Personal Data Protection

Policy and Guidelines

Siam Land Flying Co., Ltd.

Contents

Personal Data Protection Policy and Guidelines

Siam Land Flying Co., Ltd.

1. Intent

Siam Land Flying (SLF) respects and values the human right to the protection of Personal Data owned by all directors, management, staff, customers, suppliers and business partners. Thus, SLF shall protect all Personal Data from possible misuse, and maintain such data security based on international laws and standards.

2. Scope

This Personal Data Protection Policy and Guidelines apply to Charoen Pokphand Group, (hereafter "the Group") which includes Charoen Pokphand Group Co., Ltd., and all of its subsidiary companies. The term "company" hereafter refers to any such company individually that has adopted this Personal Data Protection Policy and Guidelines. This document shall be reviewed at least once a year, or as conditions require.

3. Objectives

3.1 To ensure the security, reliability and protection of Personal Data owned by all directors, management, staff, customers, suppliers and business partners in every transaction with SLF.

3.2 To prevent the damage caused by misuse of Personal Data, as well as misuse of such data for monetary gain

4. Roles and Responsibilities

4.1 Board of Directors

4.1.1 Ensure that the Personal Data Protection Policy and Guidelines are in place.

4.1.2 Ensure that the policy and guidelines are properly implemented.

4.2 Management

4.2.1 Establish rules and procedures to suit the nature of the business, while remaining consistent with the Policy and Guidelines, relevant local data

protection laws where the company operates, and international data protection standards.

4.2.2 Ensure that the organizational structure and related functions are in place.

4.2.3 Ensure there are selection procedures when hiring third parties with standardized data protection systems to handle Personal Data on behalf of the company.

4.2.4 Monitor the effective implementation of policy, guidelines, and regulations and identify areas for improvement, in addition to ensuring regular performance reports related to this Policy and Guidelines.

4.3 Data Protection Officer

4.3.1 Monitor and review the processing of Personal Data by the company to ensure compliance with the relevant data privacy laws, including to arrange awareness campaigns and training programs on the proper usage of Personal Data.

4.3.2 Advise and recommend the Board of Directors, management, and staff on the proper usage of Personal Data under the relevant local data protection laws.

4.3.3 Serve as the contact point for issues related to Personal Data and protection of the rights of data subjects, including coordinating and cooperating with the Office of the Personal Data Protection Commission.

4.3.4 Ensure the confidentiality of Personal Data obtained over the course of performing their duties.

4.4 Staff

4.4.1 Handle Personal Data with care, as well as maintain strict compliance with the relevant laws, rules and regulations.

4.4.2 Notify the Data Protection Officer in collecting Personal Data immediately in the event of any data breach

4.4.3 Notify the company through the relevant whistleblowing channels, if any failure to comply with this policy is found.

5. Guidelines

5.1 Collection of Personal Data

5.1.1 Collect Personal Data only according to the purpose notified to the Data Subject.

5.1.2 Do not collect Sensitive Personal Data that may cause discrimination or unfair bias to the data subject without their explicit consent, except if it is controlled under the law.

5.2 Storage of Personal Data

5.2.1 Security measures are required for all Personal Data storage locations to prevent the unauthorized access, use, modification, and disposal of said data, as well as to prevent Personal Data leak threats.

5.2.2 All Personal Data storage locations, including internal and Third-Parties, must have internationally-accepted data protection systems, and must only store Personal Data as appropriate for their intended usage in compliance with the relevant local data protection laws.

5.3 Transfer of Personal Data

5.3.1 Transfers of Personal Data require the consent or request to transfer from the Data Subject.

5.3.2 Transfers of Personal Data to a destination country are permitted under any of the following conditions:

1) The Data Subject has provided consent on the transfer and has been informed that the data protection standards at the destination country may be inadequate.
2) The Data Subject has requested the data transfer, or meets an obligation to a contract in which the Data Subject is a party.
3) The Data Subject is incapable of giving their consent, but the data transfer is necessary to prevent or suppress danger to the life, body, or health of the data subject.

5.4 Data Subject Rights

5.4.1 The Data Subject has the right to access or request a copy of their Personal Data.

5.4.2 The Data Subject has the right to request information on how their Personal Data was collected if no consent was provided.

5.4.3 The Data Subject has the right to notify the company in order to modify or change their Personal Data if they are inaccurate.

