Announcement of Global Power Synergy Public Company Limited

No. 014/ 21

Subject: GPSC PDPA Management Guideline (PDPA Management)

1. Objective

1.1 In order for Global Power Synergy Public Company Limited and Glow Energy Public Company Limited (GPSC Group) to possess standards and best practices for handling personal information and for these to be in accordance with the Personal Data Protection Act B.E. 2562 (2019) (Personal Data Protection Act) as well as other relevant laws, including the privacy policy of the GPSC Group

1.2 To prevent damages from the risk of non-compliance with applicable laws and regulations

1.3 In order for GPSC Group personnel to know their roles and duties, while having strict guidelines for adherence to performance

2. Scope of this guideline

This guideline applies to GPSC group personnel, including executives, employees of all levels of the GPSC group and includes employees of companies that hold GPSC shares and come to work with the Company as the secondment of the GPSC Group, who are the personal data controllers (Data Controller) and personal data processors (Data Processor).

3. Guidelines

3.1 Obtaining Personal Information

When each segment receives personal information directly from the data subject, regardless of the legal basis, each department shall notify the subject of that collection, including the intended use of the personal data by informing the data subject, by any means, as well as to study and understand the privacy policies available on the GPSC group website.

The GPSC Group, as a business entity, which relies on the data acquisition lawful bases for collection, usage or disclosure of personal data is required by law to adhere to the following:

1) Consent
2) Contract
3) Legal obligation

4) Vital interest

5) Legitimate interests

The nature of activities and objectives of each department in determining the data acquisition base are identified in the GPSC Group's Data Inventory. However, if any department wishes to add information in the data inventory, division of Corporate Governance and Compliance (GGM) must be notified to consider and revise such databases.

In the event that personal data is under the consent base, each department must define guidelines (sub-procedures) to support the process of obtaining consent from the data subject, which includes the methods and the person responsible for logging into the OneTrust system.

3.2 Use of personal information

Use as specified in the privacy policy of the company, only or to the extent required by law, shall not be used other than for the purpose as stated to the GPSC Group.

In the event that personal data is under the consent base, each department must define guidelines (sub-procedures) to support the intended use process, which must identify the responsible person, the frequency and procedure for data acquisition from the OneTrust system for review purposes without the consent of the data subject, and the non-consenting data handling practices that have been established, which will not be used.

3.3 Handling of processors of personal data

All departments shall determine a method for determining the nature of the activities or services that are transacted with business partners, whether they are in connection with the collection, usage or disclosure of personal information as directed by, or on behalf of the GPSC Group or activities or services not during the procurement process.

In the case of hiring a personal data processor to do so, such a partner shall sign an attachment to a contract or any other document that can indicate that the personal data processor's responsibility is identified as required by law.

In the event that the department responsible for the handling of personal information is required to provide services under the Shared Service Agreement to affiliates, the practice set out in the department shall also apply to the shared service for affiliated companies.

3.4 Handling the exercise of the data subject rights

The related departments must establish guidelines (sub-procedures) to support the exercise of the right of data subjects as stipulated by law, with the representative being responsible for monitoring and reporting of the results of the request through the OneTrust system, methods for determining the conditions of exercise and the approval of the action.

In addition, all departments are required to cooperate in requesting the exercise of the data subject's rights if requested by the relevant departments.

The responsible department is required to report results whether or not to approve or disapprove of the claim of the data subject within 30 days from the date of receipt of the matter.

3.5 Violation and non-compliance incident management

GPSC's Regulations on Information and Communication Technology Policy Standard Practice (GGM) is the central agency to receive reports of infringement from both internal and external agencies and after considering the infringement, will notify the matter to the relevant departments to proceed through the OneTrust system. The project owner must complete the investigation, along with reporting and identifying the root cause within 48 hours in order to report the effects on the division of GGM, to propose such to the Corporate Governance Committee and the Chief Executive Officer and President to consider and approve the report of violations and actions to the supervisory authority within 72 hours from the date of receipt of the matter.

