิงห์ และท่านอาจารย์จุฬา สุขมานพ อาจารย์ที่ปรึกษาร่วม ซึ่งท่านอาจารย์ที่ปรึกษามีความมุ่งมั่น เสียสละเวลา ในการให้คำปรึกษาแนะนำและให้แนวคิดในการจัดทำรายงาน ตลอดจนตรวจสอบ ปรับแก้ไขจนทำให้รายงานการศึกษาส่วนบุคคลฉบับนี้มีความครบถ้วนสมบูรณ์ ท่านรองจีระภา บุญรัตน์ รองเลขาธิการสำนักงานประกันสังคม ผู้บังคับบัญชาที่เป็นผู้ให้คำปรึกษาอย่างเชี่ยวชาญในการจัดทำรายงานการศึกษา ผู้ศึกษาจึงขอกราบขอบพระคุณท่านอาจารย์ที่ปรึกษาทั้ง 3 ท่านและท่านรองเลขาธิการสำนักงานประกันสังคม เป็นอย่างสูง

สุดท้ายนี้ขอกราบขอบพระคุณท่านเลขาธิการสำนักงานประกันสังคม (นายบุญสงค์ ทัพชัยยุทธ์) สำนักงานประกันสังคม ผู้บังคับบัญชาที่ให้โอกาสผู้ศึกษาได้รับเข้าการอบรมในครั้งนี้ ทำให้ผู้ศึกษาได้รับ การเพิ่มพูนความรู้ พัฒนาทักษะด้านต่างๆ ซึ่งผู้ศึกษาจะพัฒนาตนเอง พัฒนางาน เพื่อนำพาองค์กรบรรลุตามเป้าหมายได้อย่างมีประสิทธิภาพดียิ่งขึ้นต่อไป

นางสาวมุทิตา ชูประดิษฐ์

30 เมษายน 2567

สารบัญ

สารบัญตาราง

สารบัญภาพ

1. วิสัยทัศน์ของตำแหน่งเป้าหมาย

(ข้อมูลส่วนบุคคลไม่เผยแพร่)

และการมอบบริการที่ให้ความสำคัญกับรายละเอียดและความเป็นไปได้ บริการที่เป็นเลิศมักจะช่วยสร้างความประทับใจให้กับลูกค้า สร้างความเชื่อมั่นให้กับลูกค้า และสร้างฐานลูกค้าที่เชื่อถือได้ในระยะยาว

กล่าวโดยสรุปได้ว่า เมื่อได้รับการแต่งตั้งในตำแหน่งรองเลขาธิการสำนักงานประกันสังคม ผู้ศึกษามุ่งมั่นที่จะปฏิบัติงานไปสู่เป้าหมายในการผลักดันให้สำนักงานประกันสังคมมีระบบเทคโนโลยีสารสนเทศเพื่อให้บริการด้านงานประกันสังคมที่มีประสิทธิภาพโดยใช้การประมวลผลข้อมูลและข้อมูลจากระบบเทคโนโลยีสารสนเทศ เช่น ปัญญาประดิษฐ์ (Artificial Intelligence) หรือการเรียนรู้ของเครื่องคอมพิวเตอร์ (Machine Learning) ในการวิเคราะห์ข้อมูล และในขณะเดียวกันมุ่งมั่นพัฒนาเจ้าหน้าที่สำนักงานประกันสังคม ให้มีทักษะการให้บริการที่มีคุณภาพและมีความเอื้ออำนวยต่อผู้รับบริการอย่างดีเยี่ยม เพื่อให้ผู้ประกันตนและผู้ใช้บริการได้รับความพึงพอใจ

2 ข้อเสนอเพื่อขับเคลื่อนนโยบายสู่การปฏิบัติ

2.1 การกำหนดประเด็นการศึกษา

หัวข้อการศึกษา “แนวทางการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน”

ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลใด ๆ ที่สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าจะเป็นทางตรงหรือทางอ้อมก็ตาม ตัวอย่าง เช่น ชื่อ-นามสกุล เลขประจำตัวประชาชน เลขที่หนังสือเดินทาง เลขที่บัตรประกันสังคม เลขที่ใบอนุญาตขับขี่ เลขที่ประจำตัวผู้เสียภาษี เลขที่บัญชีธนาคาร เลขที่บัตรเครดิต ที่อยู่ อีเมล์แอดเดรส เลขหมายโทรศัพท์ วันเกิดและสถานที่เกิด เชื้อชาติ สัญชาติ น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งที่อยู่ (location) ข้อมูลการแพทย์ ข้อมูลการศึกษา ข้อมูลทางการเงิน ข้อมูลการจ้างงาน ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address MAC address Cookie ID ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน หรือข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้

การละเมิดข้อมูลส่วนบุคคล หมายถึง เหตุการณ์ หรือการกระทำที่นำไปสู่การเก็บรวบรวม เข้าถึง สูญหาย ทำลาย เปลี่ยนแปลง หรือเปิดเผยโดยไม่ได้รับอนุญาต ไม่ว่าจะเป็นการเจตนา หรือเกิดความผิดพลาดโดยไม่ตั้งใจ เช่น สถาบันการเงินส่งไปใบแจ้งหนี้ไปผิดคน โรงพยาบาลส่งผลตรวจสุขภาพไปผิดบ้าน หน่วยงานโดนโจมตีทางไซเบอร์ ศูนย์ข้อมูลทำงานผิดพลาดจนทำให้ข้อมูลเสียหาย หรือถูกโจรกรรม การส่งต่อข้อมูลหรือแชร์โดยเจ้าของข้อมูลไม่อนุญาต พนักงานในองค์กรขโมยข้อมูลลูกค้าไปขายหรือใช้ประโยชน์ส่วนตัว ซึ่ง ข้อมูลส่วนบุคคลที่เกิดการรั่วไหลหรือละเมิดอาจจะมีผลที่ตามมา เช่น การทำให้เจ้าของข้อมูลมีความเสี่ยงทั้งความเสี่ยงต่อทางร่างกาย สุขภาพจิต ชื่อเสียง ทรัพย์สิน เสียโอกาส ถูกปฏิบัติที่ไม่เป็นธรรม หรือผลกระทบในด้านลบต่างๆ อันเป็นผลจากการถูกเปิดเผยข้อมูลส่วนบุคคล

สำนักงานประกันสังคมมีภารกิจหลักในการบริหารงานกองทุนประกันสังคมโดยการจัดเก็บเงินสมทบจากนายจ้างและผู้ประกันตน ในอัตราที่เท่ากันคือร้อยละ 5 ของค่าจ้างตามความเป็นจริง โดยต้องไม่ต่ำกว่า เพดานขั้นต่ำของค่าจ้าง ที่พระราชบัญญัติประกันสังคม พ.ศ.2533 กำหนด คือ 1,650 บาท และขั้นสูง 15,000 บาท การจัดเก็บเงินสมทบเข้ากองทุนประกันสังคมก็เพื่อนำไปบริหารจัดการจ่ายสิทธิประโยชน์ให้แก่ผู้ประกันตนเพื่อให้ผู้ประกันตนซึ่งเป็นแรงงานมีหลักประกันการดำรงชีวิตที่มั่นคง ด้วยภารกิจที่ต้องบริหารจัดเก็บเงินและจัดการจ่ายสิทธิประโยชน์ให้ถูกต้องสำนักงานประกันสังคมจึงต้องทำการจัดเก็บข้อมูลส่วนบุคคลของผู้ประกันตน อาทิเช่น ชื่อ นามสกุล เลขประจำตัวประชาชน เพศ อายุ ข้อมูลการทำงาน รายได้ ข้อมูลเงินสะสมชราภาพ ข้อมูลการเบิกจ่ายสิทธิประโยชน์ ข้อมูลการเลือกโรงพยาบาลตามสิทธิประกันสังคม ข้อมูลสุขภาพส่วนบุคคล และอื่นๆ ล้วนแต่เป็นคลังข้อมูล ที่เป็นประโยชน์ ต่อภาครัฐและภาคเอกชน ภายใต้บริบทสังคมปัจจุบันที่เป็นยุคแห่งข้อมูลข่าวสาร สำนักงานประกันสังคมจึงเป็นหน่วยงานหนึ่งในหลายหน่วยงานที่ได้จัดเก็บข้อมูลส่วนบุคคลไว้เป็นจำนวนมาก และข้อมูลดังกล่าวได้ถูกขอเชื่อมโยงเพื่อใช้ประโยชน์จากหน่วยงานภาครัฐอื่นๆหลายหน่วยงานด้วยกันภายใต้อำนาจของกฎหมายที่ให้อำนาจหน่วยงานนั้นๆ และด้วยความจำเป็นของสำนักงานเองในการต้องเชื่อมโยงข้อมูลกับภาคเอกชน เช่น ธนาคาร หน่วยงานผู้ให้บริการทางด้านการเงิน หรือ โรงพยาบาล เพื่อให้ผู้ประกันตนได้รับบริการที่มีประสิทธิภาพ แต่สำนักงานประกันสังคมพบว่ามีผู้ประกันตนในบางส่วนได้รับผลกระทบจากการรั่วไหลของข้อมูลส่วนบุคคล ซึ่งไม่แน่ชัดว่าเป็นการรั่วไหลจากหน่วยปฏิบัติไม่ว่าภาครัฐหรือเอกชนใดที่อาจมีข้อมูลเช่นเดียวกัน

สำนักงานประกันสังคมได้บริหารจัดการข้อมูลภายใต้กฎหมายพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 ขณะเดียวกันในปี พ.ศ. 2562 ภาครัฐได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 ขึ้นโดยกำหนดหลักเกณฑ์กลไกหรือมาตรการกำกับดูแลการให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นการกำหนดมาตรฐานใหม่ในเรื่องการให้ความคุ้มครองส่วนบุคคลของประเทศไทยให้เทียบเท่ากับสากล สำนักงานประกันสังคมเป็นหน่วยงานหนึ่งที่เร่งพัฒนาคุ้มครองข้อมูลส่วนบุคคลของผู้ประกันตน นายจ้างให้สอดรับหลักกฎหมายดังกล่าว โดยพัฒนาระบบการจัดการข้อมูลส่วนบุคคลให้สามารถทำการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล การจัดการความยินยอมของเจ้าของข้อมูล การจัดการใช้สิทธิ์ของเจ้าของข้อมูลส่วนบุคคล และการจัดการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย ดังกล่าว แต่ด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้อย่างละเอียด เช่น เจ้าของข้อมูลมีสิทธิ์คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ ดังนั้นหากหน่วยงานที่จัดเก็บข้อมูลที่มีความสำคัญเช่นสำนักงานประกันสังคมสามารถที่จะพัฒนาระบบสารสนเทศ ให้เจ้าของข้อมูลสามารถที่จะทราบได้ว่า ข้อมูลส่วนบุคคล ได้ถูกนำไปใช้โดยหน่วยงานใด เมื่อใด และเพื่อวัตถุประสงค์ใด ก็จะส่งผลให้เกิดประโยชน์แก่ผู้ประกันตนซึ่งเป็นเจ้าของข้อมูลและส่งผล ถึงความเชื่อมั่นที่ ผู้ประกันตนมีต่อสำนักงานประกันสังคม กระทรวงแรงงานตลอดจนเพิ่มความเชื่อมั่นและไว้วางใจของประชาชนที่มีต่อภาครัฐ

2.1.1 ปัญหา ความท้าทาย

บริบทสังคมปัจจุบันพบว่ามีภัยคุกคามจากการละเมิดข้อมูลส่วนบุคคล ซึ่งตกเป็นข่าวมากมาย ที่ได้พบบ่อยครั้งและบางครั้งเกิดขึ้นกับตัวเราเองหรือคนใกล้ชิด กรณีการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ทางธุรกิจโดยไม่ได้รับอนุญาตอันเป็นการสร้างความเดือดร้อนรำคาญแก่เจ้าของข้อมูล หรือในบางกรณีส่งผลร้ายแรงถึงขนาดทำให้เกิดการสูญเสียทรัพย์สิน เงินทอง ดังเช่นข่าวต่อไปนี้

“แฉกลยุทธ์ใหม่! แก๊งคอลเซ็นเตอร์ หลอกคุย 2 นาที ดูดเงินได้เกลี้ยงบัญชี”