5.4.4 The Data Subject has the right to delete or destroy their Personal Data, or request the anonymization of the data, in accordance with relevant local data protection laws.

5.4.5 The Data Subject has the right to request the transfer of their Personal Data from one data controller to another controller.

5.4.6 The Data Subject has the right to restrict the usage of their Personal Data, in accordance with relevant local data protection laws.

5.4.7 The Data Subject has the right to object to the collection, usage or disclosure of their Personal Data.

5.4.8 The Data Subject has the right to file a complaint if the data usage is found to have infringed the stated purpose of collection.

5.5 Use or Disclosure of Personal Data

5.5.1 Do not use or disclose Personal Data that is different from the purposes set out by this Policy, in addition to disclosing to third parties, except if it is permitted under relevant local data protection laws.

5.5.2 All internal and Third Parties are prohibited from using Personal Data for illegal purposes, and must strictly adhere to guidelines contained in this Policy, including relevant local data protection laws in respective countries where SLF operates.

5.6 Disposal of Personal Data

5.6.1 In the event where stored Personal Data is not relevant or finished serving its purpose, or if the Data Subject has objected to or withdrew consent to the processing of their Personal Data, the said data shall be securely disposed of to prevent any potential data leakage.

5.6.2 Dispose and delete any stored Personal Data once the usage period has expired as initially agreed in the purpose of collection, except if required to comply with the relevant local data protection laws

5.7 Control of Personal Data

As a Data Controller, SLF must ensure the proper use of Personal Data by complying and applying the following data protection principles set out below:

1) The Data Subject is informed of the purpose of collecting their Personal Data, as well as their terms and rights, including to request their consent (if any) prior to collection, processing or disclosure.
2) Personal Data are collected, processed, and disclosed only as specified in the purpose notified to the Data Subject.
3) Measures are in place to prevent the use or disclosure of Personal Data without permission.
4) Security measures are established for the collection, use, disclosure and transfer of Personal Data, as well as ensure that the measures are properly reviewed and updated to be compliant with the relevant local data protection laws.
5) Personal Data may only be modified or disposed of on request of the Data Subject.
6) Personal Data must be monitored and reviewed before deletion or destruction in the following cases:
    - The data storage period expires.
    - The data is irrelevant or unnecessary in relation to the purpose it was originally collected for.
    - The data subject requests the removal of their Personal Data or withdraws their consent.
7) Rights and restrictions on access to Personal Data are established.
8) Data subjects could access and review the list of all Personal Data collected by the company when requested.
9) Data Protection Officers and the Data Subject are informed immediately of any data breach.

5.8 Processing of Personal Data

SLF will ensure that, regardless if Personal Data is processed internally or by Third parties, SLF shall take appropriate actions with the aim of preventing such person from using or disclosing such Personal Data unlawfully or without authorization. These actions include the following:

1) Personal Data are collected, processed or disclosed only as specifically instructed by the Data Controller.
2) Data security measures are established to prevent the loss or the unauthorized use, modification and disclosure of Personal Data.

3) Records of all Personal Data usage are created and maintained on a regular basis.
4) Data Controllers are informed immediately of any data breach

5.9 Privacy Protection

In compliance with relevant local data protection law requirements, all of SLF's companies are required to provide a Privacy Notice to inform data subjects on the collection of their Personal Data. The Privacy Notice should contain at least the following details:

5.9.1 The target groups and Personal Data Sources the company may collect Personal Data from, including customers, suppliers, employees, job applicants, share/securities holders, and third parties.

5.9.2 The purpose of collecting Personal Data from the Data Subject, and method of collection.

5.9.3 The types of Personal Data to be collected, including name, physical address, telephone number, email address, IP address etc.

5.9.4 The length of time the Personal Data is stored by the company.

5.9.5 The rights entitled to the Data Subject.

5.9.6 The option for Data Subject to confirm or withdraw their consent to the storage of their Personal Data.

5.9.7 The measures to maintain the security of the Data Subject's Personal Data.

5.9.8 The contact information of the Data Controller or the Data Protection Officer (if available), so Data Subjects may contact for inquiries related to the website's use of personal data or exercise their rights.

5.9.9 The outside persons or juristic persons that may have access to the Personal Data.

5.9.10 The company's Cookie Policy, if the company collects Personal Data through a website or application.

6. Training

The Company shall communicate the Personal Data Protection Policy and Guidelines and cascade it through training programs, conferences, and other appropriate channels to its directors,

management, and staff. The effectiveness of such training and communications programs shall be evaluated on a regular basis.