In order to strictly comply with the law, the GGM can organize an urgent meeting, in order to determine the emergency working group, the subject owner and related departments that must cooperate and prioritize the management of this breach as an important task.

3.6 Determination of the period of retention and destruction of information;

The related department must establish guidelines (sub-procedures) to cover the storage period of the responsible person and stipulate the frequency of verification of the received personal information including processes for destroying any unused information or the expiration of the storage period.

The maximum storage period as set out in the Privacy Policy is not more than 10 years from the end of the legal relationship with each segment that may be specified less than the specified time, taking into account other relevant laws.

3.7 Data inventory updates

Do not use personal information other than for the purposes specified in the Data Inventory in the OneTrust system. In the event of any changes or additions to the purpose of use of personal information, the person responsible for the data shall notify the division of Corporate Governance and Compliance (GGM) to rectify the information.

In addition, the division of GGM will provide annual reviews of the content of the Data Inventory, with the department responsible for reviewing, revising, or verifying the information within a specified period of time.

3.8 Security of personal information

Personnel of the GPSC Group are required to comply with the GPSC's Regulations on Information and Communication Technology Policy Standard Practice.

In addition, personnel of the GPSC Group must take actions in accordance with the Personal Data Protection Act, which are defined as follows:

1) GPSC Group personnel must comply with the data access requirements in their own right for the use, disclosure and processing of personal data. This is in accordance with the procedures specified in the GPSC's Regulations on Information and Communication Technology Policy Standard Practice.

2) GPSC Group personnel are required to keep information secure, must not alter, modify, transfer or disclose other than those stated for the purpose of use in accordance with the privacy policy.

3.9 Reporting to the Privacy Committee and the Management Committee

the division of Corporate Governance and Compliance (GGM) section reports annual performance to the Corporate Governance Committee on matters such as compliance with related policies, non-consent transaction management, data subject rights management, infringement management etc.

If there is an important issue that affects the image of the GPSC Group, the Corporate Governance Committee can propose matters to the Management Committee on an agenda basis or as urgently, as the case may be.

ประกาศบริษัท โกลบอล เพาเวอร์ ซินเนอร์ยี่ จำกัด (มหาชน)

ที่ 014 / 64

เรื่อง แนวปฏิบัติการจัดการข้อมูลส่วนบุคคล (PDPA Management)

1. วัตถุประสงค์

1.1 เพื่อให้บริษัท โกลบอล เพาเวอร์ ซินเนอร์ยี่ จำกัด (มหาชน) และบริษัท โกลว์ พลังงาน จำกัด (มหาชน) (กลุ่ม GPSC) มีมาตรฐานแนวทางปฏิบัติเกี่ยวกับการจัดการข้อมูลส่วนบุคคล และเป็นไปตามที่บัญญัติไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ) รวมถึงกฎหมายอื่น ๆ ที่เกี่ยวข้อง รวมถึงนโยบายความเป็นส่วนตัวของกลุ่มGPSC

1.2 เพื่อป้องกันความเสียหายจากความเสี่ยงของการไม่ปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง

1.3 เพื่อให้บุคลากรของกลุ่ม GPSC ทราบถึงบทบาทหน้าที่ของตนเอง และมีแนวทางปฏิบัติให้ยึดมั่นในการปฏิบัติงานอย่างเคร่งครัด

2. ขอบเขต

แนวปฏิบัตินี้ใช้บังคับกับบุคลากรของกลุ่ม GPSC ซึ่งหมายรวมถึง ผู้บริหาร พนักงาน ลูกจ้าง ทุกระดับของกลุ่ม GPSC และให้หมายรวมถึงพนักงานของบริษัทที่ถือหุ้นกลุ่ม GPSC และมาปฏิบัติงานกับบริษัทฯ ในฐานะ Secondment ของกลุ่ม GPSC ที่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