วันที่ 12 ก.พ. 2567 นายเอ นามสมมุติ อายุ 23 ปี เป็นหนึ่งในแก๊งคอลเซ็นเตอร์ คนไทยที่ถูกหลอกไปทำงานที่เมืองปอยเปต กัมพูชา ได้เข้าให้ข้อมูลกับเพจสายไหมต้องรอด หลังหาทางหลบหนีออกมาได้ โดยเขาระบุว่าเดินทางไปทำงาน เมื่อวันที่ 1 ม.ค.2567 ในภูริคาสิโน ซึ่งเขาอ้างว่า ถูกหลอกให้ทำงานโดยการโทรกลับมาหลอกคนไทย เพื่อดูดเงิน ภายหลังได้พยายามหาทางหลบหนีออกมา เมื่อวันที่ 4 ก.พ.ที่ผ่านมาพอหนีรอดพ้นก็เข้ามาที่เพจสายไหมต้องรอดเพื่อที่จะให้ข้อมูล และเตือนประชาชนคนไทยทุกคน นายเอ เล่าให้ฟังว่า แก๊งคอลเซ็นเตอร์ที่ตนไปทำงานนั้น มีเทคโนโลยีที่ล้ำสมัยมากมีเครื่องดูดเงินจำนวน 4 เครื่อง เป็นเครื่องที่มีมูลค่า มากกว่า 120 ล้านบาท ซึ่งแก๊งคอลเซ็นเตอร์แก๊งนี้เจ้าของเป็นคนจีน ได้ซื้อข้อมูลจากธนาคารรัฐแห่งหนึ่งในประเทศไทย และค่ายมือถือค่ายหนึ่ง ซึ่งตนเป็นคนที่เห็นข้อมูลของคนไทย พบว่าส่วนใหญ่ข้อมูลที่ถูกขายมาจะเป็นกลุ่ม ข้าราชการชั้นผู้ใหญ่ที่มีเงินในบัญชีหมุนเวียน อย่างต่ำ 60 ล้านบาท โดยนายเอ ยังอธิบายว่า ตนจะได้รับหน้าที่ในการโทรไปหาเหยื่อ ซึ่งเป็นข้าราชการหรือคนที่มีเงิน เป็นกลุ่มเป้าหมายอยู่แล้ว จากนั้นก็จะให้เหยื่อยืนยันหมายเลขบัตรประชาชนว่าใช่หรือไม่ เพราะข้อมูลบัตรประชาชนจะถูกโยงกับข้อมูลธนาคาร โดยที่ตนเองนั้นจะบอกเหยื่อว่าเป็นเจ้าหน้าที่หน่วยงานใดหน่วยงานหนึ่ง โทรมาตรวจสอบข้อมูล ให้เหยื่อบอกข้อมูล ยืนยันตัวตน ใช้เวลาคุย 1 - 2 นาที เพื่อให้เครื่องสามารถดูดข้อมูลของเหยื่อได้ หลังจากนั้นเงินของเหยื่อก็จะหายไปเกลี้ยงบัญชี หลังจากเงินของเหยื่อหายแล้วก็จะโทรกลับมาอีก เราก็จะเรียกเงินประกัน เพื่อให้เงินคืนก็จะทำให้ได้รับเงินอีก แต่ละวันสามารถดูดเงินคนไทย ได้ถึง 150 ล้านบาท

“เผย 7 ช่องทางสำรวจแก๊งมิจฉาชีพอย่าง Call Center เอาเบอร์โทรศัพท์ของคุณมาจากไหน พร้อมแนวทางป้องกัน”

คุณเป็นหนึ่งคนที่โดนแก๊งคอลเซ็นเตอร์โทรกวนใจใช่หรือไม่ แล้วคุณเคยสงสัยบ้างไหมว่าแก๊งคอลเซ็นเตอร์เอาเบอร์โทรของคุณมาจากที่ไหน นี่เป็นคำถามที่หลายคนก็ต่างตั้งข้อสงสัยอยู่ไม่น้อยเลยทีเดียว เมื่อแก๊งต้มตุ๋นที่มาในรูปแบบของการโทรขอข้อมูลกลับมาระบาดอีกครั้งในปี 2565 บ้างก็อ้างว่าคุณมีพัสดุที่ยังไม่ได้รับ บ้างก็อ้างว่าคุณมียอดบัตรเครดิตที่ยังไม่ชำระ หรือแม้กระทั่งว่ามีการปล่อยเงินกู้ดอกเบี้ยถูก ซึ่งข้ออ้างเหล่านี้ได้สร้างความรำคาญใจ สร้างปัญหาและสร้างมูลค่าความเสียหายอย่างมหาศาล ส่งผลให้ยอดผู้เสียหายสูงถึง 270% เมื่อเทียบกับปี 2564 แต่ทว่าการหลอกลวงแบบแก๊งคอลเซ็นเตอร์นั้นเป็นเพียงรูปแบบหนึ่งที่ใช้ในการโจรกรรมข้อมูลของมิจฉาชีพเท่านั้น ไม่ใช่แค่เบอร์โทรศัพท์ที่แก๊งมิจฉาชีพนี้ต้องการ แต่ยังรวมถึงข้อมูลส่วนตัวอีกมากมาย เช่น ชื่อ นามสกุล เลขประจำตัวประชาชน และเลขบัตรเครดิต ที่ซึ่งการโทรไปหลอกนั้นจะ

สามารถเป็นประตูเปิดทางให้แก๊งมิจฉาชีพล้วงข้อมูลเหล่านี้ไปได้ ดังนั้นเพื่อเป็นการปกป้องข้อมูลส่วนตัวของคุณ คุณจึงควรกลับไปแก้ไขที่ต้นตอ ลองสำรวจว่าคุณเคยเปิดเผยข้อมูลส่วนตัวที่ไหนบ้าง แล้วแก๊งคอลเซ็นเตอร์ได้ข้อมูลของคุณมาอย่างไร

7 ข้อสำรวจแก๊ง Call Center เอาเบอร์โทรศัพท์ของคุณมาจากไหน

(1) จากเว็บไซต์สมัครงาน เว็บสมัครงานถือเป็นแหล่งข้อมูลชั้นดีของแก๊งคอลเซ็นเตอร์เลยก็ว่าได้ เพราะหลาย ๆ คนได้ลงข้อมูลส่วนตัวไว้ในโปรไฟล์ก็ดี บน Resume ก็ดี โดยที่จะใช้ข้อมูลนั้นในการสมัครงานและหวังว่านั่นจะเป็นช่องทางที่คุณจะได้รับการติดต่อกลับนั่นเอง แต่ว่าคุณเองก็คงลืมเอะใจไปว่าชื่อ นามสกุล เบอร์โทร อีเมล และที่อยู่ของคุณก็ต่างเป็นที่หมายปองของแก๊งมิจฉาชีพอย่างเช่นแก๊งคอลเซ็นเตอร์ หรือแม้กระทั่งแก๊งโทรขายตรงหรือโทรขายฝันก็รวมอยู่ในเว็บไซต์รับสมัครงานกันไม่น้อยเลยทีเดียว

(2) จาก Social Media ส่วนตัว Social Media ช่องทางยอดฮิตอีกช่องทางหนึ่งที่คุณอาจจะเปิดเผยข้อมูลโดยไม่รู้ตัวว่ามิจฉาชีพก็สามารถนำข้อมูลจากช่องทางนี้ไปใช้ได้เช่นกัน ลองกลับไปเช็คที่โปรไฟล์ของคุณดูว่าคุณได้ใส่เบอร์โทรหรืออีเมลไว้หรือไม่ เพราะจริง ๆ แล้วแค่มีข้อมูล 2 อย่างนี้ แก๊งมิจฉาชีพก็สามารถเอามาทำอะไรได้หลายอย่าง เช่น การโทรหลอกเอาข้อมูลหรือที่หลายคนเรียกว่าแก๊งคอลเซ็นเตอร์และการล้วงข้อมูลทางอีเมลแบบ Phishing หากใครที่มีข้อมูลเหล่านี้อยู่บนโปรโฟล์ ก็แนะนำว่าอย่าใส่จะดีกว่า ไม่ว่าจะเป็น Facebook, Instagram, YouTube หรือ TikTok ก็ควรเก็บข้อมูลส่วนตัวไว้เป็นความลับ

(3) จากการคลิกลิงก์ คุณเคยเจอบ้างไหมลิงก์แปลก ๆ ที่ถูกส่งมาในข้อความโดยมีคำพูดที่เย้ายวนใจราวกับว่าเขาอ่านความคิดคุณออก ซึ่งยากที่จะหักห้ามใจไม่กดเข้าไปเหลือเกิน หารู้ไม่ว่าเพียงแค่คุณคลิกเข้าไปแค่ครั้งเดียวแก๊งต้มตุ๋นก็สามารถล้วงความลับของคุณได้แล้วง่าย ๆ หรืออีกรูปแบบหนึ่งคือการตอบคอมเมนต์โดยการแนบลิงก์ลงบน Social Media ซึ่งหากคุณเผลอคลิกเข้าไป ลิงก์นั้นสามารถนำคุณไปยังอีกเว็บไซต์หนึ่งที่ดูไม่น่าเชื่อถือได้ทันที

(4) จากการกรอกแบบฟอร์ม หากคุณเป็นหนึ่งคนที่ให้ความสนใจกับกิจกรรมออนไลน์เป็นพิเศษ คุณคือหนึ่งในเป้าหมายของแก๊งนี้ ซึ่งการหลอกลวงเช่นนี้ยังไม่เป็นที่แพร่หลายนัก แต่อย่างไรก็ตามป้องกันไว้ก่อนดีกว่าตามแก้ทีหลัง โดยการทำงานของแก๊งนี้จะมาในรูปแบบของการประชาสัมพันธ์โปรโมชันต่าง ๆ เช่น การเปิดจองสินค้าใหม่หรือการเปิดแบบฟอร์มกรอกใบสมัครงานที่ซึ่งทำให้คุณนั้นหลงกลใส่ข้อมูลส่วนตัวด้วยความเต็มใจนั่นเอง

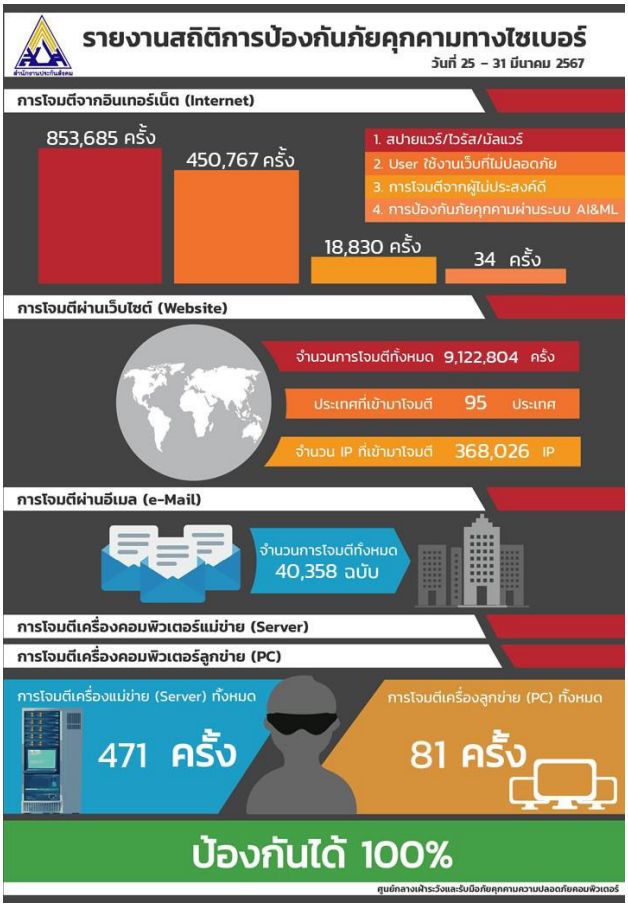
(5) จากการตกลงยินยอมสมัครใช้บริการบางอย่าง สาเหตุนี้มักจะเกิดจากการดาวน์โหลดแอปพลิเคชันบางอย่างแล้วคุณนั้นต้องกดยินยอมเพื่ออนุญาตให้เขาเก็บข้อมูลส่วนตัวของคุณไว้ได้ แต่ทว่าคุณจะตกลงยินยอมให้ทางผู้ให้บริการนำข้อมูลของคุณไปขายหรือใช้เชิงพาณิชย์จริง ๆ หรอ? หยุดพิจารณาสักนิดเพื่อปกป้องสิทธิ์ของคุณกันเถอะ เพราะคุณไม่รู้ว่าแอปที่คุณดาวน์โหลดปลอดภัยหรือไม่ มาจากบริษัทที่น่าเชื่อถือหรือไม่ ซึ่งถ้าหากเขามีข้อมูลคุณอยู่ในมือแล้วเขาก็สามารถนำข้อมูลไปขายได้ง่าย ๆ

(6) จากการแฮกอีเมล หลายคนคงคุ้นหน้าคุ้นตากันดีกับการโดนหลอกแฮกข้อมูลจากทางอีเมล เมื่อคุณเปิดอีเมลหรือคลิกลิงก์ที่แนบอยู่เพียงเท่านั้น ทั้ง Phishing และ Malware ก็แย่งกันเข้ามาหาคุณโดยทันที ทั้งปล่อยไวรัสเข้าอุปกรณ์ของคุณ ทั้งล้วงข้อมูลส่วนตัวมากมายที่ไม่ใช่แค่เบอร์โทร แต่ยังสามารถล้วงไปถึงข้อมูลบัตรประชาชนและข้อมูลบัตรเครดิตที่ซึ่งนับว่าเจ้าข้อมูลพวกนี้แหละเป็นทุกสิ่งทุกอย่างของคุณเลยก็ว่าได้ เนื่องจากหลายคนใช้อีเมลในการทำธุรกรรมต่าง ๆ บนโลกออนไลน์ไม่ว่าจะเป็นการชำระค่าบริการหรือการสมัครใช้งานใด ๆ คุณล้วนแต่ต้องกรอกข้อมูลด้วยการเชื่อมกับอีเมลทั้งนั้น ดังนั้นหากไม่อยากโดนหลอกครั้งใหญ่ก็ควรป้องกันไว้ก่อนไม่ว่าจะทางใดก็ตาม