7. Whistleblowing

In case a violation of this Personal Data Protection Policy and Guidelines is found, a report must be filed by following the procedure stated in the Whistleblowing Policy and Guidelines. The information of complainant or whistleblower will be protected and the information will be kept confidential during the investigation and after the completion of the investigation process.

8. Policy Advice

In case of suspicion on the action that may violate laws, regulations and this Personal Data Protection Policy and Guidelines, the employee can seek advice from her or his supervisors; team or persons responsible for protecting personal data within the Company, the Compliance Department or Legal Department before making any decision or carrying out any action.

9. Penalties

In the event of an investigation, all employees must fully cooperate with internal and external entities. If an employee violates or fails to comply with this Policy and Guidelines, either directly or indirectly, the employee will be subject to disciplinary action in accordance with Company's regulations.

10. Related Laws, Regulations, and Policies

10.1 Relevant local data protection laws in countries where SLF operates

10.2 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

10.3 Guidelines for the Regulation of Computerized Personal Data Files by the Office of the United Nations High Commissioner for Human Rights (OHCHR)

11. Appendix

The following appendix is attached to this Policy and Guidelines:

11.1 Appendix A: Definitions

Appendix A
Definitions

Personal Data

Any data of a living person that enables the identification of such person, whether directly or indirectly (excluding data of deceased persons).

Data Controller

A person or a juristic person having the power and duties to make decisions regarding the collection, usage or disclosure of Personal Data.

Data Processor

A person or a juristic person who operates in relation to the collection, usage or disclosure of Personal Data, pursuant to the orders given by or on behalf of a Data Controller, whereby such person or juristic person is not the Data Controller.

Data Subject

The person identified by the Personal Data.

Sensitive Personal Data

A specific set of Personal Data that is prohibited from collection without explicit consent from the Data Subject due to the risk of improper discriminatory use, and therefore must be treated with extra security. This includes ethnicity, race, skin color, political opinions, religious beliefs, sexual orientation, criminal convictions, personal health information, disability and trade union membership, genetic and biometric data, as well any other data classified as such under relevant local data protection laws.

Personal Data Source

The initial location where the Data Subject has provided Personal Data to the company, which includes the following cases:

- Contacting the company for business or any other inquiries, or submitting a comment through the company's website, application, telephone, email, in person or other method
- Participating in the company's promotional marketing campaigns, sweepstakes, and other related events
- Receiving a service provided through the company website, application or an e-Commerce service provider

- Accessing personal data from publicly-available sources, including business sources, commercial sources and social media, regardless if the Data Subject has disclosed these sources in person or has permitted the above sources to disclose them on their behalf
- Accessing personal data from third-parties, including from family members, emergency contacts, beneficiaries, job guarantors, employment websites, reference persons, state agencies, educational institutions, securities depositories, banks or bond dealers, regardless if the Data Subject has disclosed these sources in person or has permitted another person to disclose them on their behalf
- Providing supporting documents for a business or work contract with the company
- Providing supporting documents for a job application at the company
- Appearing in captured videos or images through CCTV cameras within company premises
- Visiting the company website, regardless if it is intentionally or not

Third-parties

Natural or juristic persons outside the Data Subject, Data Controller and Data Processor who are authorized to process Personal Data on behalf of SLF

Data Protection Officer (DPO)

The person appointed to advise and monitor Data Controllers and Data Processors to ensure compliance with relevant local data protection laws.

Privacy Notice

A document that inform the Data Subject on how the company gathers, uses, discloses and manages their Personal Data.

Cookie

a unique file created by a website stored on the user's computer or mobile device, and designed to collect the user's personal information, activities or preferences for the purpose of improving user experience while using the website.