3. แนวปฏิบัติ

3.1 การได้มาซึ่งข้อมูลส่วนบุคคล

เมื่อแต่ละส่วนงานได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง ไม่ว่าจะเป็นการรวบรวมด้วยฐานกฎหมายใดก็ตาม แต่ละส่วนงานจะต้องแจ้งการเก็บรวบรวมนั้น รวมถึงวัตถุประสงค์การใช้งานต่อเจ้าของข้อมูลส่วนบุคคล โดยแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบโดยวิธีการใดวิธีการหนึ่ง ในการเข้าไปศึกษาและทำความเข้าใจนโยบายความเป็นส่วนตัว ที่อยู่บนเว็ปไซต์ของกลุ่ม GPSC

กลุ่ม GPSC ในฐานะนิติบุคคลที่ดำเนินธุรกิจ อาศัยฐานการได้มาซึ่งข้อมูลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามที่กฎหมายกำหนด ดังนี้

1) ฐานความยินยอม
2) ฐานการปฏิบัติตามสัญญา
3) ฐานการปฏิบัติตามกฎหมาย
4) ฐานเพื่อป้องกันอันตรายต่อชีวิตและร่างกาย
5) ฐานเพื่อประโยชน์อันชอบด้วยกฎหมาย

ลักษณะของกิจกรรมและวัตถุประสงค์ของแต่ละส่วนงาน ในการกำหนดฐานการได้มาของข้อมูลถูกระบุอยู่ใน Data Inventory ของกลุ่ม GPSC ทั้งนี้ หากส่วนงานใดมีความประสงค์จะเพิ่มเติมข้อมูลใน Data Inventory ให้ดำเนินการแจ้งส่วนกำกับกฎหมายและกฎระเบียบองค์กร (GGM) เพื่อพิจารณาและดำเนินการแก้ไขปรับปรุงฐานข้อมูลดังกล่าว

กรณีเข้าข่ายฐานความยินยอม แต่ละส่วนงานจะต้องกำหนดแนวปฏิบัติ (Sub-Procedure) เพื่อรองรับกระบวนการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ซึ่งหมายรวมถึงวิธีการและผู้รับผิดชอบในการบันทึกเข้าระบบ OneTrust

3.2 การนำข้อมูลส่วนบุคคลไปใช้

ให้ใช้ได้เท่าที่กำหนดไว้ในนโยบายความเป็นส่วนตัวของบริษัทฯ เท่านั้น หรือเท่าที่กฎหมายกำหนดไว้ ห้ามใช้นอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับกลุ่ม GPSC

กรณีเข้าข่ายฐานความยินยอม แต่ละส่วนงานจะต้องกำหนดแนวปฏิบัติ (Sub-Procedure) เพื่อรองรับกระบวนการการใช้งานตามวัตถุประสงค์ซึ่งจะต้องระบุถึงผู้รับผิดชอบ ความถี่ และขั้นตอนการนำข้อมูลจากระบบ OneTrust มาตรวจสอบวัตถุประสงค์ที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และมีการกำหนดแนวทางการจัดการกับข้อมูลที่ไม่ได้รับความยินยอม ซึ่งจะไม่นำข้อมูลดังกล่าวไปใช้

3.3 การจัดการผู้ประมวลผลข้อมูลส่วนบุคคล

ทุกส่วนงานจะต้องกำหนดวิธีการพิจารณาลักษณะกิจกรรมหรือบริการที่มีธุรกรรมกับคู่ค้า ว่าเข้าข่ายการดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของกลุ่ม GPSC หรือไม่ ในกระบวนการจัดซื้อจัดจ้าง

กรณีเข้าข่ายเป็นการจ้างผู้ประมวลผลข้อมูลส่วนบุคคล ให้ดำเนินการให้คู่ค้าดังกล่าวลงนามในเอกสารแนบท้ายสัญญา หรือกเอกสารอื่นใดที่แสดงได้ว่า มีการระบุความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