(7) จากการแฮกข้อมูลองค์กรที่คุณทำงานอยู่ ข้อสุดท้ายนี้จะขอพูดถึงการถูกล้วงข้อมูลหรือการเปิดเผยข้อมูลพนักงานในองค์กรกันบ้าง ซึ่งปัญหานี้ถือเป็นปัญหาใหญ่และทุกบริษัทควรให้ความสำคัญอย่างมาก เพราะหากบริษัทไม่มีนโยบายหรือระบบรักษาความปลอดภัยของข้อมูล (Data Loss Prevention) ที่เพียงพอ ไม่สามารถเก็บข้อมูลส่วนตัวของพนักงานไว้เป็นความลับได้ เป็นเหตุให้ข้อมูลพนักงานถูกเปิดเผยไปต่อสาธารณะหรือตกไปสู่มือของมิจฉาชีพได้ง่าย ซึ่งองค์กรจะได้รับโทษทางกฎหมายตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลหรือ Personal Data Protection Act (PDPA)

จากการศึกษา ข้อมูลของ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ซึ่งเป็นหน่วยงานภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ณ วันที่ 8 พฤศจิกายน 2566 พบเหตุละเมิดข้อมูลส่วนบุคคลถึง 416 เรื่อง โดยแบ่งเป็นเรื่องที่ได้รับแจ้ง 224 เรื่อง และเรื่องที่ศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล PDPC Eagle Eye ตรวจพบ 192 เรื่อง และ ข้อมูล ณ วันที่ 9 พฤศจิกายน 2566 – 12 มกราคม 2567 สามารถแบ่งเหตุการณ์การละเมิดข้อมูลส่วนบุคคลออกตามประเภทธุรกิจ เป็น ธุรกิจการเงินและการธนาคารเป็นกลุ่มธุรกิจที่มีการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลมากที่สุด รองลงมาเป็นหน่วยงานภาครัฐ และรัฐวิสาหกิจ สาเหตุหลักของการละเมิดข้อมูลส่วนบุคคลนั้นเกิดจากข้อมูลรั่วไหล รองลงมาเป็นความผิดพลาดของบุคลากรในองค์กร และ Google Hack ขณะที่การเฝ้าระวังโดยศูนย์ PDPC Eagle Eye มีการตรวจพบว่าหน่วยงานภาครัฐและรัฐวิสาหกิจ ถูกละเมิดข้อมูลส่วนบุคคลมากที่สุด ด้วยวิธีการ Google Hack

ด้วยสำนักงานประกันสังคมเป็นหน่วยงานหนึ่งในหลายหน่วยงานของภาครัฐที่มีฐานข้อมูลส่วนบุคคลเป็นจำนวนมาก ศูนย์กลางเฝ้าระวังและรับมือภัยคุกคามความปลอดภัยคอมพิวเตอร์ (SSO Security Operation Center) ของสำนักงานประกันสังคม จัดเก็บข้อมูลสถิติภัยคุกคามในเรื่องความมั่นคงคอมพิวเตอร์ของสำนักงานประกันสังคม พบว่าโดยเฉลี่ยในแต่ละสัปดาห์ ยกตัวอย่าง ช่วงเวลา 25 – 31 มีนาคม 2567 มีการโจมตีจากอินเทอร์เน็ต 853,685 ครั้ง การโจมตีผ่านเว็บไซต์ 9,122,804 ครั้ง ตรวจพบการโจมตีจำนวน 368,026 IP และมาจาก 95 ประเทศ การโจมตีผ่านอีเมล 40,358 ครั้ง การโจมตีเครื่องแม่ข่าย 471 ครั้ง การโจมตีเครื่องลูกข่าย 81 ครั้ง



(แหล่งที่มา ข้อมูลจาก สำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม พ.ศ.2567)

สำนักงานประกันสังคมมีภารกิจในการให้บริการจ่ายสิทธิประโยชน์ให้แก่ผู้ประกันตน เพื่อให้เกิดประสิทธิภาพในการดำเนินงาน จึงมีความจำเป็นต้องทำการเชื่อมโยงข้อมูลกับหน่วยงานภายนอก ทั้งภาครัฐและเอกชน ดังนี้

ข้อมูลหน่วยงานที่ตกลงเชื่อมโยงข้อมูลกับสำนักงานประกันสังคม		
หน่วยงาน	**จำนวน (หน่วยงาน)**	**ภาพรวมประเภทข้อมูลที่เชื่อมโยง**
ภาครัฐ	17	ข้อมูลผู้ประกันตน ข้อมูลรายได้ ข้อมูลสถานที่ทำงาน ข้อมูลประวัติการจ้างงาน ข้อมูลนายจ้าง ฐานว่าจ้าง การเลือกสถานพยาบาล จำนวนผู้ใช้สิทธิประโยชน์ 7 กรณี

ข้อมูลหน่วยงานที่ตกลงเชื่อมโยงข้อมูลกับสำนักงานประกันสังคม		
หน่วยงาน	**จำนวน (หน่วยงาน)**	**ภาพรวมประเภทข้อมูลที่เชื่อมโยง**
สถาบันการเงิน	19	ข้อมูลการรับเงินกองทุนประกันสังคมผ่านธนาคารข้อมูลการจ่ายเงินประโยชน์ทดแทนกรณีสงเคราะห์บุตรทางธนาคาร ข้อมูลจ่ายเงินประโยชน์ทดแทนกรณีบำนาญชราภาพผ่านธนาคาร
สถานพยาบาล	14,849	ข้อมูลผู้ประกันตน ข้อมูลการรักษาพยาบาล
รวม	14,885	-

(แหล่งที่มา ข้อมูลจาก สำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม พ.ศ.2567)

จากปัญหาการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นในสังคมปัจจุบัน ไม่ว่าจะเป็นลักษณะการนำข้อมูลส่วนบุคคลไปใช้ประมวลผล หรือเปิดเผย หรือกระทำการใด ๆ ที่ทำให้เจ้าของข้อมูลส่วนบุคคล ได้รับความเสียหาย ไม่ว่าจะเป็นด้านความปลอดภัยต่อชีวิต ร่างกาย สิทธิเสรีภาพ หรือการนำข้อมูลไปใช้ ประโยชน์ทางธุรกิจโดยไม่ได้รับอนุญาตอันเป็นการสร้างความเดือดร้อนรำคาญแก่เจ้าของข้อมูล สำนักงานประกันสังคมในฐานะที่เป็นผู้ควบคุมฐานข้อมูลส่วนบุคคลเป็นจำนวนมาก

นอกเหนือจากการพัฒนาระบบเฝ้าระวังเพื่อป้องกันการถูกโจมตีทางไซเบอร์ การถูกโจรกรรมข้อมูลที่ถือครองแล้วนั้น สำนักงานก็ควรที่จะพัฒนาระบบสารสนเทศ ให้เจ้าของข้อมูลสามารถที่จะทราบได้ว่าข้อมูลส่วนบุคคล ได้ถูกนำไปใช้โดยหน่วยงานใด เมื่อใด และเพื่อวัตถุประสงค์ใด ก็จะส่งผลให้เกิดประโยชน์แก่ผู้ประกันตนซึ่งเป็นเจ้าของข้อมูลและส่งผล
ถึงความเชื่อมั่นที่ ผู้ประกันตนมีต่อสำนักงานประกันสังคม กระทรวงแรงงานตลอดจนเพิ่มความเชื่อมั่นและไว้วางใจของประชาชน ต่อภาครัฐ

2.1.2 แนวโน้มของปัญหาในอนาคต และผลกระทบที่เกิดขึ้น

ปัจจุบันสำนักงานประกันสังคมมีการใช้งานระบบเทคโนโลยีสารสนเทศเป็นจำนวนมาก การรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศถือเป็นหัวใจสำคัญ ในการดำเนินงานของสำนักงานประกันสังคม
ที่จะละเลยไปไม่ได้ ด้วยความสำคัญของระบบสารสนเทศที่นับวันจะยิ่งเพิ่มสูงขึ้นและการโจมตีระบบสารสนเทศที่นับวันจะยิ่งซับซ้อนขึ้น ทำให้สำนักงานประกันสังคมมีความจำเป็นต้องใส่ใจทางด้านการรักษาความปลอดภัยสารสนเทศเพิ่มมากขึ้นตามไปด้วย เพื่อป้องกันไม่ให้ข้อมูลของสำนักงานประกันสังคมถูกโจรกรรมโดยผู้ไม่ประสงค์ดี

รวมถึงป้องกันการเกิด Downtime ขึ้นในระบบสารสนเทศ อันจะนำมาซึ่งความเสียหายทางระบบสารสนเทศทำให้สำนักงานประกันสังคมสูญเสียชื่อเสียงและความน่าเชื่อ ดังนั้น เพื่อยกระดับการเฝ้าระวังและรับมือกับภัยคุกคามทางไซเบอร์ ในปี พ.ศ. 2565 สำนักงานประกันสังคมจึงมีความจำเป็นต้องดำเนินการจัดตั้งศูนย์กลางเฝ้าระวังและรับมือภัยคุกคามความปลอดภัยคอมพิวเตอร์ (SSO Security Operation Center) เพื่อให้สามารถรับรู้ถึงสถานการณ์ภัยคุกคามต่าง ๆ ในเครือข่ายของสำนักงานประกันสังคมได้อย่างครอบคลุม และระบุถึงเหตุการณ์ผิดปกติได้อย่างรวดเร็วและแม่นยำรวมถึงตอบสนองต่อเหตุการณ์นั้นได้ทันท่วงที ภัยคุกคามในเรื่องความมั่นคงคอมพิวเตอร์ ของสำนักงานประกันสังคม ในช่วงที่ผ่านมานับตั้งแต่ เดือนกันยายน ปี 2565 ถึงปัจจุบัน ศูนย์กลางเฝ้าระวัง และรับมือภัยคุกคามความปลอดภัยคอมพิวเตอร์ (SSO Security Operation Center) ได้ตรวจจับพบว่าสถิติภัยคุกคามความปลอดภัยมีแนวโน้มเพิ่มขึ้นเป็นลำดับ ในปี 2565 ช่วงเดือนกันยายน - เดือนธันวาคม สถิติการโจมตีจำนวน 118,090,709 ครั้ง เปรียบเทียบช่วงระยะเวลาเดียวกัน ในปี 2566 พบสถิติการโจมตีจำนวน 223,065,555 ครั้ง และเปรียบเทียบเพิ่มเติม ในปี 2566 ช่วงระยะเวลา เดือนมกราคม 2566 - เดือนมีนาคม 2566 สถิติการโจมตีจำนวน 138,162,984 ครั้ง เปรียบเทียบช่วงระยะเวลาเดียวกัน ในปี 2566 พบสถิติการโจมตีจำนวน 169,318,036 ครั้ง

รายงานสถิติการป้องกันภัยคุกคามทางไซเบอร์ สำนักงานประกันสังคม พ.ศ. 2565						
เดือน	การโจมตีจากอินเทอร์เน็ต	การโจมตีผ่านเว็บไซต์	การโจมตีผ่านอีเมล	การโจมตีเครื่องแม่ข่าย	การโจมตีเครื่องลูกข่าย	**รวม**
ก.ย.	5,255,527	16,765,484	34,449	4,143	27,302	22,086,905
ต.ค.	6,893,744	20,633,567	79,057	23,020	50,650	27,680,038
พ.ย.	6,702,082	23,200,344	51,181	4,189	307	29,958,103
ธ.ค.	8,131,646	30,171,665	59,579	2,671	102	38,365,663
รวม	**26,982,999**	**90,771,060**	**224,266**	**34,023**	**78,361**	**118,090,709**

(แหล่งที่มา ข้อมูลจาก สำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม พ.ศ.2567)

รายงานสถิติการป้องกันภัยคุกคามทางไซเบอร์ สำนักงานประกันสังคม พ.ศ. 2566						
เดือน	การโจมตีจากอินเทอร์เน็ต	การโจมตีผ่านเว็บไซต์	การโจมตีผ่านอีเมล	การโจมตีเครื่องแม่ข่าย	การโจมตีเครื่องลูกข่าย	**รวม**
ม.ค.	8,163,565	28,277,205	37,713	1,647	159	36,440,770
ก.พ.	8,173,886	30,184,837	59,212	1,355	231	38,358,723

รายงานสถิติการป้องกันภัยคุกคามทางไซเบอร์ สำนักงานประกันสังคม พ.ศ. 2566						
เดือน	การโจมตีจากอินเทอร์เน็ต	การโจมตีผ่านเว็บไซต์	การโจมตีผ่านอีเมล	การโจมตีเครื่องแม่ข่าย	การโจมตีเครื่องลูกข่าย	**รวม**
มี.ค.	8,518,949	54,844,542	131,321	1,607	288	63,363,491
เม.ย.	8,069,982	104,108,582	198,675	1,568	848	112,178,564
พ.ค.	7,219,813	54,997,154	98,488	1,587	488	62,216,967
มิ.ย.	8,492,432	51,260,498	140,238	4,456	71	59,752,930
ก.ค.	10,789,650	37,259,983	169,833	2,146	469	48,049,633
ส.ค.	8,252,903	27,364,114	104,577	1,519	96	35,617,017
ก.ย.	10,011,738	51,306,076	411,588	1,640	736	61,317,814
ต.ค.	12,678,131	39,100,922	108,078	902	803	51,779,053
พ.ย.	13,240,472	41,282,477	97,302	1,047	120	54,522,949
ธ.ค.	6,718,981	48,726,758	184,093	1,267	126	55,445,739
รวม	**110,330,502**	**568,713,148**	**1,741,118**	**20,741**	**4,435**	**679,043,650**

(แหล่งที่มา ข้อมูลจาก สำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม พ.ศ.2567)