นโยบายและแนวปฏิบัติ
ด้านการคุ้มครองข้อมูลส่วนบุคคล
บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด

สารบัญ

นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล
บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด

1. ความสำคัญ

บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด เคารพและให้ความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของบุคลากร ลูกค้าคู่ค้าธุรกิจ และพันธมิตรทางธุรกิจ โดยบริษัทจะปกป้องข้อมูลส่วนบุคคลจากการถูกนำไปใช้ในทางที่ผิดและรักษาข้อมูลดังกล่าวให้ปลอดภัยตามกฎหมายและมาตรฐานสากล

2. ขอบเขตนโยบาย

นโยบายและแนวปฏิบัตินี้ใช้บังคับกับเครือเจริญโภคภัณฑ์ ต่อไปนี้เรียกว่า “เครือฯ” หมายถึง บริษัท เครือเจริญโภคภัณฑ์ จำกัด และบริษัทในเครือทุกบริษัท ซึ่ง “บริษัท” ที่จะกล่าวถึงในเอกสารฉบับนี้ให้หมายถึง บริษัทหนึ่ง ๆ ที่นำเอาเอกสารฉบับนี้ไปบังคับใช้ ทั้งนี้จะมีการทบทวนโยบายฉบับนี้อย่างน้อยปีละหนึ่งครั้ง หรือกรณีมีเหตุอันสมควร

3. วัตถุประสงค์

3.1 เพื่อให้การทำธุรกรรมกับบริษัทมีความมั่นคงปลอดภัย น่าเชื่อถือ มีการคุ้มครองข้อมูลส่วนบุคคลของบุคลากร ลูกค้า คู่ค้าธุรกิจ และพันธมิตรทางธุรกิจทั้งหมด

3.2 เพื่อป้องกันความเสียหายที่เกิดจากการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์โดยทุจริตหรือนำไปใช้ในทางที่ผิด

4. หน้าที่และความรับผิดชอบ

4.1 คณะกรรมการบริษัท

4.1.1 กำหนดให้มีนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลบุคคล

4.1.2 กำกับดูแลให้มีการนำนโยบายไปปฏิบัติอย่างเป็นรูปธรรม

4.2 ผู้บริหาร

4.2.1 จัดให้มีระเบียบปฏิบัติและมาตรการในการจัดเก็บข้อมูลส่วนบุคคลให้เหมาะสมกับบริบทของแต่ละบริษัท โดยให้สอดคล้องกับนโยบายและแนวปฏิบัติ กฎหมายของแต่ละประเทศที่บริษัทประกอบธุรกิจ และมาตรฐานสากล

4.2.2 จัดให้มีโครงสร้างผู้รับผิดชอบเพื่อดูแลการดำเนินงานให้เป็นไปตามระเบียบปฏิบัติ

4.2.3 จัดให้มีระบบการคัดเลือกบุคคลหรือนิติบุคคลที่มีระบบการคุ้มครองข้อมูลที่ได้มาตรฐานและสอดคล้องตามกฎหมาย ในกรณีที่บริษัทว่าจ้างบุคคลหรือนิติบุคคลอื่นให้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลแทน

4.2.4 กำกับดูแลให้มีการปฏิบัติตามนโยบาย แนวปฏิบัติ และระเบียบปฏิบัติ ตลอดจนพัฒนาปรับปรุงวิธีการปฏิบัติให้มีประสิทธิภาพ รวมทั้งให้มีการรายงานผลอย่างสม่ำเสมอ

4.3 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

4.3.1 ควบคุม และตรวจสอบการดำเนินการของบริษัทให้ถูกต้องตามที่กฎหมายกำหนด รวมถึงการจัดกิจกรรมสร้างความตระหนักรู้ ตลอดจนการฝึกอบรมที่เกี่ยวข้องกับการดำเนินงานด้านข้อมูลส่วนบุคคล

4.3.2 ให้คำปรึกษาและแนะนำคณะกรรมการบริษัท ผู้บริหาร และพนักงาน ในการปฏิบัติตามกฎหมายให้ถูกต้อง

4.3.3 เป็นศูนย์กลางในการติดต่อเรื่องข้อมูลส่วนบุคคล การปกป้องสิทธิของเจ้าของข้อมูล รวมถึงการประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

4.3.4 รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

4.4 พนักงาน

4.4.1 ใช้ข้อมูลส่วนบุคคลอย่างระมัดระวัง ปฏิบัติตามกฎหมาย กฎระเบียบ ข้อบังคับของบริษัทอย่างเคร่งครัด

4.4.2 แจ้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทันที เมื่อพบการรั่วไหลหรือการละเมิดของข้อมูลส่วนบุคคล

