รับที่ 389
วันที่ 16/03/65
เวลา 09.25 น.

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.
จันที่ 15 มี.ค. 2565
เวลา
เลขรับที่ 1848
☐ กอก. ☑ กยส. ☐ กคร. ☐ กสส.
☐ กทส. ☐ ภตป. ☐ กบ.พ.
วันที่
เวลา
เลขรับที่

ที่ มท๕๔๘๐-๑-๒/๘๗๑๕/๒๕๖๕

การประปานครหลวง
๔๐๐ ถนนประชาชื่น แขวงทุ่งสองห้อง
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

วัน ๑๕ มีนาคม ๒๕๖๕

เรื่อง ขอส่งเอกสารชี้แจ้งเพิ่มเติม งานซื้อโครงการรักษาความปลอดภัยข้อมูลส่วนบุคคล การประปานครหลวง

เรียน คณะกรรมการ การบริหารและจัดหาคอมพิวเตอร์ของกระทรวงมหาดไทย

ตามหนังสือกระทรวงมหาดไทย สำนักงานปลัดกระทรวงมหาดไทย ที่ มท ๐๒๑๐.๕/๘๘๙ ลงวันที่ ๙ มีนาคม ๒๕๖๕ เรื่อง แจ้งผลการประชุมคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ของกระทรวงมหาดไทย ครั้งที่ ๑/๒๕๖๕ ความละเอียดแจ้งแล้วนั้น

การประปานครหลวง ใคร่ขอความเห็นชอบจัดหาระบบคอมพิวเตอร์ดังต่อไปนี้

ตามรายละเอียดเอกสารชี้แจงเพิ่มเติมของโครงการที่ได้แนบมาพร้อมบันทึกนี้

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

(นายภาคภูมิ พิระชัย)
ผู้อำนวยการฝ่ายเทคโนโลยีและสื่อสาร
การประปานครหลวง

ฝ่ายเทคโนโลยีและสื่อสาร
โทร. ๐ ๒๕๐๔ ๐๑๒๓ ต่อ ๑๓๔๒
โทรสาร. ๐ ๒๕๐๐ ๒๘๑๙ ไปรษณีย์อิเล็กทรอนิกส์: saraban@mwa.co.th

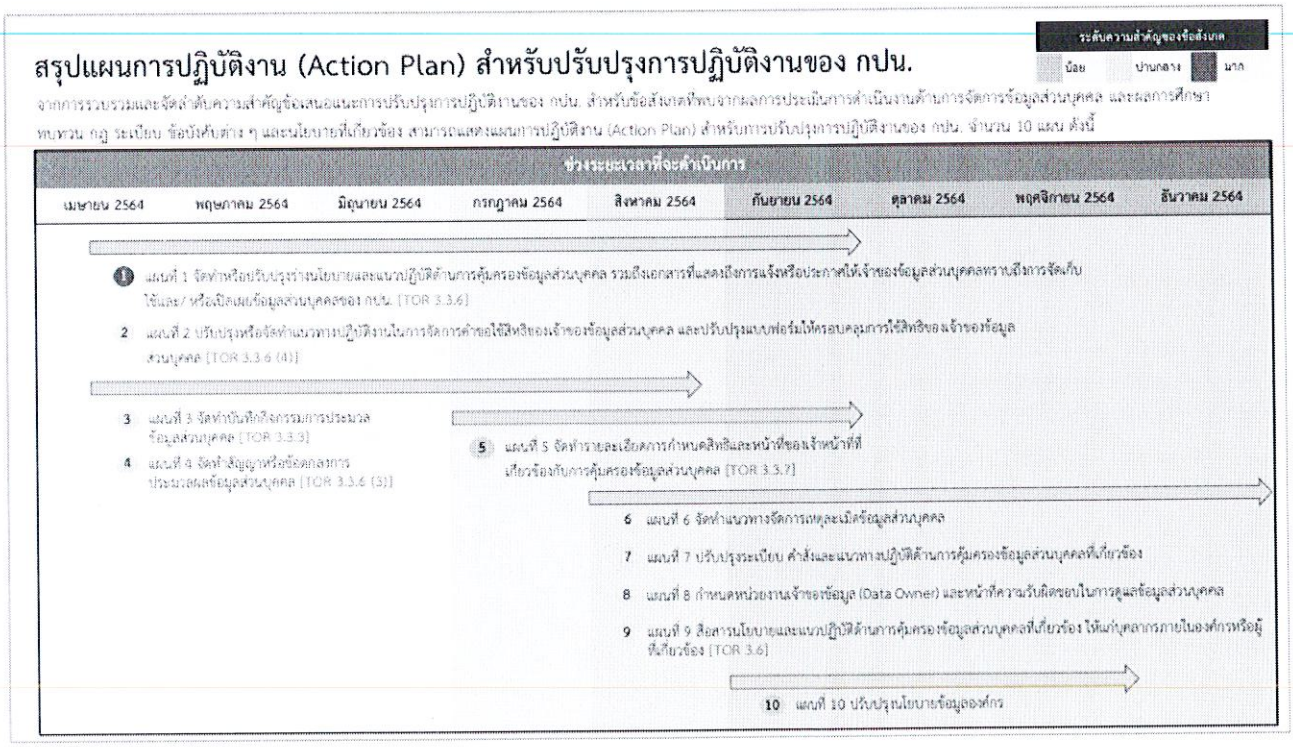
คำชี้แจงเพิ่มเติมโครงการรักษาความปลอดภัยข้อมูลส่วนบุคคล การประปานครหลวง