รายงานสถิติการป้องกันภัยคุกคามทางไซเบอร์ สำนักงานประกันสังคม พ.ศ. 2567						
เดือน	การโจมตีจากอินเทอร์เน็ต	การโจมตีผ่านเว็บไซต์	การโจมตีผ่านอีเมล	การโจมตีเครื่องแม่ข่าย	การโจมตีเครื่องลูกข่าย	**รวม**
ม.ค.	5,643,981	46,703,486	363,689	897	168	52,712,221
ก.พ.	6,066,893	49,425,980	151,851	1,074	154	55,645,952
มี.ค.	7,397,376	53,362,128	189,790	10,263	306	60,959,863
รวม	**19,108,250**	**149,491,594**	**705,330**	**12,234**	**628**	**169,318,036**

(แหล่งที่มา ข้อมูลจาก สำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม พ.ศ.2567)

รายงานสถิติการป้องกันภัยคุกคามทางไซเบอร์ สำนักงานประกันสังคม พ.ศ. 2565-2567						
ปี	**การโจมตีจากอินเทอร์เน็ต**	**การโจมตีผ่านเว็บไซต์**	**การโจมตีผ่านอีเมล**	**การโจมตีเครื่องแม่ข่าย**	**การโจมตีเครื่องลูกข่าย**	**รวม**
2022*	26,982,999	90,771,060	224,266	34,023	78,361	118,090,709
2023	110,330,502	568,713,148	1,741,118	20,741	4,435	680,809,944
2024**	**19,108,250**	**149,491,594**	**705,330**	**12,234**	**628**	**169,318,036**
รวม	156,421,751	808,975,802	2,670,714	66,998	83,424	968,218,689

(แหล่งที่มา ข้อมูลจาก สำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม พ.ศ.2567)

หมายเหตุ

*** ข้อมูล ณ เดือนกันยายน 2022 – ธันวาคม 2022**

****ข้อมูล ณ เดือนมกราคม 2024 - มีนาคม 2024**

จากสถิติตัวเลขข้างต้น แสดงให้เห็นว่าภัยคุกคามมีแนวโน้มเพิ่มขึ้น จึงวิเคราะห์ได้ว่า ข้อมูลส่วนบุคคลที่สำนักงานประกันสังคมเก็บรวบรวมนั้นมีคุณค่าเป็นที่ต้องการอาชญากรทางระบบออนไลน์เป็นอย่างมาก

ปัจจุบันสำนักงานประกันสังคมให้ความสำคัญต่อการดำเนินการป้องกันการถูกโจมตีระบบเทคโนโลยีสารสนเทศเพื่อปกป้องมิให้มีการละเมิดข้อมูลส่วนบุคคลที่จัดเก็บในระบบของสำนักงาน ดังต่อไปนี้

1. เจ้าหน้าที่ผู้ปฏิบัติงานต้องดำเนินการเปลี่ยน e-Signature (ลายมือชื่ออิเล็กทรอนิกส์) หรือ Username-Password บนเว็บไซต์ แอปพลิเคชั่นและระบบการใช้งาน เพื่อให้สามารถป้องกันภัยคุกคามใหม่ ๆ ที่เกิดขึ้น รวมทั้ง บนอุปกรณ์ ดังนี้ Intrusion Prevention System (IPS) Firewall Threat Prevention Web Application Firewall (WAF) Extended Detection and Response (XDR) (PC และ Server) E-Mail Gateway Security และ Secure Web Gateway

2. ทำการเฝ้าระวังการและวิเคราะห์พฤติกรรมการโจมตีที่เกิดขึ้นด้วยอุปกรณ์ Sandbox และนำผลค่าบ่งชี้การโจมตีที่ได้จากการวิเคราะห์ Indicator of compromise (IOC) เช่น IP Address, Domain Name และ Hash file ใส่ในอุปกรณ์ทั้งหมด เพื่อป้องกันการโจมตีในรูปแบบ Zero Day

3. จัดให้มีศูนย์กลางเฝ้าระวังและรับมือภัยคุกคามความปลอดภัยคอมพิวเตอร์ Security Operation Center (SOC) ปฏิบัติงานตลอด 7 วัน 24 ชั่วโมง เพื่อเฝ้าระวัง และตอบสนองต่อเหตุการณ์ภัยคุกคาม

4. จัดให้มีอุปกรณ์ Security Orchestrator automation and Response (SOAR) เพื่อเป็นเครื่องมือประสานการทำงานของระบบความปลอดภัยให้ราบรื่น มีการทำงานแบบอัตโนมัติ เพิ่มความเร็วใน

การตอบสนองต่อเหตุการณ์ภัย Cyber Securityจัดการลดผลกระทบ จำกัดความเสียหาย และตอบสนองภัยคุกคามที่เกิดขึ้นแบบอัตโนมัติในทันที ครอบคลุมการโจมตีที่มีผลกระทบระดับ Critical

5. จัดให้มีระบบ Security Information and event management (SIEM) เพื่อวิเคราะห์ความสัมพันธ์ และตรวจจับ Pattern การโจมตีจาก Log

6. มีการทำ Vulnerability Assessment เพื่อตรวจสอบช่องโหว่ที่เกิดขึ้นกับระบบ

7. มีการทำ Penetration Test ทดสอบเจาะระบบต่างๆเพื่อหาช่องโหว่ที่เกิดขึ้นในระดับ Application

8. ดำเนินการ Patch และ Update Operating System เพื่อป้องกันช่องโหว่

9. จัดให้มีทีมผู้เชี่ยวชาญด้าน Cyber Security ในการหาข้อมูล ข่าวสารการโจมตีที่เกิดขึ้น เพื่อนำมาให้คำแนะนำในการตั้งค่าป้องกันการโจมตีบนอุปกรณ์

10. จัดทำแนวปฏิบัติ Cyber Incident Response Plan ของสำนักงานประกันสังคมและปฏิบัติตามแนวปฏิบัติที่กำหนด

11. จัดให้มีการปฏิบัติงานตามกรอบ Cyber Security Framework ของ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา (National Institute of Standards and Technology) หรือที่รู้จักกันในนาม NIST ซึ่งกรอบดังกล่าวประกอบไปด้วย Identify (การระบุและเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง) Protect (การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร) Detect (การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ) Respond (การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น) Recovery (การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม)

12. มีการดำเนินการ และได้รับรองตามมาตรฐานสากล ในการรักษาความมั่นคงปลอดภัย ดังนี้ ISO 27001 Information Security Management Systemหรือมาตรฐานระดับสากลสำหรับจัดการความมั่นคงด้านสารสนเทศ (ISMS) ISO 27701 Privacy Information Management System หรือมาตรฐานการจัดการข้อมูลส่วนบุคคล และ ISO 22301 International Standard for Business Continuity Management หรือมาตรฐานการบริหารความต่อเนื่องทางธุรกิจ

13. ดำเนินการให้ระบบซึ่งให้บริการแก่ผู้ประกันตน ต้องใช้การพิสูจน์ตัวตนสองขั้นตอน (Two-factor Authentication) หรือ การสแกนใบหน้า (EKYC) เพื่อเพิ่มระดับความปลอดภัยในการเข้าถึงระบบขององค์กร

14. นำเทคโนโลยี Encryption และ marking มาใช้เพื่อปกป้องข้อมูลที่สำคัญของผู้ประกันตน

15.การกำหนดนโยบายและกระบวนการที่ชัดเจนในการใช้งานเทคโนโลยีสารสนเทศภายใน

สำนักงาน เช่น การตรวจสอบเครือข่าย (Network Monitoring) เพื่อตรวจจับการฝ่าฝืนนโยบายและการจัดการข้อมูล

2.1.3 ความจำเป็นในการดำเนินการแก้ไขหรือพัฒนา

ปัจจุบัน ประเทศไทยได้มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับเมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 มีวัตถุประสงค์เพื่อปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป กฎหมายฉบับนี้จึงเป็น กฎหมายที่คุ้มครองสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลที่มีข้อมูลอยู่ในความครอบครองทั้งของ ภาครัฐ และภาคเอกชน เป็นการทั่วไป ไม่เจาะจงเฉพาะกรณีใดกรณีหนึ่ง กล่าวอีกนัยหนึ่งคือพระราชบัญญัติฉบับนี้มีเป้าหมายเพื่อทำให้ข้อมูลส่วนบุคคลของประชาชนได้รับการคุ้มครองได้จริง อันจะเป็นผลดีต่อประชาชนผู้เป็นเจ้าของข้อมูลส่วนบุคคลและต่อการยอมรับในระดับสากล และยังสร้างมาตรฐาน ของบุคคลหรือนิติบุคคลในการเก็บข้อมูลส่วนบุคคล รวบรวมข้อมูลส่วนบุคคล ใช้ข้อมูลส่วนบุคคลหรือเพื่อ การเปิดเผยข้อมูลส่วนบุคคลที่จะต้องปฏิบัติตาม หากผู้ใดหรือองค์กรใดไม่ปฏิบัติตามย่อมมีบทลงโทษตามกฎหมาย ซึ่งบทลงโทษสำหรับผู้ที่ไม่ปฏิบัติตามนั้น มีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครองด้วย นับว่าเป็นกฎหมายที่ประชาชนทุกคนควรทราบและตระหนักรู้ถึงสิทธิในข้อมูลส่วนบุคคลของตนเอง อนึ่ง การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ก่อให้เกิดประโยชน์ในหลายภาคส่วน ทั้งการสร้างความมั่นใจว่าข้อมูลส่วนบุคคลของตนได้รับการเก็บรักษา ใช้ และเผยแพร่อย่างปลอดภัยและเหมาะสมในภาคประชาชน การเพิ่มความเชื่อมั่นในมาตรฐานการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลซึ่งช่วยเพิ่มขีดความสามารถและโอกาสในการทำธุรกิจที่มีการใช้ข้อมูลส่วนบุคคลร่วมกับต่างประเทศในภาคธุรกิจ และการมีมาตรการกำกับดูแลรวมถึงเครื่องมือกำกับการดำเนินงานการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพและมีความทัดเทียมนานาอารยประเทศในด้านกฎหมาย ด้านการคุ้มครองข้อมูลส่วนบุคคลในภาครัฐ ซึ่งการคุ้มครองข้อมูลส่วนบุคคลที่มีความชัดเจน นั้น แสดงให้เห็นถึงการมีธรรมาภิบาลในการด้านการคุ้มครองข้อมูลส่วนบุคคลที่โปร่งใสและตรวจสอบได้อีกด้วย
(การคุ้มครองข้อมูลส่วนบุคคล พิธุวรรณ กิติคุณ

กฎหมาย**คุ้มครองข้อมูลส่วนบุคคล** กำหนดหน้าที่ให้ธุรกิจในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ขอความยินยอม (Consent) ต่อเจ้าของข้อมูลส่วนบุคคล เพื่อเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ดังนั้น จึงเป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลที่จะให้ความยินยอมให้ใช้ข้อมูลเหล่านั้นหรือไม่ก็ได้ ในกรณีที่ให้ความยินยอมแล้ว เจ้าของข้อมูลก็ยังคงมีสิทธิในข้อมูลของตัวเองตามกฎหมาย และสามารถใช้สิทธินั้นได้โดยแบ่งออกได้ ดังนี้

1.สิทธิได้รับการแจ้งให้ทราบ ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องแจ้งรายละเอียดและวัตถุประสงค์ในการรวบรวมข้อมูล การใช้ หรือเผยแพร่ให้เจ้าของข้อมูลทราบก่อนหรือขณะ

เก็บรวบรวมข้อมูล โดยเจ้าของข้อมูลมีสิทธิที่จะทราบว่าจะจัดเก็บข้อมูลอะไรบ้าง รวมถึงระยะเวลาการจัดเก็บ สถานที่ และวิธีการติดต่อกับผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเรามักจะเห็นการแจ้งข้อมูลเหล่านี้ตามข้อกำหนดและเงื่อนไขก่อนที่ผู้ใช้งานเว็บไซต์จะสมัครสมาชิก หรืออาจเป็นการขอความยินยอมผ่านแบบฟอร์มก็ได้

2.สิทธิในการแก้ไขข้อมูล เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้ถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยตามเว็บไซต์ส่วนใหญ่ เราจะสามารถเข้าไปแก้ไขข้อมูลส่วนตัว เช่น ที่อยู่ เบอร์โทรศัพท์ รหัสผ่าน ในหน้าบัญชีสมาชิกเองได้

3.สิทธิในการเพิกถอนความยินยอม กรณีเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไป ต่อมาเกิดเปลี่ยนใจหรือไม่ได้ใช้บริการกับธุรกิจนั้นแล้ว ก็สามารถยกเลิกความยินยอมนั้นเมื่อไหร่ก็ได้ เช่น เราสามารถขอยกเลิกติดตามข่าวสารทางอีเมลของเว็บไซต์ได้ โดยกดที่ปุ่ม unsubscribe ที่แนบมาในอีเมล โดยการยกเลิกนี้ไม่ควรเป็นวิธีที่ยุ่งยากซับซ้อน ไม่กำหนดเงื่อนไขหรือต้องให้เจ้าของข้อมูลส่วนบุคคลเสียค่าใช้จ่าย

4.สิทธิในการขอระงับการใช้ข้อมูล ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือไม่ต้องการให้ทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการเรียกร้องสิทธิ ก็สามารถทำได้