4.4.3 หากพบเห็นการกระทำที่อาจเข้าข่ายเป็นการฝ่าฝืนนโยบายฉบับนี้ ให้แจ้งผ่านช่องทางการแจ้งเบาะแสและข้อร้องเรียนของบริษัท

5. แนวปฏิบัติ

5.1 การเก็บรวบรวมข้อมูลส่วนบุคคล

5.1.1 จัดเก็บข้อมูลส่วนบุคคลอย่างจำกัดเท่าที่จำเป็นแก่การใช้งานตามวัตถุประสงค์ที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคล

5.1.2 ไม่จัดเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลที่อ่อนไหวหรือข้อมูลที่ก่อให้เกิดการเลือกปฏิบัติโดยไม่เป็นธรรม หรือความไม่เท่าเทียมกัน ซึ่งอาจส่งผลกระทบต่อเจ้าของข้อมูล เว้นแต่เป็นการจัดเก็บตามกฎหมาย

5.2 การเก็บรักษาข้อมูลส่วนบุคคล

5.2.1 ต้องมีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูลส่วนบุคคล เพื่อป้องกันการทำลาย การดัดแปลงแก้ไขและการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และเพื่อป้องกันไม่ให้เกิดการรั่วไหลข้อมูลส่วนบุคคล

5.2.2 การจัดเก็บข้อมูลส่วนบุคคลโดยบุคคลภายใน บุคคลภายนอก หรือบริษัทภายนอกต้องมีระบบการคุ้มครองข้อมูลตามมาตรฐานสากล มีข้อตกลงการเก็บรักษาข้อมูลส่วนบุคคลตามวัตถุประสงค์เท่าที่จำเป็นแก่การใช้งาน

5.3 การส่งหรือโอนข้อมูลส่วนบุคคล

5.3.1 การส่งหรือโอนข้อมูลส่วนบุคคลต้องได้รับการร้องขอหรือให้ความยินยอมจากเจ้าของข้อมูล

5.3.2 การโอนข้อมูลส่วนบุคคลระหว่างประเทศสามารถทำได้ในกรณีดังต่อไปนี้

1) เจ้าของข้อมูลส่วนบุคคลรับทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางที่อาจมีไม่เพียงพอ พร้อมทั้งได้ให้การยินยอม
2) การโอนข้อมูลส่วนบุคคลเป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา ซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเป็นการดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคล
3) การโอนข้อมูลส่วนบุคคลได้ทำเพื่อป้องกันหรือระงับอันตรายต่อชีวิต หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้การยินยอมได้

5.4 สิทธิเจ้าของข้อมูลส่วนบุคคล

5.4.1 มีสิทธิขอเข้าถึงและขอรับสำเนาเกี่ยวกับข้อมูลของตนเองได้

5.4.2 มีสิทธิขอให้เปิดเผยถึงการได้มา หากเป็นข้อมูลที่ยังไม่ได้รับความยินยอม

5.4.3 มีสิทธิแจ้งเพื่อให้มีการแก้ไข เปลี่ยนแปลง ในกรณีที่ข้อมูลไม่ถูกต้อง

5.4.4 มีสิทธิลบ หรือทำลายข้อมูลส่วนบุคคลของตนเอง หรือทำให้ข้อมูลไม่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ ตามที่กฎหมายกำหนด

5.4.5 มีสิทธิโอนย้ายข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น

5.4.6 มีสิทธิระงับการใช้ข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

5.4.7 มีสิทธิคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

5.4.8 มีสิทธิร้องเรียน หากพบการละเมิดการใช้ข้อมูลตามวัตถุประสงค์ที่ได้ระบุ

5.5 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

5.5.1 ไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลนอกเหนือไปจากวัตถุประสงค์ และไม่เปิดเผยต่อบุคคลภายนอก หรือบริษัทภายนอก ยกเว้นเป็นไปตามที่กฎหมายกำหนด

5.5.2 ห้ามบุคลากร บุคคลภายนอก หรือบริษัทภายนอกนำข้อมูลส่วนบุคคลไปใช้ในทางที่ผิดกฎหมายและต้องปฏิบัติตามนโยบาย และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศที่บริษัทประกอบธุรกิจ

5.6 การทำลายข้อมูลส่วนบุคคล

5.6.1 ในกรณีข้อมูลส่วนบุคคลที่จัดเก็บนั้นไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ หรือเมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านหรือถอดถอนความยินยอม ในการประมวลข้อมูลส่วนบุคคล ให้ทำลายและลบข้อมูลออกจากระบบการจัดเก็บโดยวิธีการที่ปลอดภัยและไม่ให้ข้อมูลรั่วไหล