กรณีที่ส่วนงานที่รับผิดชอบเกี่ยวกับการจัดการข้อมูลส่วนบุคคล จะต้องจัดทำบริการภายใต้สัญญา Shared Service Agreement ให้กับบริษัทในเครือ ให้นำแนวปฏิบัติที่กำหนดไว้ในส่วนงาน มาบังคับใช้กับการบริการ Shared Service ให้บริษัทในเครือด้วย

3.4 การจัดการการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ส่วนงานที่เกี่ยวข้องจะต้องกำหนดแนวปฏิบัติ (Sub-Procedure) เพื่อรองรับการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด โดยมีการกำหนดตัวแทนผู้รับผิดชอบในการติดตามและแจ้งผลการร้องขอผ่านระบบ OneTrust วิธีการพิจารณาเงื่อนไขในการใช้สิทธิ และผู้อนุมัติการดำเนินการ

นอกจากนี้ ทุกส่วนงานจะต้องให้ความร่วมมือในการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลหากมีการร้องขอจากส่วนงานที่เกี่ยวข้อง

ส่วนงานที่รับผิดชอบ จะต้องแจ้งผลไม่ว่าจะอนุมัติหรือไม่อนุมัติคำร้องต่อเจ้าของข้อมูลส่วนบุคคล ภายใน 30 วัน นับแต่วันที่ได้รับเรื่อง

3.5 การจัดการเหตุละเมิด

ส่วนกำกับกฎหมายและกฎระเบียบองค์กร (GGM) จะเป็นหน่วยงานกลางในการรับเรื่องการแจ้งเหตุละเมิด ทั้งจากหน่วยงานภายในและบุคคลภายนอก และภายหลังจากพิจารณาเหตุละเมิดแล้ว จะแจ้งเรื่องไปให้ส่วนงานที่เกี่ยวข้องเพื่อดำเนินการผ่านระบบ OneTrust ซึ่งส่วนงานเจ้าของเรื่อง จะต้องดำเนินการตรวจสอบรายงาน และระบุสาเหตุ (Root Cause)ให้แล้วเสร็จภายใน 48 ชั่วโมง เพื่อแจ้งผลต่อส่วนกำกับกฎหมายและกฎระเบียบองค์กร (GGM) เพื่อดำเนินการเสนอคณะกรรมการกำกับดูแลการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่พิจารณาอนุมัติในแจ้งเหตุละเมิดและผลการดำเนินการต่อหน่วยงานกำกับดูแล ภายใน 72 ชั่วโมง นับแต่วันที่ได้รับเรื่อง

ทั้งนี้เพื่อให้เป็นการปฏิบัติตามกฎหมายอย่างเคร่งครัด ส่วนกำกับกฎหมายและกฎระเบียบองค์กร (GGM) สามารถจัดประชุมเป็นการด่วน เพื่อกำหนดคณะทำงานฉุกเฉินได้ โดยส่วนงานเจ้าของเรื่องและส่วนงานที่เกี่ยวข้องจะต้องให้ความร่วมมือและจัดลำดับการจัดการเหตุละเมิดนี้เป็นงานสำคัญ

3.6 การกำหนดระยะเวลาการจัดเก็บข้อมูลและการทำลายข้อมูล

ส่วนงานที่เกี่ยวข้องจะต้องกำหนดแนวปฏิบัติ (Sub-Procedure) ให้ครอบคลุมถึงระยะเวลาการจัดเก็บข้อมูล ผู้รับผิดชอบและกำหนดความถี่ในการตรวจสอบข้อมูลส่วนบุคคลที่ได้รับมา และรวมถึงกระบวนการทำลายข้อมูลที่ไม่ใช้แล้วหรือพ้นกำหนดระยะเวลาการจัดเก็บ