๑. การปรับปรุงการปฏิบัติงานของ กปน. ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ที่ผ่านมา กปน. มีโครงการเตรียมความพร้อมการดำเนินงานของการประปานครหลวงให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) โดยจ้างที่ปรึกษาเพื่อการดำเนินการ ปรับปรุงการปฏิบัติงานการทำงานของ กปน. เป็นไปตามพระราชบัญญัติ ลงนามสัญญาจ้างเมื่อวันที่ ๒ เมษายน ๒๕๖๔ โดยมีรายละเอียดการดำเนินการของที่ปรึกษาดังนี้

- ศึกษา และวิเคราะห์โครงสร้างองค์กร บทบาทหน้าที่ ความรับผิดชอบ สายการรายงาน และการสื่อสารในปัจจุบันของหน่วยงานภายใน กปน. ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
- ศึกษา และวิเคราะห์แนวทางการกำหนดโครงสร้าง บทบาทหน้าที่ และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรวมถึงผู้มีส่วนเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และแนวปฏิบัติที่ดี
- จัดทำโครงสร้างการกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล บทบาทหน้าที่ และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรวมถึงผู้มีส่วนเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
- เพื่อให้เหมาะสมกับการดำเนินงานของ กปน. กำหนดบทบาท และ ความเชื่อมโยงในแต่ละกิจกรรมของผู้ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

จากการรวบรวมและจัดลำดับความสำคัญข้อเสนอแนะการปรับปรุงการปฏิบัติงานของ กปน. สำหรับข้อสังเกตที่พบจากการประเมินการดำเนินการจัดการข้อมูลส่วนบุคคล และผลการศึกษา ทบทวน กฎ ระเบียบข้อบังคับต่างๆ และนโยบายที่เกี่ยวข้อง สามารถแสดงแผนการปฏิบัติงาน (Action Plan) สำหรับการปรับปรุงการปฏิบัติงานของ กปน. ในปีงบประมาณ ๒๕๖๔ จำนวน ๑๐ แผนงานดังภาพ



ในปีงบประมาณ ๒๕๖๕ มีการกำหนดแผนงานจำนวน ๓ แผนงาน ได้แก่

แผนงานที่ ๑ : โครงการรักษาความปลอดภัยข้อมูลส่วนบุคคล รายละเอียดโครงการ เพื่อให้เป็นไปตามแผนงานที่ ๗ ของปีงบประมาณ ๒๕๖๔ ปรับปรุงระเบียบ คำสั่งและแนวทางปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง และ มาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์เพิ่มเติม โดยจัดหาระบบ Data Masking / Encryption

แผนงานที่ ๒ : เช่าใช้ระบบการบริหารจัดการความยินยอม (ระบบ Consent Management) ลงนามสัญญาเมื่อวันที่ ๑๐ มี.ค. ๖๕

แผนงานที่ ๓ : ติดตามการดำเนินงานตาม พรบ.คุ้มครองข้อมูลส่วนบุคคลปี ๒๕๖๒ ปรับปรุงตามข้อเสนอแนะของที่ปรึกษา