5.6.2 ทำลายและลบข้อมูลส่วนบุคคลออกจากระบบการจัดเก็บเมื่อพ้นระยะเวลาการใช้งานตามวัตถุประสงค์ เว้นแต่ในกรณีที่ต้องเก็บรักษาข้อมูลไว้ตามที่กฎหมายกำหนด

5.7 การควบคุมข้อมูลส่วนบุคคล

บริษัทสยามแลนด์ ฟลายอิ้ง จำกัด ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการตามหลักการคุ้มครองข้อมูลส่วนบุคคลตามที่ระบุด้านล่างนี้ เพื่อให้เกิดการใช้ข้อมูลส่วนบุคคลอย่างถูกต้อง บริษัทต้องจัดการให้มีการปฏิบัติดังต่อไปนี้

1) แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ เงื่อนไขและขอความยินยอม (ถ้ามี) ก่อนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
2) เก็บ รวบรวม ใช้ และเปิดเผย ข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์ที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคล
3) ป้องกันไม่ให้มีการนำข้อมูลไปใช้หรือเปิดเผยโดยไม่ได้รับอนุญาต
4) จัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลในการจัดเก็บ ใช้ หรือเปิดเผย รวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลไปยังบุคคลอื่นและต้องมีการทบทวนมาตรการให้สอดคล้องกับการเปลี่ยนแปลง
5) แก้ไข เปลี่ยนแปลง ลบ หรือทำลายข้อมูลตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ

6) จัดให้มีการติดตาม ตรวจสอบการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อ
   - การเก็บข้อมูลเกินกำหนดระยะเวลา
   - ข้อมูลที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ที่ได้ระบุไว้
   - เจ้าของข้อมูลร้องขอหรือถอนความยินยอม
7) จัดให้มีการกำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
8) จัดให้มีการบันทึกรายการข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงหรือตรวจสอบได้
9) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลทันทีเมื่อตรวจพบ

5.8 การประมวลผลข้อมูลส่วนบุคคล

ในการประมวลผลข้อมูลส่วนบุคคล บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด จัดให้มีการดำเนินการเพื่อป้องกันการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยโดยผิดกฎหมายหรือปราศจากการให้ความยินยอม โดยให้ผู้ประมวลข้อมูลให้บริษัท ซึ่งรวมทั้งบุคคลภายในบุคคลภายนอก และนิติบุคคลภายนอกดำเนินการดังต่อไปนี้

1) ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามที่ได้รับคำสั่งจากผู้ควบคุมข้อมูลส่วนบุคคล
2) จัดให้มีมาตรการรักษาความปลอดภัย เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล
3) บันทึกและเก็บรักษารายการการประมวลผลข้อมูลส่วนบุคคล
4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลทันทีเมื่อตรวจพบ

5.9 การคุ้มครองความเป็นส่วนตัว

เพื่อเป็นการปฏิบัติตามกฎหมายที่กำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด ต้องแจ้งประกาศความเป็นส่วนตัวที่ระบุถึงการเก็บรวบรวมข้อมูลส่วนบุคคล โดยมีการแจ้งถึงรายละเอียดการรวบรวมข้อมูลส่วนบุคคลอย่างน้อยตามหัวข้อดังต่อไปนี้

5.9.1 ระบุประเภทของกลุ่มบุคคลที่บริษัทมีการเก็บรวบข้อมูลส่วนบุคคล ได้แก่ ลูกค้า คู่ค้า พนักงาน ผู้สมัครงาน ผู้ถือหุ้นหรือผู้ถือหลักทรัพย์ และบุคคลภายนอก รวมถึงแหล่งที่มาของข้อมูลส่วนบุคคล

5.9.2 อธิบายถึงวัตถุประสงค์และวิธีการเก็บข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

5.9.3 ระบุถึงข้อมูลส่วนบุคคลที่เก็บรวบรวม ได้แก่ ชื่อ ที่อยู่ หมายเลขโทรศัพท์ อีเมล หมายเลขไอพี เป็นต้น

5.9.4 ระบุระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

5.9.5 ระบุสิทธิทั้งหมดของเจ้าของข้อมูลส่วนบุคคล

5.9.6 ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม และการถอนความยินยอมจากการจัดเก็บข้อมูลส่วนบุคคล

5.9.7 ระบุถึงมาตรการที่ดำเนินการทั้งหมดเพื่อปกป้องข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

5.9.8 ระบุช่องทางการติดต่อผู้ควบคุมข้อมูลส่วนบุคคล หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อ หรือสอบถามเพิ่มเติม หรือใช้สิทธิในฐานะเจ้าของข้อมูลส่วนบุคคล

5.9.9 ระบุประเภทของบุคคลหรือหน่วยงานภายนอกองค์กรที่อาจนำข้อมูลส่วนบุคคลไปใช้

5.9.10 ระบุนโยบายการใช้คุกกี้ในกรณีที่บริษัทมีการจัดเก็บข้อมูลส่วนบุคคลผ่านทางเว็บไซต์ และแอปพลิเคชัน

6. การฝึกอบรม

จัดให้มีการสื่อสารและถ่ายทอดนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลผ่านการฝึกอบรม การประชุม หรือกิจกรรมในรูปแบบต่าง ๆ ให้แก่กรรมการ ผู้บริหารและพนักงานและให้มีการประเมินประสิทธิผลอย่างต่อเนื่อง

7. การแจ้งเบาะแส

ร้องเรียนหรือแจ้งเบาะแสเมื่อพบเห็นการกระทำที่เชื่อได้ว่าเป็นการละเมิดนโยบายและแนวปฏิบัตินี้ โดยขั้นตอนให้เป็นไปตามนโยบายและแนวปฏิบัติเกี่ยวกับการแจ้งเบาะแส ทั้งนี้ผู้ร้องเรียนหรือผู้แจ้งเบาะแสจะได้รับความคุ้มครองและข้อมูลจะถูกเก็บเป็นความลับ โดยไม่มีผลต่อตำแหน่งงาน ทั้งในระหว่างดำเนินการสอบสวนและหลังเสร็จสิ้นกระบวนการ

8. การขอคำแนะนำ

ในกรณีที่มีข้อสงสัยว่าการกระทำนั้นอาจฝ่าฝืนกฎหมาย ระเบียบ นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลสามารถขอคำแนะนำจากผู้บังคับบัญชา หน่วยงานหรือบุคคลผู้รับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านกำกับการปฏิบัติตามกฎเกณฑ์หรือด้านกฎหมายก่อนตัดสินใจหรือดำเนินการใด ๆ

9. บทลงโทษ

ในกรณีที่เกิดการสอบสวน พนักงานทุกคนต้องให้ความร่วมมือกับหน่วยงานภายในและภายนอกอย่างเต็มที่ ทั้งนี้หากผู้บริหารและพนักงานกระทำการใด ๆ ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบาย

ฉบับนี้ไม่ว่าทางตรงหรือทางอ้อม ผู้บริหารและพนักงานจะถูกพิจารณาโทษทางวินัยตามระเบียบข้อบังคับการทำงาน

10. กฎหมาย กฎระเบียบและนโยบายที่เกี่ยวข้อง

10.1 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศที่บริษัท สยามแลนด์ ฟลายอิ้ง จำกัด ประกอบธุรกิจ

10.2 การคุ้มครองข้อมูลส่วนบุคคลตามแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)

10.3 แนวทางการควบคุมข้อมูลส่วนบุคคลที่จัดเก็บด้วยคอมพิวเตอร์ (Guidelines for the Regulation of Computerized Personal Data Files ของ Office of the United Nations High Commissioner for Human Rights: OHCHR)

11. ภาคผนวก

นโยบายและแนวปฏิบัตินี้ ประกอบด้วยภาคผนวก ดังต่อไปนี้

11.1 ภาคผนวก ก คำนิยาม

ภาคผนวก ก
คำนิยาม

ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายถึง บุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายถึง บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องไม่เป็นบุคคลเดียวกับผู้ควบคุมข้อมูลส่วนบุคคล

เจ้าของข้อมูล (Data Subject) หมายถึง เจ้าของข้อมูลส่วนบุคคล

ข้อมูลที่อ่อนไหว (Sensitive Personal Data) หมายถึง ข้อมูลส่วนบุคคลที่มีลักษณะเป็นข้อมูลที่อ่อนไหว ห้ามมิให้เก็บรวบรวม โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เนื่องจากสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ อันได้แก่ เชื้อชาติ เผ่าพันธุ์ สีผิว ความคิดเห็นทางการเมือง ศาสนา รวมถึงพฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ และข้อมูลอื่นใดตามที่กฎหมายแต่ละประเทศกำหนด

แหล่งที่มาของข้อมูลส่วนบุคคล (Personal Data Source) หมายถึง แหล่งที่ได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล เช่น

- การติดต่อธุรกรรม กรอกแบบฟอร์ม ให้ความเห็น ให้คำติชม หรือสอบถามข้อมูลผ่านช่องทางเว็บไซต์ แอปพลิเคชัน โทรศัพท์ อีเมล การพบปะกันโดยตรง หรือโดยวิธีการอื่นใด
- การเข้าร่วมกิจกรรมทางการตลาด การจับสลากชิงโชค งานอีเว้นท์ และกิจกรรมอื่น ๆ
- การให้บริการผ่านเว็บไซต์ แอพพลิเคชัน หรือผู้ให้บริการ E-Commerce
- การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งข้อมูลสาธารณะ แหล่งข้อมูลเกี่ยวกับธุรกิจ แหล่งข้อมูลทางการค้า หรือแหล่งข้อมูลจาก Social Media ไม่ว่าเจ้าของข้อมูลส่วนบุคคลจะเป็นผู้เปิดเผยข้อมูลด้วยตนเอง หรือได้ให้ความยินยอมแก่ผู้ใดในการเปิดเผยข้อมูลส่วนบุคคลดังกล่าว
- การเก็บรวบรวมข้อมูลส่วนบุคคลจากบุคคลที่สาม อาทิ บุคคลในครอบครัว บุคคลที่สามารถติดต่อได้ในกรณีฉุกเฉิน ผู้รับผลประโยชน์ ผู้ค้ำประกันการทำงาน เว็บไซต์สมัครงาน บุคคลอ้างอิงบริษัทจัดหางาน หน่วยงานของรัฐ สถานศึกษา ศูนย์รับฝากหลักทรัพย์ ธนาคารหรือผู้ที่ได้รับอนุญาตให้เสนอขายหุ้นกู้ของบริษัท ไม่ว่าเจ้าของข้อมูลส่วนบุคคลจะเป็นผู้เปิดเผยข้อมูลด้วยตนเอง หรือได้ให้ความยินยอมแก่ผู้ใดในการเปิดเผยข้อมูลส่วนบุคคลดังกล่าว

- การส่งมอบเอกสารประกอบการทำสัญญาทางธุรกิจ หรือสัญญาจ้างกับบริษัท
- การส่งมอบเอกสารประกอบใบสมัครงาน
- การบันทึกภาพนิ่งหรือภาพเคลื่อนไหวโดยกล้องวงจรปิด (CCTV) ในสถานที่อยู่ภายใต้การควบคุมของบริษัท
- การเข้าชมเว็บไซต์บริษัทไม่ว่าจะโดยเจตนา หรือไม่เจตนา

บุคคลภายนอก หรือ บริษัทภายนอก (Third parties) หมายถึง บุคคลหรือนิติบุคคลนอกเหนือจากเจ้าของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลข้อมูลส่วนบุคคลที่ได้รับจ้างให้ประมวลข้อมูลในนามบริษัท สยามแลนด์ ฟลายอิ้ง จำกัด

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หมายถึง บุคคลที่ถูกแต่งตั้งให้มีหน้าที่ให้คำแนะนำและตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลให้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประกาศความเป็นส่วนตัว (Privacy Notice) หมายถึง การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ วิธีการรวบรวม ประมวล และจัดเก็บข้อมูลส่วนบุคคลของบริษัท

คุกกี้ (Cookie) หมายถึง ไฟล์เป็นเอกลักษณ์ซึ่งสร้างโดยเว็บไซต์และจัดเก็บบนคอมพิวเตอร์ หรืออุปกรณ์สื่อสารของผู้ใช้งานซึ่งจะจัดเก็บข้อมูลส่วนบุคคล การใช้งาน และการตั้งค่าต่าง ๆ ของผู้ใช้งานเพื่อปรับปรุงประสบการณ์ใช้งานเว็บไซต์ของผู้ใช้งาน