5.สิทธิในการเข้าถึง ขอสำเนา หรือให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคล ถ้าเจ้าของข้อมูลส่วนบุคคลไม่แน่ใจว่าได้เคยให้ความยินยอมกับภาคธุรกิจไปหรือไม่ ก็สามารถใช้สิทธิการเข้าถึงข้อมูลนั้นได้โดยต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล และการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น ตัวอย่างเช่นผู้ใช้งานเว็บไซต์อาจเข้าไปดูข้อมูลตนเองในบัญชีสมาชิกของตนเองได้ หรือร้องขอกับผู้ดูแลระบบเพื่อขอดูข้อมูลของตนเองได้

6.สิทธิในการขอรับและให้โอนย้ายข้อมูลส่วนบุคคล ในกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องการให้ธุรกิจที่มีข้อมูลส่วนบุคคลของตนโอนข้อมูลนั้นให้กับอีกธุรกิจอีกราย ซึ่งข้อมูลที่โอนไปนั้นเจ้าของข้อมูลส่วนบุคคลก็ยังขอรับสำเนาข้อมูลนั้นจากธุรกิจที่เป็นผู้จัดทำข้อมูลได้อีกด้วย แต่การใช้วิธีการดังกล่าวต้องไม่ขัดต่อกฎหมาย สัญญา หรือละเมิดสิทธิเสรีภาพของบุคคลอื่น เช่น การย้ายพนักงานจากบริษัทหนึ่งไปยังอีกบริษัทหนึ่ง ตัวพนักงานก็สามารถใช้สิทธิให้บริษัทแรกโอนย้ายข้อมูลส่วนบุคคลไปยังบริษัทที่กำลังจะย้ายไปได้ รวมถึงขอรับสำเนาข้อมูลของตนเองได้

7.สิทธิในการขอคัดค้านการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ โดยร้องขอต่อผู้ควบคุมข้อมูลเมื่อไรก็ได้ โดยร้องขอผ่านแบบฟอร์มที่ผู้ให้บริการจัดไว้ หรือติดต่อกับผู้ดูแลระบบ

8.สิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคล ธุรกิจจะต้องเป็นผู้รับผิดชอบค่าใช้จ่าย ถ้าเจ้าของข้อมูลขอให้ธุรกิจลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็น

ข้อมูลที่ไม่สามารถระบุตัวตนได้ ในกรณีที่ข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ หรือธุรกิจนำข้อมูลไปเผยแพร่ในที่สาธารณะ หรือเจ้าของข้อมูลเห็นว่าข้อมูลของตนนั้นสามารถเข้าถึงได้ง่ายเกินไป

9.สิทธิในการร้องเรียน เจ้าของข้อมูลมีสิทธิร้องเรียนต่อพนักงานเจ้าหน้าที่และคณะกรรมการตาม PDPA ได้ ถ้าผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย รวมถึงมีสิทธิในการเรียกค่าสินไหมทดแทนทางศาลด้วย

สถิติการคุกคามทางไซเบอร์ ที่มีแนวโน้มเพิ่มขึ้น ส่งผลให้ เราต้องตระหนักถึงการบริหารจัดการข้อมูลภายใต้การบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 ซึ่งหากสามารถบริหารจัดการให้ลูกค้า ผู้เป็นเจ้าของข้อมูล หรือผู้ประกันตน สามารถดูแล บริหารจัดการข้อมูลของตนเองได้ ก็จะส่งผลต่อภาพลักษณ์ความน่าเชื่อถือของสำนักงานประกันตนสังคม ลดการถูกร้องเรียน

2.2 การกำหนดข้อเสนอเชิงนโยบาย

2.2.1 หลักการและแนวคิดในการจัดทำข้อเสนอ

(1) แนวคิด ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

ปัจจุบันเราใช้ชีวิตเชื่อมโยงกับอินเทอร์เน็ตในหลากหลายมิติ จากผลสำรวจพฤติกรรมการใช้อินเทอร์เน็ตของประเทศไทยในปี 2563 ของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) หรือ ETDA กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม นั้น คนไทยใช้อินเทอร์เน็ตในการทำกิจกรรมมากมาย ตั้งแต่การทำธุรกรรมออนไลน์ (56.5%) การซื้อของ (67.3%) การหาข้อมูล (82.2%) การติดต่อสื่อสาร (77.8%) ความบันเทิง (ดูหนัง/คลิป/โทรทัศน์/ฟังเพลง ที่ 85%) และอื่น ๆ อีกมากมาย ทั้งหมดนี้ หากการรักษาความมั่นคงปลอดภัยไซเบอร์อ่อนแอ ก็อาจทำให้ผู้ประสงค์ร้ายเข้ามาทำอันตรายต่อเราและข้อมูลส่วนบุคคลของเราได้ ตั้งแต่การเข้าถึงข้อมูลส่วนบุคคลของเราที่เราไม่ได้ตั้งใจจะเปิดเผย เช่น เพศวิถี อายุ สัญชาติ ศาสนา จนอาจนำไปสู่การขโมยข้อมูลของเราไปใช้ อาทิ รหัสบัตร ATM ข้อมูลบัตรเครดิต การสวมรอยเป็นเราไปจนถึงการเรียกค่าไถ่เพื่อแลกกับการไม่เปิดเผยข้อมูลของเรา

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 3 ให้ความหมายคำที่น่าสนใจไว้ ดังนี้ “การรักษาความมั่นคงปลอดภัยไซเบอร์” ไว้ว่า “มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ” “เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือ การดำเนินการใดๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิด

ความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัย ไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

(2) แนวคิดการคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) หมายถึง การดูแลปกป้องบุคคลจากการถูกละเมิดเกี่ยวกับข้อมูลส่วนบุคคลโดยกฎหมาย ซึ่งเป็นการจำกัดสิทธิและเสรีภาพบางประการของบุคคลที่เก็บรวบ ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้อื่น เพื่อให้เกิดการคุ้มครองข้อมูลส่วนบุคคลและมาตรการเยียวยาเจ้าของข้อมูลที่มีประสิทธิภาพ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีสาระสำคัญ คือการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องมีการดำเนินการดังนี้ ให้เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอม ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล Consent ต้องแยกออกจากส่วนอื่นชัดเจน มีแบบหรือข้อความที่อ่านแล้วเข้าใจได้โดยง่ายและต้องไม่เป็นการหลอกลวง และ เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้

สิทธิของเจ้าของข้อมูลส่วนบุคคล ภายใต้พระราชบัญญัติฯ ประกอบไปด้วย

1. สิทธิได้รับแจ้งรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล (Right to be Informed)
2. สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)
3. สิทธิขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
4. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
5. สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (Right to erasure/right to be forgotten)
6. สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล (Right to restrict processing)
7. สิทธิขอให้แก้ไขข้อมูลส่วนบุคคล (Right to rectification)
8. สิทธิในการร้องเรียนกรณีที่ผู้ควบคุมหรือผู้ประมวลผลไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

(3) แนวคิด good governance

ธรรมาภิบาล (good governance) เป็นกระแสที่ทุกภาคส่วนไม่ว่าจะเป็นภาครัฐ ภาคธุรกิจเอกชน และภาคประชาชน ให้ความสนใจและนำมาประยุกต์ใช้ในการดำเนินงานขององค์กรด้วยหลักธรรมาภิบาล ซึ่งประกอบด้วยหลักสำคัญ 6 ประการคือ หลักนิติธรรม หลักคุณธรรม หลักความโปร่งใส หลักการมีส่วนร่วม หลักสำนึกรับผิดชอบ และหลักความคุ้มค่าเป็นความสอดคล้องกับความรู้สึก และความต้องการของสาธารณะชน และสาธารณะชนก็มีความคาดหวังให้ทุกภาคส่วนมีการปฏิบัติอย่างแท้จริง มิใช่เป็นเพียงแต่กระแสนิยมเท่านั้น

(4) แนวคิด Data tracker กรณีตัวอย่างของประเทศเอสโตเนีย

ในประเทศเอสโตเนียได้พัฒนา State portal Eesti.ee ให้เป็น เว็บไซต์ในการเข้าใช้บริการอิเล็กทรอนิกส์ต่างๆของประชาชนในประเทศ รวมถึงการเข้าถึงฐานข้อมูลอิเล็กทรอนิกส์ของประชาชนในประเทศเอสโตเนีย ข้อมูลทั้งหมดของประชาชนจะถูกจัดหมวดหมู่เอาไว้เพื่อง่ายต่อ การใช้งาน ประชาชนสามารถเข้าถึงข้อมูลต่างๆของตนเองได้อย่างสะดวกและรวดเร็ว เช่น หมวดหมู่ health care ที่สามารถดูใบสั่งยาดิจิทัลได้ หรือ หมวดหมู่ การศึกษา ที่สามารถดูผลคะแนนสอบของตนได้ จากฐานข้อมูลนี้ จนไปถึงข้อมูลครอบครัว อสังหาริมทรัพย์ โดยประชาชนสามารถเข้าถึงฐานข้อมูลนี้ได้โดย log in ผ่านเลขประจำตัวประชาชน

และภายใต้ แพลตฟอร์ม State portal Eesti.ee หรือเว็บไซต์ ดังกล่าวข้างต้นรัฐบาลของเอสโตรเนียได้พัฒนา “ระบบ Data tracker”(ระบบติดตามข้อมูลส่วนบุคคล) ขึ้นมา ตั้งแต่ปี 2017 เพื่อให้บริการประชาชน ในการตรวจสอบว่ามีใคร เข้าถึงข้อมูลของตน และด้วยเหตุผลอะไร ทำให้ประชาชนเห็นภาพรวมของการใช้ข้อมูลส่วนบุคคลของตนเอง ตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของเอสโตเนีย และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) กำหนด โดยหลักการทำงาน ของ Data tracker เครื่องมือนี้จะตรวจสอบประวัติการรับและส่งข้อมูลที่เข้าออกจาก database และ จัดเก็บเอาไว้ใน data recorder ข้อมูลเหล่านี้จะไปปรากฏในช่องทางเว็บไซต์ของภาครัฐเพื่อให้ประชาชนเข้าไปตรวจสอบการ ไหลข้อมูลของตน และรายการของผู้ที่เข้าถึงข้อมูลของตนทั้งหมดได้

และสืบเนื่องต่อไปจากการที่ประชาชนสามารถตรวจสอบข้อมูลดังกล่าวข้างต้นได้แล้ว ประชาชนของเอสโตเนียสามารถบริหารจัดการข้อมูลของตนเองได้ในการให้ความยินยอมหรือไม่ให้ความยินยอมแก่ภาครัฐในการส่งข้อมูลให้แก่บุคคลที่ 3 ผ่าน “ระบบ The consent service”(ระบบบริการการให้ความยินยอม) คือ ระบบบริการอิเล็กทรอนิกส์ที่ให้ประชาชนเข้ามามีส่วนร่วมในการจัดการการ ใช้ข้อมูลของตน เริ่มใช้ในปี 2021 ภายใต้หลักการที่ ประชาชนสามารถให้ความยินยอมให้รัฐส่งข้อมูลส่วนบุคคลของตนที่ถูกจัดเก็บไว้ที่รัฐ ไปยังบุคคลที่ 3 ที่กำหนดไว้โดยเฉพาะเจาะจง ได้ โดยเมื่อมีบุคคลที่ 3 มาขอข้อมูลส่วนตัวของประชาชนท่านใดไป ในหน้าช่องทางเว็บไซต์ของรัฐ (eesti.ee) ระบบจะมีการแจ้งเตือนไปยังเจ้าของข้อมูลส่วนบุคคลเพื่อ ขอความยินยอมว่าจะให้รัฐส่งข้อมูลนี้ให้แก่บุคคลที่ 3 หรือไม่ ในการแจ้งนั้นจะมีทั้งเนื้อหาว่าข้อมูลใดบ้างที่ จะถูกส่งไป และวัตถุประสงค์ของการส่งครั้งนี้คืออะไร

จากการที่ประเทศเอสโตเนียมีการระบบติดตามข้อมูลส่วนบุคคล โดยเจ้าของข้อมูลส่วนบุคคลสามารถเห็นภาพรวมของข้อมูลส่วนบุคคลของตนได้ว่ามีใครใช้ข้อมูล ส่วนบุคคลนี้บ้างหรือการใช้งานเป็นไปเพื่อวัตถุประสงค์ใด ทำให้ประชาชนสามารถเข้ามามีส่วนร่วมกับการจัดการการใช้ ข้อมูลส่วนบุคคลของตนได้มากขึ้น สามารถตัดสินใจได้ว่าจะให้ใครบ้างใช้ข้อมูลของตน บริการนี้ทำให้การบริหารจัดการข้อมูลของประชาชนมีความโปร่งใสและช่วยให้สามารถแบ่งปันข้อมูลส่วนบุคคลระหว่างรัฐและ เอกชน

จากแนวคิดที่ต้องการให้ประชาชนสามารถบริหารจัดการข้อมูลส่วนบุคคลของตนเองได้ การพัฒนาระบบ“ระบบ Data tracker”(ระบบติดตามข้อมูลส่วนบุคคล) และ“ระบบ The consent service” (ระบบบริการการให้ความยินยอม) ทั้งหมดทำให้รัฐบาลเอสโตรเนียสามารถพัฒนาการบริการภาครัฐต่อไปได้อีกมากมาย เช่น การให้ความร่วมมือกับสถาบันทางการเงิน ธนาคาร และร้านค้าต่างๆ เพื่อทำการเชื่อมโยงฐานข้อมูลเกี่ยวกับข้อมูลทางการเงิน หรือข้อมูลส่วนบุคคลอื่น ยกตัวอย่างเช่น ธนาคารจะสามารถตรวจสอบความสามารถในการชำระหนี้ของเจ้าของข้อมูลส่วนบุคคลนั้นจากฐานข้อมูลของศุลกากรได้หาก เจ้าของข้อมูลให้การยินยอม ประชาชนก็จะได้รับความสะดวกในเรื่องทางการเงิน การอนุมัติเงินกู้ต่างๆ

โดยสรุป ระบบ“ระบบ Data tracker”(ระบบติดตามข้อมูลส่วนบุคคล) และ“ระบบ The consent service”(ระบบบริการการให้ความยินยอม) เหมือนเป็นช่องทางกลางที่ให้บุคคลมาให้ความยินยอมและบริหารจัดการ ความยินยอมในการใช้ข้อมูลส่วนบุคคลของตนที่ถูกจัดเก็บไว้กับรัฐ หลังจากที่เจ้าของข้อมูลได้ให้หรือไม่ให้ความยินยอมแล้ว เจ้าของข้อมูลส่วนบุคคลยังคงสามารถเข้าไป บริหารจัดการความยินยอมได้ที่หน้าเว็บไซต์ การให้ความยินยอมจะต้องเป็นไปโดยอิสระและด้วยความสมัครใจเสมอ อีกทั้งเจ้าของข้อมูลส่วนบุคคลยัง สามารถเพิกถอนความยินยอมได้ตลอดเวลา หากมีการถอนความยินยอมเกิดขึ้นการส่งข้อมูลไปยังบุคคลที่ 3 จะถูกระงับทันที ถึงแม้ว่าปัจจุบันจุดเริ่มต้นจะเริ่มจากการแบ่งปันข้อมูลทางการเงินเท่านั้น และในอนาคตรัฐบาลเอสโตเนียได้วางแผนการขยายบริการนี้ไปยัง ข้อมูลอื่นๆด้วยอย่างแน่นอน เช่น ข้อมูลสุขภาพ ข้อมูลเกี่ยวกับการศึกษา เป็นต้น

2.2.2 วิเคราะห์ข้อมูลเพื่อประกอบการจัดทำข้อเสนอ

สำนักงานประกันสังคมเป็นหน่วยงานที่มีการจัดเก็บข้อมูลเป็นจำนวนมาก และเป็นข้อมูลที่มีความสำคัญไม่ว่าจะเป็นข้อมูลนายจ้าง ข้อมูลผู้ประกันตนที่ ข้อมูลสถานพยาบาล รวมไปถึงข้อมูลการจ่ายสิทธิประโยชน์ ข้อมูลเหล่านี้จำเป็นต้องมีการป้องกันการเข้าถึง จากข้อมูลสถิติภัยคุกคามทางไซเบอร์ของไทยรวบรวม โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) พบว่าความพยายามบุกรุกเข้าระบบสารสนเทศ (Intrusion Attempts) เป็นภัยคุกคามไซเบอร์อันดับ 1 ของประเทศไทย ไม่ว่าจะเป็นการเผยแพร่ ข้อมูลที่ไม่เป็นจริงการพยายามบุกรุกเข้าระบบการโจมตีสภาพการใช้งานของระบบ การพัฒนาโปรแกรมที่ไม่พึ่งประสงค์อันก่อให้เกิดความเสียหายแก่ประเทศชาติ ภาคธุรกิจ รายบุคคล และสถิติจากศูนย์กลางเฝ้าระวังและรับมือภัยคุกคามความปลอดภัยคอมพิวเตอร์ (SSO Security Operation Center) ของสำนักงานประกันสังคมใน นับแต่เดือนกันยายน ปี 2565 - เดือนมีนาคม 2567 ระยะเวลา 19 เดือน พบว่ามีภัยคุกคามและการโจมตีทางไซเบอร์ ที่ได้ตรวจพบทั้งหมด 968,218,689 เหตุการณ์ เช่น การโจมตีจาก Malware ผ่านเครือข่ายอินเทอร์เน็ตการโจมตีผ่านระบบเครือข่าย เป็นต้น

ในปี พ.ศ. 2565 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมาย PDPA (Personal Data Protection Act) มีผลใช้บังคับ ดังนั้นในการทำการใดก็ตามที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจึงจำเป็นต้องปฏิบัติตาม พ.ร.บ.ความคุ้มครองข้อมูลส่วนบุคคล ดังกล่าว สาระสำคัญของกฎหมายคือการ

คุ้มครองและให้สิทธิที่ผู้ใช้งานควรมีต่อข้อมูลส่วนบุคคลของผู้ใช้งานได้ รวมไปถึงการสร้างมาตรฐานของบุคคลหรือนิติบุคคล ในการเก็บข้อมูลส่วนบุคคล รวบรวมข้อมูลส่วนบุคคล ใช้ข้อมูลส่วนบุคคล หรือเพื่อการเปิดเผยข้อมูลส่วนบุคคลก็ตาม ล้วนจะต้องปฏิบัติตาม หากผู้ใดหรือองค์กรในไม่ปฏิบัติตามย่อมมีบทลงโทษตามกฎหมาย ดังนั้นหากต้องทำการป้องกันข้อมูล (Data Protection) จำเป็นต้องมีองค์ประกอบ 2 ส่วน ได้แก่ ส่วนที่ 1 ความปลอดภัยของข้อมูล (Data Security) คือการตรวจสอบสิทธิ์การใช้งาน (Authentication) การเข้ารหัสข้อมูล (Encryption) การป้องกันข้อมูลสูญหาย (Data Loss Prevention) การตอบโต้ละเมิด (Breach Response) การเฝ้าระวังการจู่โจมหรือการโจมตี (Threat Monitoring) และการควบคุมการเข้าถึง (Access Control) ส่วนที่ 2 ข้อมูลส่วนบุคคล (Data Privacy) ได้แก่ ข้อกฎหมายหรือพ.ร.บ. (Legislation) การกำหนดสิทธิหน้าที่และความรับผิดชอบในการบริหารจัดการข้อมูลหรือธรรมาภิบาลข้อมูล (Data Governance) การบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล (DataSubject Access Request : DSAR) เป็นต้นดังนั้น ถ้าหน่วยงานใดมีองค์ประกอบ 2 ส่วนนี้แล้วจะทำให้ข้อมูลที่นำไปใช้จะมีความปลอดภัยและน่าเชื่อถือ เพื่อให้ผู้ใช้บริการเชื่อมั่นได้ว่าสำนักงานประกันสังคมได้ดูแลรักษาข้อมูลส่วนบุคคลของผู้ประกันตนเป็นอย่างดีและจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมอีกทั้งยังสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ตั้งแต่กระบวนการเก็บรวมรวมการจัดเก็บรักษา การใช้ การเปิดเผยตลอดจนการเปิดโอกาสให้เจ้าของข้อมูลส่วนบุคคลมีส่วนร่วมในการตรวจสอบและขอใช้สิทธิของตนเองตามที่กฎหมายกำหนด

2.2.3 แนวทางการพัฒนา

สำนักงานประกันสังคม มีภารกิจหลักในการบริหารงานกองทุนประกันสังคมและกองทุนเงินทดแทนที่ทันสมัย มีประสิทธิภาพ และโปร่งใส ตามยุทธศาสตร์ภายใต้แผนปฏิบัติราชการสำนักงานประกันสังคมระยะ 5 ปี (พ.ศ. 2566 - 2570) ทั้ง 3 ยุทธศาสตร์ ได้แก่ ยุทธศาสตร์ที่ 1 การพัฒนาเทคโนโลยีและนวัตกรรม เพื่อสร้าง การให้บริการเชิงรุกแก่ทุกคน ยุทธศาสตร์ที่ 2 การสร้างพลังแห่งการขับเคลื่อนสู่องค์กรแห่งความเชื่อมั่น ความไว้วางใจ และมีธรรมาภิบาล และยุทธศาสตร์ที่ 3 การเพิ่มประสิทธิผลในการสร้างและเข้าถึงหลักประกันสังคมให้แก่แรงงาน ทุกกลุ่ม ทุกวัย สำนักงานประกันสังคมจึงมุ่งเชื่อมโยงสังคมแรงงานด้วยเครือข่ายดิจิทัล และปฏิรูปดำเนินงานขององค์กรให้ก้าวทันต่อการเปลี่ยนแปลงสู่โลกยุคดิจิทัล เพื่อให้เกิดประโยชน์ต่อสังคมแรงงานของประเทศ แรงงานมีหลักประกันการดำรงชีวิตที่มั่นคง รวมทั้งสร้างการเข้าถึงและให้บริการแก่ผู้รับบริการได้อย่างเต็มศักยภาพ ด้วยการจัดการที่มีประสิทธิภาพ ทันสมัย และสอดคล้องกับนโยบายและแผนระดับชาติ ดังนั้น สำนักงานประกันสังคมจึงจำเป็นต้องมีการเก็บรวบรวม จัดเก็บ ใช้ข้อมูลส่วนบุคคลของพนักงานเจ้าหน้าที่ บุคลากรภายในองค์กร ผู้ประกอบกิจการในฐานะนายจ้าง และประชาชนบุคคลทั่วไปในฐานะลูกจ้างผู้ประกันตนเป็นจำนวนมาก ทั้งยังมีการเชื่อมโยงข้อมูลไปยังหลากหลายหน่วยงาน ไม่ว่าจะเป็นหน่วยงานรัฐหรือหน่วยงานเอกชน เพื่ออำนวยความสะดวกให้แก่เจ้าของ

ข้อมูลสามารถส่งต่อหรือโอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอกได้อย่าง สะดวกและรวดเร็ว ด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดหลักเกณฑ์ กลไก หรือมาตรการการกำกับดูแลการให้ความคุ้มครองข้อมูลส่วนบุคคลอันเป็นหลักการทั่วไป โดยกำหนดมาตรฐานใหม่ในเรื่องการให้ความคุ้มครองส่วนบุคคลของประเทศไทยให้เทียบเท่าสากลซึ่งมีความเกี่ยวข้องกับทุกภาคส่วน ทั้งหน่วยงานของรัฐ เอกชน และประชาชน โดยเฉพาะอย่างยิ่งการส่งหรือการเปิดเผยข้อมูลส่วนบุคคลนั้น จะต้องสามารถอ้างอิงฐานการประมวลผลหรือเงื่อนไขพิเศษตามมาตรา 24 มาตรา 26 ประกอบมาตรา 27 ได้ รวมถึงจะต้องมีการแจ้งรายละเอียดของการเปิดเผยข้อมูลส่วนบุคคล บุคคลหรือประเภทบุคคลที่ได้รับการเปิดเผยข้อมูลส่วนบุคคล และฐานการประมวลผลที่ใช้อ้างอิงตามมาตรา 21 และมาตรา 23

นอกจากการที่สำนักงานประกันสังคมจะต้องปฏิบัติตามมาตรฐาน ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แล้ว สถิติการคุกคามทางไซเบอร์ ที่มีแนวโน้มเพิ่มขึ้น ในช่วงที่ผ่านมา นับตั้งแต่ เดือนกันยายน ปี 2565 ถึงปัจจุบัน ศูนย์กลางเฝ้าระวัง และรับมือภัยคุกคามความปลอดภัยคอมพิวเตอร์ (SSO Security Operation Center) ได้ตรวจจับพบว่าสถิติภัยคุกคามความปลอดภัยมีแนวโน้มเพิ่มขึ้นเป็นลำดับ ในปี 2565 ช่วงเดือนกันยายน - เดือนธันวาคม สถิติการโจมตีจำนวน 118,090,709 ครั้ง เปรียบเทียบช่วงระยะเวลาเดียวกัน ในปี 2566 พบสถิติการโจมตีจำนวน 223,065,555 ครั้ง และเปรียบเทียบเพิ่มเติม ในปี 2566 ช่วงระยะเวลา เดือนมกราคม 2566 - เดือนมีนาคม 2566 สถิติการโจมตีจำนวน 138,162,984 ครั้ง เปรียบเทียบช่วงระยะเวลาเดียวกัน ในปี 2566 พบสถิติการโจมตีจำนวน 169,318,036 ครั้ง ซึ่งสาเหตุหนึ่งในหลายสาเหตุที่แฮกเกอร์เหล่านี้ต้องการนั้นก็คือ ข้อมูลส่วนบุคคลจำนวนมหาศาลที่สำนักงานประกันสังคมได้ จัดเก็บ ควบคุมไว้ในระบบสารสนเทศ สำนักงานประกันสังคม

ดังนั้น ข้อเสนอเรื่อง “แนวทางพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน” จึงมีความสำคัญต่อผู้ประกันตนเป็นอย่างมาก ในปัจจุบันสำนักงานประกันสังคมมีความจำเป็นตามกฎหมายและการพัฒนาการให้บริการ ในการต้องเชื่อมโยงข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอกทั้งภาครัฐและภาคการเงินการธนาคารซึ่งเป็นภาคเอกชน หากสามารถพัฒนา “ระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน” เพื่อเป็นช่องทางให้บริการแก่ผู้ประกันตนซึ่งเป็นเจ้าของข้อมูลสามารถตรวจสอบการส่งหรือการเปิดเผยข้อมูลส่วนบุคคลของตน เห็นภาพรวมของการใช้ข้อมูลส่วนบุคคลของตนเอง และที่สำคัญสามารถบริหารจัดการข้อมูลของตนเองได้ในการให้ความยินยอมหรือไม่ให้ความยินยอมแก่สำนักงานประกันสังคมในการส่งข้อมูลให้แก่บุคคลที่ 3 ที่สำนักงานประกันสังคมได้เชื่อมโยงไปยังหน่วยงานภายนอกได้ ประโยชน์ที่ผู้ประกันตนจะได้รับจากแนวทางการพัฒนานี้ คือ ได้รับสิทธิการจัดการข้อมูลส่วนบุคคลอย่างสมบูรณ์ตามที่กฎหมายกำหนด และในระยะยาวเพื่อประโยชน์สูงสุดในการรับบริการของผู้ประกันตนภายใต้ความยินยอมของเจ้าของข้อมูล สำนักงานประกันสังคมสามารถพัฒนาระบบเชื่อมโยงข้อมูลให้เชื่อมโยงกับภาคธุรกิจที่มีความจำเป็นต้องใช้ข้อมูลส่วนบุคคล เช่น การยื่นขอกู้เงินต่อสถาบันทางการเงินของสถาบันทางการเงินหากมีความจำเป็นต้องใช้หลักฐานข้อมูลความมั่งคงทางการเงิน ทางด้านสุขภาพ

ทางครอบครัว ก็จะสามารถตรวจสอบได้ภายใต้ความยินยอมของเจ้าของข้อมูล ลดระยะเวลาการรอคอยการอนุมัติเงินกู้เช่นในปัจจุบัน ตลอดจนเชื่อมั่นว่า สถิติการคุกคามทางไซเบอร์น่าจะลดลงเนื่องจากธุรกิจเอกชนสามารถเชื่อมโยงข้อมูลได้โดยตรงกับหน่วยงานที่มีข้อมูลภายใต้ความยินยอมของเจ้าของข้อมูล ก็จะลดความเดือดร้อนรำคาญจากการได้รับโทรศัพท์เสนอขายสินค้าจากภาคเอกชน และสุดท้ายสำนักงานประกันสังคมก็จะเป็นหน่วยงานอันมีธรรมาภิบาลที่ดี มีภาพลักษณ์ที่โปร่งใสเป็นที่น่าเชื่อถือของผู้ประกันตนผู้รับบริการ

2.2.3.1. การออกแบบพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน

ข้อเสนอเรื่อง “แนวทางพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน” ผู้ศึกษาจึงออกแบบ “ระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน อันประกอบไปด้วยระบบย่อย” ดังนี้

1. ระบบการจัดเก็บข้อมูล (Data Storage Unit) เพื่อเป็นเครื่องมือจัดเก็บข้อมูลที่จะถูกติดตามในหน่วยความจำที่มีประสิทธิภาพ เพื่อดำเนินการประมวลผลและการเรียกใช้ข้อมูลเมื่อต้องการ

2. ระบบประมวลผลข้อมูล (Data Processing Unit) เพื่อเป็นเครื่องมือประมวลผลข้อมูลที่ถูกจัดเก็บ ซึ่งรวมถึงการวิเคราะห์และนำเสนอข้อมูลออกมาในรูปแบบที่เข้าใจง่าย

3. ระบบเซิร์ฟเวอร์ (server) เพื่อเป็นเครื่องมือสนับสนุนการให้บริการ ดำเนินการจัดการข้อมูลและบริการต่างๆ ในเครือข่ายคอมพิวเตอร์

4. ระบบแสดงผล (User Interface) เพื่อเป็นเครื่องมือให้ผู้ใช้งานสามารถเข้าถึงข้อมูลและการแสดงผลผ่านอินเทอร์เฟซที่ออกแบบให้ใช้งานง่าย และช่วยให้ผู้ใช้สามารถทำกิจกรรมต่างๆบนระบบได้ด้วยความสะดวก

5. ระบบบันทึกการกระทำ (Audit Logging) เพื่อเป็นเครื่องมือในการบันทึกข้อมูลการกระทำที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่นการเข้าถึงข้อมูล การเปลี่ยนแปลงข้อมูล และการลบข้อมูล เพื่อการตรวจสอบและติดตามการใช้ข้อมูลในอดีต

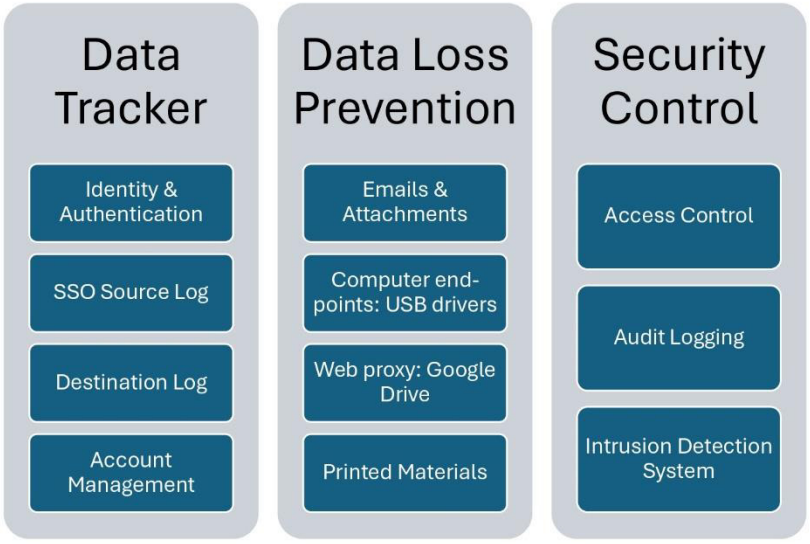
6. การตรวจจับการละเมิด (Intrusion Detection) เพื่อเป็นเครื่องมือในการตรวจจับและแจ้งเตือนในกรณีมีการละเมิดความปลอดภัยของข้อมูลหรือการเข้าถึงข้อมูลโดยไม่ถูกต้อง

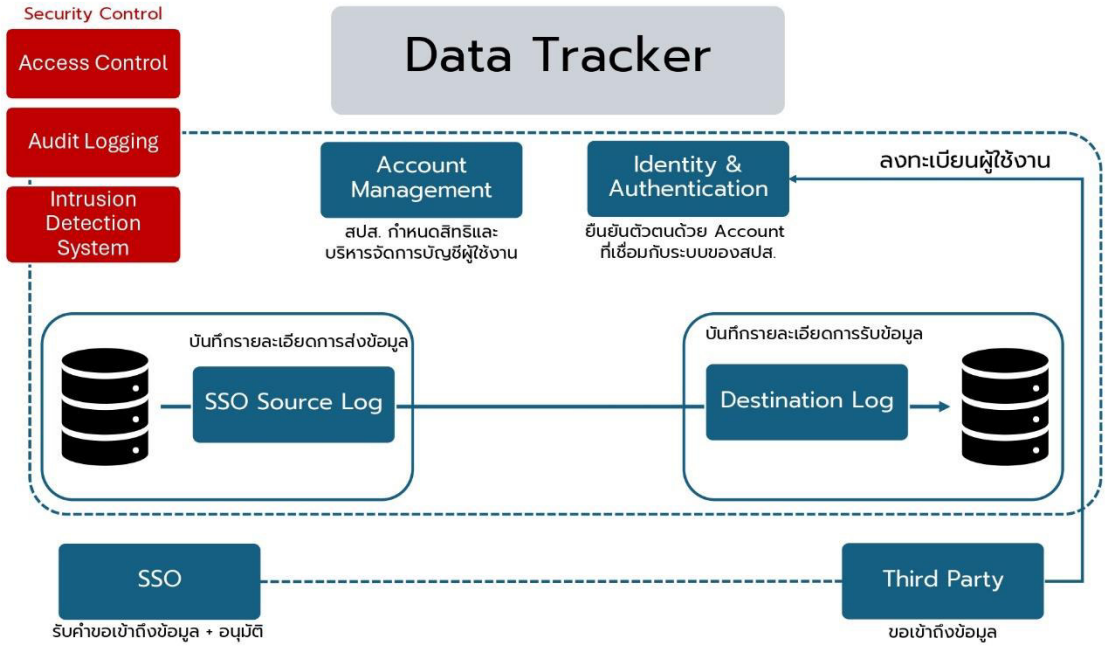
7.ระบบรักษาความปลอดภัย (Security System) เพื่อเป็นเครื่องมือในการควบคุมและความปลอดภัยของข้อมูลที่ถูกเก็บไว้ในระบบ เช่น การกำหนดสิทธิ์การเข้าถึงข้อมูล การเข้ารหัสข้อมูล เป็นต้น

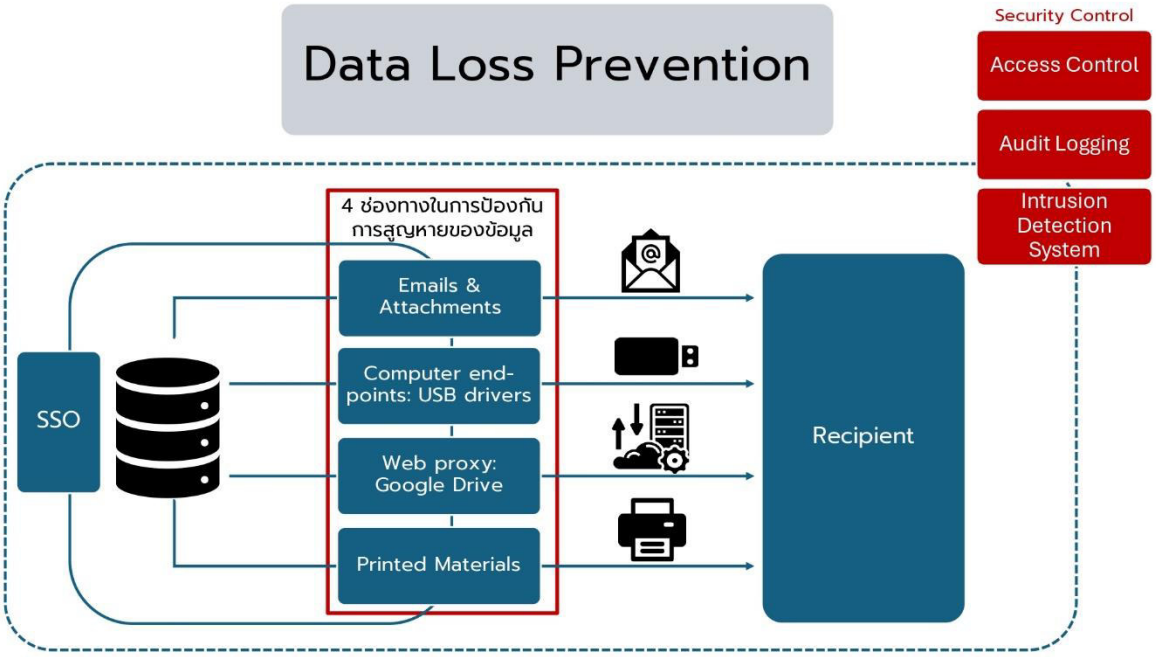
8. ระบบการตรวจสอบการเข้าถึงข้อมูล (Access Control) เพื่อเป็นเครื่องมือในการควบคุมการเข้าถึงข้อมูลให้เฉพาะบุคคลที่มีสิทธิ์เท่านั้น และป้องกันการเข้าถึงข้อมูลจากบุคคลที่ไม่มีสิทธิ์

9.การยืนยันตัวตน (Authentication)**: เพื่อเป็นเครื่องมือในการตรวจสอบความถูกต้องของผู้ใช้งานและอำนาจในการเข้าถึงข้อมูล เช่นการใช้งานรหัสผ่าน การสแกนลายนิ้วมือ ใบหน้า หรือการใช้งานการรับรองประสิทธิภาพสูง (Multi-factor authentication)

Data Tracker Diagram







2.2.3.2. ภาพรวมของระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน

การยืนยันตัวตน	บริการที่รองรับ	การจัดเก็บข้อมูล
ผู้ประกันตนจะต้องทำการยืนยันตัวตนผ่าน เว็บไซต์ของสำนักงานประกันสังคม ที่ www.sso.go.th หรือระบบแอพพลิเคชั่นของประกันสังคม ชื่อว่า sso plus หรือระบบ Thai D ของกรมการปกครอง กระทรวงมหาดไทย	ระบบจะถูกวางบนเว็บไซต์ของสำนักงานประกันสังคม ที่ www.sso.go.th และแอพพลิเคชั่น sso plus เพื่อแสดงผล ดังนี้ - ผู้ประกันตนที่เป็นเจ้าของข้อมูลเท่านั้นจะสามารถเข้าถึงข้อมูลเฉพาะของตน - ผู้ประกันตนสามารถเข้าถึงข้อมูลส่วนบุคคล ทำการเปลี่ยนแปลงข้อมูล ตรวจสอบการนำใช้ข้อมูลส่วนบุคคลไปใช้	ข้อมูลที่กำหนดจัดเก็บในหน่วยความจำที่มีประสิทธิภาพ และมีความมั่นคงปลอดภัย และข้อมูลจะถูกทำการบันทึกข้อมูลการกระทำที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่นการเข้าถึงข้อมูล การเปลี่ยนแปลงข้อมูล และการลบข้อมูล เพื่อการตรวจสอบและติดตามการใช้ข้อมูลในอดีต เพื่อดำเนินการประมวลผล นำเสนอผู้ใช้งาน

การยืนยันตัวตน	บริการที่รองรับ	การจัดเก็บข้อมูล
	และสามารถใช้สิทธิ์อนุญาตหรือไม่อนุญาตให้ใช้ข้อมูล	

2.2.3.3. ขั้นตอนการดำเนินงานในการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน

ข้อเสนอเรื่อง “แนวทางพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน”ผู้ศึกษาจึงกำหนด**ขั้นตอนการดำเนินงานของสำนักงานประกันสังคม ไว้ดังต่อไปนี้**

1) กองวิจัยและพัฒนา และ สำนักบริหารเทคโนโลยีสารสนเทศ ร่วมกัน ศึกษาและรวบรวมรายละเอียดของกฎหมาย ระเบียบ ข้อบังคับ นโยบาย และแนวทางปฏิบัติที่เกี่ยวข้องกับการส่งหรือเปิดเผยข้อมูลส่วนบุคคล เช่น พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น โดยจะต้องสรุปประเด็นที่เกี่ยวข้องในการพัฒนาระบบติดตามข้อมูลส่วนบุคคล ซึ่งรวมถึงประเภทข้อมูลที่จะเก็บบันทึกในระบบติดตามข้อมูลส่วนบุคคลตลอดจน หน้าที่ของผู้ที่มีหน้าที่ควบคุม และผู้ประมวลผลข้อมูล ภายใต้ พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

2) สำนักบริหารเทคโนโลยีสารสนเทศ ยกร่างโครงการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน โดยมีรายละเอียดคุณลักษณะเฉพาะด้านเทคนิคที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ นโยบาย และแนวทางปฏิบัติที่เกี่ยวข้องกับการส่ง/เปิดเผยข้อมูลส่วนบุคคล ตามที่ได้ศึกษาในข้อ 1) และกำหนดรายละเอียดขั้นตอนการทำงาน รายละเอียดขั้นตอนการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ และปริมาณที่ใช้ต้องงาน และอุปกรณ์รักษาความมั่นคงปลอดภัย ระยะเวลาที่ใช้ในการดำเนินการ

3) กองวิจัยและพัฒนาศึกษาโครงสร้างข้อมูลผู้ประกันตนในระบบฐานข้อมูล เพื่อเตรียมความพร้อมในการพัฒนาระบบ

4) สำนักบริหารเทคโนโลยีสารสนเทศ ตรวจสอบวิเคราะห์ความพอเพียงของทรัพยากรที่มีในระบบโครงสร้างพื้นฐานเทคโนโลยี ของสำนักงานประกันสังคม อันประกอบไปด้วย อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบฐานข้อมูล เพื่อกำหนดระบบงานหลักภายใต้โครงการโดยคัดเลือกจากความสำคัญของแต่ละระบบงาน

5) สำนักบริหารเทคโนโลยีสารสนเทศและกองวิจัยและพัฒนา ร่วมกันจัดทำแผนการดำเนินงานโครงการ (Project Plan) โดยสรุปข้อกำหนดรายละเอียดขั้นตอนการทำงาน รายละเอียดขั้นตอนการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์

และปริมาณที่ใช้ต้องงาน และอุปกรณ์รักษาความมั่นคงปลอดภัย ระยะเวลาที่ใช้ในการดำเนินการ และประมาณการงบประมาณที่ต้องใช้งาน

6) สำนักบริหารเทคโนโลยีสารสนเทศดำเนินการเสนอขอรับการจัดสรรงบประมาณ ต่อคณะกรรมการประกันสังคม ภายใต้โครงการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน

7) สำนักบริหารเทคโนโลยีสารสนเทศและกองวิจัยและพัฒนา ร่วมกันจัดหาผู้รับผิดชอบการพัฒนาระบบโครงการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน และดำเนินการบริหารโครงการจนเสร็จสิ้น

8) สำนักบริหารเทคโนโลยีสารสนเทศจัดทำนโยบายการเข้าถึงข้อมูลของผู้ใช้งานระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน นโยบายและเงื่อนไขการให้บริการ (Term of service) และนโยบายคุ้มครองข้อมูลส่วนบุคคลของระบบติดตามข้อมูลส่วนบุคคล เพื่อกำหนด ผู้เข้าใช้งานระบบ สิทธิและความรับผิดชอบของผู้ใช้งาน รวมถึงมาตรการในการรักษาความเป็นส่วนตัว

9) สำนักบริหารเทคโนโลยีสารสนเทศจัดอบรมเพื่อชี้แจงแนวทางการใช้งาน และการแก้ไขปัญหาเบื้องต้นของระบบติดตามข้อมูลส่วนบุคคลให้กับเจ้าหน้าที่ของสำนักงานประกันสังคมที่เกี่ยวข้อง เพื่อเตรียมความพร้อมในการให้บริการแก่ผู้ประกันตน

10) ศูนย์สารนิเทศจัดทำแผนประชาสัมพันธ์ ระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน ต่อสาธารณะ

11) สำนักบริหารเทคโนโลยีสารสนเทศติดตามผลการใช้งาน ระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน โดยรวบรวมความเห็นของผู้ใช้งานมาปรับปรุงพัฒนาระบบเป็นระยะ

ผลลัพธ์ที่คาดว่าจะได้รับจากแนวทางพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน สำหรับผู้ประกันตน (เจ้าของข้อมูล) สามารถติดตามการส่งหรือเปิดเผยข้อมูลส่วนบุคคลจากสำนักงานประกันสังคมไปยังบุคคลภายนอกได้โดยสะดวกเป็นปัจจุบัน และมีส่วนร่วมในกระบวนการติดตาม ตรวจสอบ การส่งหรือเปิดเผยข้อมูลส่วนบุคคล ให้เป็นไปตามกฎหมาย สำหรับสำนักงานประกันสังคม ความโปร่งใสเกี่ยวกับกระบวนการส่ง หรือเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก โดยช่วยให้ได้รับความไว้วางใจจากเจ้าของข้อมูล

2.2.4 ปัจจัยที่มีผลกระทบต่อความสำเร็จของการดำเนินการตามข้อเสนอ “แนวทางการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน”

สำนักงานประกันสังคมได้จัดทำแผนปฏิบัติการด้านดิจิทัลสำนักงานประกันสังคม ระยะ 5 ปี (พ.ศ. 2566-2570) แผนฯ ดังกล่าวประกอบไปด้วยโครงการเป็นจำนวนมากที่จะต้องดำเนินการเพื่อพัฒนาระบบทั้งภายในองค์กร ระบบให้บริการภายนอกแก่บุคคลภายนอก เช่นนายจ้าง ผู้ประกันตน ระบบความ

มั่นคงปลอดภัยของระบบสารสนเทศ ตลอดจนโครงสร้างหลักด้านเทคโนโลยีสารสนเทศขององค์กร การดำเนินการตามข้อเสนอ อาจมีความล่าช้า เนื่องจากทรัพยากรบุคลากรของสำนักงานประกันสังคมด้านเทคโนโลยีสารสนเทศมีจำนวนไม่มาก ดังนั้นเพื่อความสำเร็จของการดำเนินการตามข้อเสนอสำนักงานต้องทำการปรับแผนปฏิบัติการด้านดิจิทัลฯ โดยกำหนดให้แนวทางการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตนเป็นภารกิจงานที่ต้องดำเนินการเร่งด่วน

2.3 ภาวะผู้นำเพื่อการขับเคลื่อนข้อเสนอ

ภาวะผู้นำเพื่อการขับเคลื่อนข้อเสนอ เรื่อง **“แนวทางการพัฒนาระบบติดตามและตรวจสอบการใช้ข้อมูลส่วนบุคคลของผู้ประกันตน”** ให้ประสบความสำเร็จประกอบไปด้วยคุณลักษณะสำคัญ ดังนี้

1. การนำทีม ต้องสร้างทีมที่มีความเชี่ยวชาญและมุ่งสู่เป้าหมายร่วมกัน อย่างมีประสิทธิภาพและมีความสมดุลในการทำงานร่วมกัน

2. การวางแผนและบริหารการดำเนินงาน ต้องสามารถวางแผนและบริหารจัดการองค์ความรู้ ระยะเวลา และทรัพยากรอื่นๆ อย่างเหมาะสมเพื่อให้งานดำเนินไปด้วยความสอดคล้องกับเป้าหมายที่กำหนด

3. การสร้างสัมพันธภาพและความไว้วางใจ ต้องสร้างความไว้วางใจและความสัมพันธ์ที่ดีกับผู้ปฏิบัติงานภายในทีมและผู้อื่น ซึ่งจะช่วยส่งเสริมความสัมพันธ์ที่ดีและสร้างบรรยากาศที่กระตุ้นให้ทุกคนทำงานร่วมกันได้เป็นอย่างดี

4. การเรียนรู้และพัฒนา ต้องสนับสนุนการเรียนรู้และพัฒนาทักษะของทีม เพื่อให้ทีมงานสามารถทำงานอย่างมีประสิทธิภาพและเติบโตไปพร้อมกันกับองค์กร

5. การตัดสินใจและแก้ไขปัญหา ต้องตัดสินใจอย่างรวดเร็วและมีเหตุผล และมีการแก้ไขปัญหาได้อย่างมีประสิทธิภาพ คุณลักษณะข้อนี้เป็นสิ่งสำคัญในการนำทีมไปสู่ความสำเร็จ

3. แผนพัฒนาตนเอง

3.1 การวิเคราะห์ตนเอง

ผู้ศึกษาได้ทำการประเมินทักษะที่จำเป็นสำหรับนักบริหารระดับสูง ประกอบไปด้วยทักษะจำนวน 4 กลุ่ม 14 ทักษะ โดยจำแนกเป็น กลุ่มทักษะการรู้คิด (Cognitive Skills) จำนวน 3 ทักษะ กลุ่มทักษะทางสังคมและอารมณ์ (Social and Emotional Skills) จำนวน 3 ทักษะ กลุ่มทักษะการปฏิบัติ (Practical Skill) จำนวน 1 ทักษะ และกลุ่มทักษะด้านภาวะผู้นำ (Leadership Skillset) จำนวน 7 ทักษะ

3. แผนพัฒนาตนเอง

(ข้อมูลส่วนบุคคลไม่เผยแพร่)

บรรณานุกรม

พิธุวรรณ กิติคุณ.//(2567,1 เมย.).// การคุ้มครองข้อมูลส่วนบุคคล.// (https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=103870&filename=Thai_National_Assembly)

ดร.แสงชัย อภิชาตธนพัฒน์ รหัส 590446.//(2567, 1 เมย.).//หลักธรรมาภิบาลในการบริหารองค์กร (**https://www.constitutionalcourt.or.th/occ_web/ewt_dl_link.php?nid=8735)**

Cybersecurity.// (2564,08 june).//CS101ความมั่นคงปลอดภัยไซเบอร์เบื้องต้น.//( )

DEMETER.//(2022,4 april).//เผย 7 ช่องทางสำรวจแก๊งมิจฉาชีพอย่าง Call Center เอาเบอร์โทรศัพท์ของคุณมาจากไหน? พร้อมแนวทางป้องกัน(https://www.dmit.co.th/th/google-workspace-updates-th/7-channels-that-give-info-to-fake-call-center/

DCT.// (2567,01 april).//สรุปสาระสำคัญพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562.// (https://www.dct.or.th/upload/downloads/1612025563SummaryPDPA_DigitalCouncilofThailand.df)

Estonian Information System Authority.// (2024,04/04).// Usage of personal data // (https://www.eesti.ee/en/security-and-defense/safety-and-security/usage-of-personal-data#data-tracker /)

One Fence.// (2023,12 dec).//สถิติส่งท้ายปี ไทยมีเหตุละเมิดข้อมูลส่วนบุคคลแล้ว กว่า 400 เรื่อง.// (https://www.onefence.co/pdpc-privacy-security/)

Pornpilast.su.//(2023,10 มีค.).// ใครต้องรับผิดชอบ?หากเกิดการละเมิดข้อมูลส่วนบุคคล ตามบทบัญญัติของกฎหมาย PDPA.//(https://pdpathailand.com/news-article/responsible-pdpa/)

PPTV Online.//(2567,12 ก.พ.).// แฉกลยุทธ์ใหม่! แก๊งคอลเซ็นเตอร์ หลอกคุย 2 นาที-ดูดเงินได้เกลี้ยงบัญชี.//
(https://www.pptvhd36.com/news/%E0%B8%AA%E0%B8%B1%E0%B8%87%E0%B8%84%E0%B8%A1/216876)

Post today.// (2567,14 ม.ค.).//เปิดผลงาน/เดือน สกัดข้อมูลรั่ว5,000เคส จับผู้ขาย5ราย โทษหนักจำคุก.//
(https://www.posttoday.com/general-news/704425)

PDPACore.// (2021,08 june).//บทลงโทษหากไม่ปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล.//
(https://pdpacore.com/th/blogs/pdpa-penalties)

Pdpathai.com.// (2567,01 april).//การคุ้มครองข้อมูลส่วนบุคคล.//
(https://pdpathailand.com/pdpa/content/article9905.php)

ประวัติผู้เขียนรายงานการศึกษาส่วนบุคคล

นางสาวมุทิตา ชูประดิษฐ์

ประวัติการศึกษา

ปริญญาตรี นิติศาสตร์	มหาวิทยาลัยธรรมศาสตร์ ปี 2538
ปริญญาโท สังคมสงเคราะห์ศาสตร์ สาขาพัฒนาแรงงาน	มหาวิทยาลัยธรรมศาสตร์ ปี 2547

ประสบการณ์การรับราชการ

ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ
ประกันสังคมจังหวัดอุดรธานี
รักษาราชการนักวิชาการเชี่ยวชาญ สำนักเงินสมทบ
เลขานุการกรม
ผู้อำนวยการศูนย์สารนิเทศ

ตำแหน่งหน้าที่ปัจจุบัน

ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ
สำนักงานประกันสังคม
กระทรวงแรงงาน