ผลการดำเนินงาน ตามแผนปฏิบัติการ (Action Plan) การปรับปรุงการปฏิบัติงานของ กปน. ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

รายละเอียดตามแผนปฏิบัติการ	สถานะ
แผนที่ ๑ จัดทำหรือปรับปรุงร่างนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล รวมถึงเอกสารที่แสดงถึงการแจ้งหรือประกาศให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการจัดเก็บใช้และ/หรือเปิดเผยข้อมูลส่วนบุคคลของ กปน.	เริ่มจัดทำ เม.ย. ๖๔ เสร็จสิ้นในเดือน กย. ๖๔
แผนที่ ๒ ปรับปรุงหรือ จัดทำแนวทางปฏิบัติงานในการจัดการคำขอให้สิทธิของเจ้าของข้อมูลส่วนบุคคล และปรับปรุงแบบฟอร์มให้ครอบคลุมการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล **หมายเหตุ** - กปน. เช่าใช้ระบบการบริหารจัดการความยินยอม (ระบบ Consent Management) ลงนามสัญญาเมื่อวันที่ ๑๐ มี.ค. ๖๕	เริ่ม เม.ย. ๖๔ เสร็จสิ้น ต.ค. ๖๔
แผนที่ ๓ จัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล	เริ่ม เม.ย. ๖๔ เสร็จสิ้น ส.ค. ๖๔
แผนที่ ๔ จัดทำสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคล	เริ่ม เม.ย. ๖๔ เสร็จสิ้น ส.ค. ๖๔
แผนที่ ๕ จัดทำรายละเอียดการกำหนดสิทธิและ หน้าที่ของเจ้าหน้าที่ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล	เริ่ม ก.ค. ๖๔ เสร็จสิ้น ก.ย. ๖๔
แผนที่ ๖ จัดทำแนวทางจัดการเหตุละเมิดข้อมูลส่วนบุคคล **หมายเหตุ** การจัดทำแนวทางจัดการเหตุละเมิดข้อมูลส่วนบุคคล รอพิจารณามาตรการเยียวยา	เริ่ม ส.ค. ๖๔ เสร็จสิ้น ก.ย. ๖๔

รายละเอียดตามแผนปฏิบัติการ	สถานะ
แผนที่ ๗ ปรับปรุงระเบียบ คำสั่งและแนวทาง ปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง **หมายเหตุ** มาตรการรักษาความปลอดภัยในการเก็บรักษาข้อมูลในรูปแบบอิเล็กทรอนิกส์เพิ่มเติม **- กปน. จัดซื้อโครงการรักษาความปลอดภัยข้อมูลส่วนบุคคล** (จัดหาระบบ Data Masking / Encryption) ในปีงบประมาณ ๒๕๖๕ - กปน. จะดำเนินการในอนาคตจัดหาระบบ Data Loss Prevention (DLP) เพื่อป้องกันข้อมูลส่วนบุคคลรั่วไหล	เริ่ม ส.ค. ๖๔ เสร็จสิ้น ต.ค. ๖๔ มีแผนดำเนินการในปี ๒๕๖๖
แผนที่ ๘ กำหนดหน่วยงานเจ้าของข้อมูล (Data Owner) และหน้าที่ความรับผิดชอบในการดูแลข้อมูลส่วนบุคคล	เริ่ม ส.ค. ๖๔ เสร็จสิ้น ธ.ค. ๖๔
แผนที่ ๙ สื่อสารนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง ให้แก่ บุคลากรภายในองค์กรหรือผู้ที่เกี่ยวข้อง	เริ่ม ส.ค. ๖๔ เสร็จสิ้น ธ.ค. ๖๔
แผนที่ ๑๐ ปรับปรุงนโยบายข้อมูลองค์กร **หมายเหตุ** - ติดตามการดำเนินงานตาม พรบ.คุ้มครองข้อมูลส่วนบุคคลปี ๒๕๖๒ ปรับปรุงตามข้อเสนอแนะของที่ปรึกษา - ปรับปรุงนโยบายข้อมูลองค์กร ซึ่งจะนำเข้าคณะ Data Gov, Council พิจารณาในวันที่ ๒๓ มี.ค. ๖๕ เพื่อขอความเห็นชอบ นโยบายต่างๆ ดังนี้ - Data Policy - Data Privacy Policy - Privacy Notice ประกาศความเป็นส่วนตัว หลังจาก ได้รับความเห็นชอบ จึงประกาศใช้นโยบายต่อไป	เริ่ม ก.ย. ๖๔ เสร็จสิ้น ธ.ค. ๖๔

๒. การซื้อ Advanced Security ของ Oracle สำหรับระบบ CIS ครั้งนี้ เป็นการป้องกัน Cyber Security อย่างไร นอกจากเรื่อง PDPA

เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ กปน. ซึ่งครอบคลุมถึงป้องกันการรั่วไหลของข้อมูล หากสามารถนำข้อมูลออกไปนอกองค์กรได้โดยไม่ได้รับอนุญาต ก็ไม่สามารถเข้าถึงข้อมูลได้ และไม่สามารถนำไปใช้ประโยชน์ต่อได้

มาตรการรักษาความปลอดภัยในการเข้าถึงข้อมูลส่วนบุคคล

การควบคุมการเข้าถึงข้อมูลและอุปกรณ์จัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

Administrative Safeguard

- มาตรการควบคุมการเข้าถึงข้อมูลในระบบ (ISO๒๗๐๐๑:๒๐๑๓ User Access Policy และ Physical Entry Control Policy)

Technical Safeguard

- กำหนด Privilege และ Permission เฉพาะผู้ได้รับอนุญาตเท่านั้น

Physical Safeguard

- ลงนามก่อนเข้า DC/DR
- มี Access Control ก่อนเข้า DC/DR
- การใช้วิธียืนยันแบบ ๒-factor

๓. ถ้าเกิดเหตุข้อมูลส่วนบุคคลของลูกค้ารั่วไหล โปรแกรมที่จะซื้อครั้งนี้จะช่วยให้ กปน ปฏิบัติตามกฎหมายอะไรได้บ้าง

กปน. มีการปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ กปน. ให้ครอบคลุมรายละเอียดด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง หากข้อมูลมีการรั่วไหล ก็ไม่สามารถเข้าถึงข้อมูลได้

๔. ค่าดำเนินการติดตั้งระบบโครงการรักษาความปลอดภัยข้อมูลส่วนบุคคล โดยผู้เชี่ยวชาญ ระยะเวลาดำเนินการ ๙๐ วัน

ขอบเขตโดยสรุปประกอบด้วย

- งานติดตั้งซอฟต์แวร์

๑. ติดตั้งระบบซอฟต์แวร์ Oracle Advance Security Option บน Production Zone

๒. ติดตั้งระบบซอฟต์แวร์ Oracle Advance Security Option บน DMZ Zone

๓. ติดตั้งระบบซอฟต์แวร์ Oracle Data Masking and Subsetting บน Production Zone

๔. ติดตั้งระบบซอฟต์แวร์ Oracle Data Masking and Subsetting บน DMZ Zone

๕. อัพเกรดระบบฐานข้อมูล Oracle DB ๑๑g จาก Standard Edition to Enterprise Edition

- งานสำรวจและจัดทำรายละเอียดข้อมูลส่วนบุคคล
- งานออกแบบวิธีการ Encryption, Redaction, Masking

ตารางจำแนกค่าดำเนินการงานติดตั้ง, ออกแบบและสำรวจระบบป้องกันข้อมูลส่วนบุคคล โดยผู้เชี่ยวชาญดังนี้

ลำดับ	ตำแหน่ง	จำนวน (คน)	Manday (วัน)	การมีส่วนร่วมในโครงการ	Manrate (บาท/วัน)	รวม (บาท)
๑	Project Manaager	๑	๔๕	๕๐%	๒๐,๕๐๐	๙๒๒,๕๐๐
๒	Project Co-ordinator	๑	๔๕	๕๐%	๑๗,๒๐๐	๗๗๔,๐๐๐
๓	Business Analysis	๒	๕๔	๓๐%	๑๕,๕๐๐	๘๓๗,๐๐๐
๔	Database Administrator	๒	๑๓๕	๗๕%	๑๓,๐๐๐	๑,๗๕๕,๐๐๐
๕	System Engineer	๒	๒๗	๑๕%	๑๐,๐๐๐	๒๗๐,๐๐๐
			๓๐๖		**รวมทั้งหมด**	๔,๕๕๘,๕๐๐