ทั้งนี้ ระยะเวลาการจัดเก็บสูงสุดตามที่กำหนดไว้ในนโยบายความเป็นส่วนตัว คือ ไม่เกินระยะเวลา 10 ปีนับแต่สิ้นสุดนิติสัมพันธ์ โดยแต่ละส่วนงานอาจกำหนดให้ต่ำกว่าระยะเวลาที่กำหนดไว้ได้ โดยให้คำนึงถึงกฎหมายอื่น ๆ ที่เกี่ยวข้องด้วย

3.7 การปรับปรุง Data Inventory

ห้ามใช้ข้อมูลส่วนบุคคลนอกเหนือจากวัตถุประสงค์ที่กำหนดไว้ใน Data Inventory ในระบบ OneTrust กรณีมีการเปลี่ยนแปลงหรือเพิ่มเติมวัตถุประสงค์การใช้งานข้อมูลส่วนบุคคล ให้เจ้าของส่วนงานแจ้งส่วนกำกับกฎหมายและกฎระเบียบองค์กร (GGM) เพื่อดำเนินการแก้ไขข้อมูล

นอกจากนี้ ส่วนกำกับกฎหมายและกฎระเบียบองค์กร (GGM) จะจัดให้มีการทบทวนเนื้อหาใน Data Inventory เป็นประจำทุกปี โดยให้ส่วนงานที่รับผิดชอบทบทวน แก้ไข หรือยืนยันข้อมูล ภายในระยะเวลาที่กำหนด

3.8 การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

บุคลากรของกลุ่ม GPSC จะต้องปฏิบัติตามข้อกำหนด GPSC ว่าด้วย มาตรฐานการปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร

นอกจากนี้ ให้บุคลากรของกลุ่ม GPSC ดำเนินการตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ กำหนดไว้ ดังนี้

1) บุคลากรของกลุ่ม GPSC จะต้องปฏิบัติตามข้อกำหนดในการเข้าถึงข้อมูลตามสิทธิของตนเอง สำหรับการใช้ การเปิดเผย การประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ให้เป็นไปตามขั้นตอนที่ระบุในข้อกำหนด GPSC ว่าด้วย มาตรฐานการปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร

2) บุคลากรของกลุ่ม GPSC จะต้องรักษาความปลอดภัยของข้อมูล ห้ามเปลี่ยนแปลงแก้ไข โอนย้าย หรือเปิดเผย นอกเหนือไปจากที่ได้ระบุไว้ตามวัตถุประสงค์การใช้งานตามนโยบายความเป็นส่วนตัว

3.9 การรายงานต่อคณะกรรมการกำกับดูแลการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Privacy Committee) และคณะกรรมการการจัดการ (Management Committee)

ส่วนกำกับกฎหมายและกฎระเบียบองค์กร (GGM) มีหน้าที่รายงานผลการดำเนินงานประจำปีต่อคณะกรรมการกำกับดูแลการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ในเรื่องต่างๆ เช่น การปฏิบัติตามนโยบายที่เกี่ยวข้อง การจัดการรายการที่ไม่ให้ความยินยอม การจัดการการใช้สิทธิของเจ้าของข้อมูล การจัดการเหตุละเมิด เป็นต้น

ทั้งนี้หากมีประเด็นที่มีความสำคัญและมีผลกระทบต่อภาพลักษณ์ของกลุ่ม GPSC คณะกรรมการกำกับดูแลการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล สามารถเสนอเรื่องต่อคณะกรรมการการจัดการได้ตามวาระหรือเป็นการด่วนแล้วแต่กรณี

แนวปฏิบัตินี้มีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน 2564 เป็นต้นไป

ประกาศ ณ วันที่ 31 พฤษภาคม 2564

.....

(นายศิริเมธ ลี้ภากรณ์)
ประธานคณะกรรมการกำกับดูแลการปฏิบัติตามกฎหมาย
ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล