Bangkok Lab and Cosmetic Public Company Limited
48/1 Moo 5, Nongshaesao Road, Tumbon Namphu, Ampur Meung,
Ratchaburi 70000, Thailand

(Translation)

Management Document of Bangkok Lab Cosmetic

BLCP 10-012

Personal Data Protection Policy

Revision No. 2 Effective Date: 08/01/2026

(Translation)

Bangkok Lab and Cosmetic Public Company Limited

Personal Data Protection Policy

Approved by *Assist. Prof. Dr. Wanchai Sutananta*
(Chairman of the Board of Directors)
Based on the Resolution of the Board of Directors Meeting No. 8/2025
on December 22, 2025

Reviewed Version No. 2/2026

(Translation)

Table of Contents

Personal Data Protection Policy 2

Objectives and Scope of the Personal Data Protection Policy 2

- Key Definitions 2
- Personal Data Collection 2
- Privacy Notice for Data Subjects 4
- Sources of Personal Data 4
- Rights of the Data Subject 4
- Duties and Responsibilities of Personnel 7
- Measures for the Personal Data Protection 9
- Recording, Collection, Use, and Disclosure of Personal Information 9
- Transmission or Transfer of Personal Information to Foreign Countries or International Organizations 10

(Translation)

Personal Data Protection Policy

Objectives and Scope of the Personal Data Protection Policy

To comply with the Personal Data Protection Act, B.E. 2562 (2019), and other relevant laws, including any future amendments (the "**Personal Data Protection Law**"), Bangkok Lab and Cosmetic Public Company Limited (the "**Company**") has prepared this Personal Data Protection Policy (the "**Policy**") to describe in detail the collection, use, and disclosure of personal data to its personnel and employees, or to the personnel and employees of third parties acting on their behalf or on behalf of the Company in relation to the processing of personal data in connection with the Company's business operations in accordance with the Personal Data Protection Law.

Key Definitions

"**Personal Information**" refers to information about a natural person, which enables the person to be identified, directly or indirectly, but does not specifically include the deceased person's information.

"**Sensitive Personal Information**" refers to personal information about race, ethnicity, political opinions, doctrine, religious or philosophical beliefs, sexual behavior, criminal record, health information, disability, trade union information, genetic information, biometric information, or any other information that may give rise to unfair discrimination against the data subject or similarly affect the data subject as required by applicable data protection laws.

"**Data Subject**" refers to a natural person who owns personal data, including customers, suppliers, service providers, directors, employees, visitors, and any other natural person whose personal data the Company collects, uses, or discloses.

"**Personal Data Controller**" refers to the Company that has the authority to make decisions regarding the collection, use, or disclosure of personal data.

"**Personal Data Processor**" refers to the Company or an individual designated by the Company to process personal data on its behalf, including tasks related to processing, collecting, using, or disclosing that data.

"**Lawful Basis**" refers to the grounds under which the law provides for the collection of personal information under the Personal Data Protection Law.

Personal Data Collection

In collecting personal information, the Company has defined it as follows:

1. General Personal Information

The Company will collect personal information in accordance with one of the following lawful bases:

1.1 Consent from the personal data object (consent basis)

In the event that the data cannot be collected on another lawful basis as specified in Clauses 1.2 – 1.7, the Company will request the express consent from the data object, either before or at the time of collection of the personal data, in writing or electronically. Except that such a request for consent cannot be made, in this case, the data subject may give verbal consent. The Company will record such consent in writing and specify details of the method and the date of consent.

The Company will seek the consent of the personal data subject when the data subject freely and voluntarily consents.

Note: If the Company seeks the consent of a minor who is not of legal age, an incapacitated person, or a person deemed incapacitated, the Company must obtain consent from the person authorized to act on behalf of the minor, the guardian, or the custodian, respectively. In the case of minors 10 years of age or older, the minor can give his/her own consent, provided that the consent is solely for the benefit of the minor.

1.2 For the preparation of historical documents or archives in the public interest, research, or statistics (archives/research/statistics basis)

In cases where the Company needs to collect personal information for the preparation of historical documents or archives in the public interest or related to research studies or statistics, appropriate protection measures are in place to protect the rights and freedoms of the data subject as required by law.

1.3 To prevent or suppress harm to a person's life, body, or health (vital interest basis)

In cases where the Company needs to collect personal information to prevent or suppress harm to the life, body, or health of an individual, it is necessary for the Company to collect personal information due to an emergency accident involving the data subject.

1.4 To perform the contract between the Company and the data subject or to process the request of the data subject before entering into a contract with the Company (contract basis).

In cases where the Company needs to collect personal information in order to perform a contract to which the data subject is a party directly to the Company or to act at the request of the data subject before entering into a contract with the Company.

1.5 To perform the duties of carrying out missions for the public interest (public interest basis)

In cases where the Company must collect personal information to fulfill its duties related to public interest or to exercise the authority granted by the state.

1.6 For Legitimate Benefit (legitimate interest basis)

In the event that the Company needs to collect personal information to pursue the legitimate interests of the Company or a third party, and if the legitimate interests are less important than the fundamental rights of the data subject to the personal information, and if it is necessary for the Company to collect that personal information, the Company will seek the consent of the data subject.

1.7 To comply with the laws applicable to the Company (legal basis)

In cases where the Company needs to collect personal information to comply with applicable law, including a court order or government official.

2. Sensitive Personal Information

The Company will collect sensitive personal information only **with the express consent** of the data subject (details in Clause 1.1), unless exempted by law as follows:

- It prevents or suppresses harm to the life, body, or health of the person whose consent is not available to the data subject (this is used for emergencies).
- It is publicly available information with the express consent of the data subject.
- It is necessary to comply with the law in order to achieve the objectives regarding:
  - Preventive or occupational medicine, assessment of the employee's ability to work
  - Public health benefits, such as the purpose of preventing communicable diseases or epidemics
  - Labor protection, social security, national health insurance, and healthcare benefits according to the rights of the eligible persons under the law
  - Scientific, historical, or statistical research or other public interest studies
  - Other important public interests such as objectives of anti-money laundering

Details on the type, objective, and lawful basis of the Company's personal data collection can be found in the Privacy Notice for Different Types of Data Subjects.

3. Personal Information Collection Practices

Personal information will only be collected to the extent necessary to achieve the objectives set forth by the Company. The Company will consider and choose to collect information to the extent necessary to use and dispose of or destroy information that may be obtained unnecessarily, especially sensitive personal information, to reduce the risk of unlawfully collecting, using, and disclosing personal information of the Company.

Privacy Notice for Data Subjects

The Company has prepared and notified a privacy notice to the data subject so that the data subject can use it in consideration of consent in the event that the data collection is not on the lawful basis.

The Company will provide the privacy notice before or while collecting personal information from the data subject, except in the case of the collection, use, or disclosure of personal information that occurred before the publication of this policy. The Company will announce the privacy notice on the Company's website.

In the event that the Company makes revisions to the privacy notice in the future, it will notify users of the changes on the Company's website.

Sources of Personal Data

It is the Company's policy to collect personal information directly from the owner of personal information. If the Company collects personal information from other sources, the Company will notify the data subject of the collection of personal information and the privacy notice within 30 days from the date the Company collects it, and the Company will also seek the consent of the data subject in the event that the personal information is collected by virtue of a consent basis. The Company will notify the data subject at the time of contact or prior to the first disclosure of personal information, unless it is required to use the personal information to contact the data subject or disclose it. Unless such notification is not possible, or would hinder the Company's use or disclosure of personal data, or the data subject is already aware of the details, the Company may waive such data collection and privacy notice to the data subject.

In the event that the Company has hired the personal data processor to act on its behalf at the Company's direction, the Company may require the personal data processor to provide a privacy notice on behalf of the Company. The Company will supervise the personal data processor to comply with this policy and assume that the Company has provided details in accordance with the duties of the personal data controller as required by the personal data protection law.

Rights of the Data Subject

The Company provides a data subject rights request form to facilitate data subjects in notifying their intention to exercise various rights regarding their personal data as stipulated in the Personal Data Protection Act. In the event that the Company is unable to process the request to exercise its rights, the Company will notify the data subject in writing and keep a record of it.

1. **Right to revoke consent:** A data subject has the right to revoke in part or all of the consent throughout the period that the Company retains the personal data. The Company will inform the data subject of the impact upon revocation of the personal data. Withdrawing consent will not affect anything that the Company has previously done due to the lawful consent of the data subject.

   Reason for refusal: The Company has the right to refuse withdrawal of consent in cases where there is a statutory

restriction of the right to withdraw consent or in the case of personal data in connection with a contract that benefits the data subject.

Response period: Without delay

2. **Right to request access to and obtain a copy of personal information:** The data subject has the right to disclose the acquisition of such personal information without their consent or to request access to and acquire a copy of personal information about themselves that is under the Company's responsibility,

   Reason for rejection: The Company may only deny a request in the following circumstances:

   - Following a law or court order; or
   - When the Company deems that it will affect the fundamental rights and freedoms of others.

   However, if the Company is unable to act on the data subject's request in accordance with the above rights, the Company will record the rejection of the request and the reasons in the Company's records.

   Response period: In the event that the Company cannot refuse, it will process the request of the data subject within 30 days from the date of receipt of the request.

3. **Right to request the receipt, transfer, or transmission of personal data:** The data subject has the right to obtain personal information about himself or herself from the Company or to ask the Company to send or transfer the information to other personal data controllers in a form that can be read or used in general. This includes the right to request to obtain his or her personal information that the Company, or other individuals or personal data controllers have received and stored. Such personal information must be information that the data subject has consented to collect, use, or disclose the personal information for; to comply with a contract; or to be used only in the execution of a request before entering into a contract between the data subject and the Company.

   Reason for rejection: The Company can deny a request if such personal information is used in the public interest or for the performance of a statutory duty, or if the exercise of such rights violates the rights and freedoms of another person, such as where such personal information contains trade secrets or intellectual property information.

   However, If there are reasons for refusing the request of the data subject in accordance with the above rights, the Company will record the refusal of the request and the reasons in the Company's records.

   Response period: Without delay

4. **Right to object to the collection, use, or disclosure of personal information:** The data subject has the right to object to the collection, use, or disclosure of the Company's personal information in the following cases:

   (1) It is the collection, use, or disclosure of personal information for the legitimate benefit or public interest, including compliance with orders from government officials.

   Reason for rejection of the request (for Clause 4 (1)): The Company can demonstrate that there are legitimate grounds that outweigh the interests, rights, or freedoms of the data subject, or that the collection, use, or disclosure of data is for the purpose of establishing, complying with, using, or defending against legal claims.

   However, if there are reasons for refusing the request of the data subject in accordance with the above rights, the Company will record the refusal of the request and the reasons in the Company's records.

   (2) In the case of direct marketing, the data subject can make an objection unconditionally.

   (3) For scientific, historical, or statistical research unless it is necessary in the public interest.

   Response period: Without delay, and in the event that the Company has no grounds for rejection, the Company will promptly separate the above personal data from other data when the data subject gives notice of the objection.

5. **Right to request deletion of personal information:** The data subject has the right to ask the Company to delete,

destroy, or make the personal data into non-personally identifiable information when:

(1) Personal data is no longer necessary for its intended purpose.

(2) The data subject has withdrawn consent, and the Company can no longer use other lawful bases for collecting the data.

(3) The data subject has objected to the collection, use, or disclosure of the personal data and the Company cannot deny the objection.

(4) Personal information has been illegally collected, used, or disclosed.

Reason for rejection of the request: The Company has the right to deny the request in the following cases:

- It is retention for the purpose of exercising freedom of opinion;
- For the achievement of the objective on the basis of the preparation of historical documents or archives, research, statistics, or public interest basis;
- It is the collection of sensitive personal data, which is necessary for the performance of legal duties for the purpose of preventive medicine, occupational medicine, assessment of employee ability, and public interest in public health;
- It is used for the establishment, compliance with, or exercise of a legal claim or for defense against a legal claim;
- It is used for the performance of statutory duties.

If the personal information has been made public by the Company or has been transferred to another personal data controller and the data subject has requested that such data be deleted, destroyed, or made unidentifiable, the Company must delete, destroy, or de-identify such personal information and must notify other personal data controllers to comply with the request.

Response period: Without delay.

6. **Right to request the suspension of the use of personal information:** The data subject has the right to request the Company to suspend the use of personal information when:

   (1) The data subject has requested the Company to correct the accuracy of the personal information and is in the process of reviewing it. However, the Company may consider lifting the suspension of the use of personal data if it verifies that the requested data correction is already accurate. The Company will notify the data subject before the suspension and will provide the reasons for lifting the suspension.

   (2) It is an unlawful use of the data, but the data subject asks to suspend its use instead of deleting it.

   (3) Personal data is no longer necessary to be retained, although the data subject had previously requested the Company to retain the data because it is necessary for its use, establishment, implementation, or defense of legal claims of the data subject.

   (4) The Company is in the process of verification to refuse the objection to personal information. However, the Company may consider lifting the suspension of the use of the personal information if the Company considers that it has the right to continue using the information in accordance with the reasons for the denial of the right to object to the abovementioned personal information.

   Response period: Without delay.

7. **Right to request correction of personal information:** The data subject may request the Company to ensure that the personal information is accurate, current, complete, and not misleading.

   However, if there are reasons for refusing the data subject's request in accordance with the above rights, the Company will record the rejection of the request and the reasons in the Company's records.

Response period: Without delay.

8. **Right to complain:** The data subject has the right to complain to the expert committee when it considers that the Company or the personal data processor, including its employees or contractors, violates or fails to comply with the personal data protection law.

Duties and Responsibilities of Personnel

All employees and personnel, including those employed by the Company and employees of those employed by the Company, have a duty to comply with the law and this Personal Data Protection Policy and must strictly maintain the confidentiality of personal information and must not misuse personal information obtained during the performance of their duties for personal gain or unlawful use. The duties and responsibilities may be divided in the following order:

1. **Chief Executive Officer and Executive Personnel**

   The Chief Executive Officer and executive personnel are responsible for supervising the Company's entire personal data protection process as follows:

   - Assign employees the task of establishing practices related to the protection of personal information, including practices for managing the risks that may arise from the collection, use, and disclosure of personal information by the Company, as well as guidelines for concrete solutions in the event of a personal information breach within the Company.
   - Ensure regular control and monitoring of compliance with this policy or its suitability.
   - Approve the execution of various policies related to the protection of personal information, such as reviewing the policy's suitability or amending it to protect personal information within the Company.

   The Chief Executive Officer is responsible for overseeing the Company's entire personal data protection process as follows:

   - Designate a person or entity acting as a Data Protection Officer (DPO) and/or another person or entity to be the center of the Company for the care and receipt of matters related to the protection of personal information from various entities within the Company.
   - Consider and approve in response to requests to exercise the rights of the data subject if responding to such requests may have a significant impact on the Company, the data subject, and/or any other person.

2. **Data Protection Officer (DPO) or Person Responsible for the Protection of Personal Data of the Company**

   It is responsible for advising and reviewing the Company's entire personal data protection process as follows:

   - Analyze, evaluate, monitor, and control the Company's personal data processing activities, and provide advice to personnel or other entities within the Company to ensure that these activities comply with personal data protection laws and the Company's personal data protection policy.
   - Review and approve the privacy protection practices of each department within the Company, including practices for managing the risks that may arise from the collection, use, and disclosure of personal information by the Company, and guidelines for solving problems when personal information breaches occur within the Company.
   - Analyze, evaluate, and advise personnel and entities within the Company in response to requests to exercise the rights of the data subject if the response to such requests may have a material impact on the Company, the data subject, and/or any other person.
   - Report incidents related to the processing of personal data within the Company to the Chief Executive Officer and executive personnel.

- Coordinate and cooperate with the Office of the Personal Data Protection Committee, including the notification of personal data breaches occurring within the Company to the Office of the Personal Data Protection Committee within the period specified by law.
- Learn more about the Personal Data Protection Act B.E. 2562 (2019), rules, notifications, orders, regulations, or any other laws relating to the protection of personal data, including following the changes or amendments to such personal data protection laws and notifying the Company's personnel.
- Explain, create understanding and raise awareness among the Company's personnel regarding the protection of personal data and related personal data protection laws.

3. Department Managers, Division Managers, Division Heads

They are responsible for supervising the collection, use, or disclosure of personal information within their entities, which may vary by entity. The duties may be divided as follows:

- Allow any person to access personal information or delegate duties to employees who are responsible for the care of personal information in various parts of their entities.
- Provide guidelines and training on the protection of personal information in their entities and create a common understanding of what personal information is required to be collected and what one is not required to be collected for use within their entities.
- Establish security measures for personal information in their entities to be standardized in accordance with the law and this policy.
- Approve responding to requests to exercise the rights of personal data subjects and consult with relevant authorities on such matters, including with the personal data protection officer or the person responsible for the protection of personal data of the Company, and report to the management for approval if the response to such requests may have a significant impact on the Company, the data subject, and/or any other person.
- Consult with management and the personal data protection officer to determine appropriate practices.
- Provide recording, collection, use, or disclosure of their entity's information in accordance with the items set forth in this policy.
- Receive a report from a subordinate in case employees are notified of a personal data breach and determine whether the breach may pose a risk of affecting the rights and freedoms of the data subject, including consultation with the personal data protection officer or the responsible person regarding the protection of the Company's personal data and the management to determine whether any appropriate action is ordered in accordance with this policy.

4. Employees

They are obliged to strictly comply with this law and the personal data protection policy, in particular with respect to procedures at the operational level as follows:

- Collect, use, and disclose personal information in accordance with the law and this policy, and participate in training on the protection of personal information of the Company.
- Comply with the duties assigned to carry out the protection of personal information in relation to personal information management, such as security, transmission, disclosure, recording of information, etc.
- Inform the supervisor in the event that it considers that the collection, use, or disclosure of any personal information in the Company or any order to do so is unlawful or when it is deemed that the collection, use, or disclosure of any personal information may pose a risk of violating the fundamental rights and freedoms

of the data subject.

- Notify the supervisor for approval in the event of receipt of a request to exercise the rights of the data subject.
- Promptly notify the supervisor in the event of a personal data breach, whether the breach is caused by the intent or negligence of any person, and whether the breach may or may not have the risk of affecting the rights and freedoms of the data subject.

5. Contractors and Service Providers as the Company's Personal Data Processors

Contractors and service providers who process personal data on behalf of the Company must adhere to this policy, the legislation protecting personal data, and the terms of any personal data processing agreements they have with the Company. The duties are as follows:

- Collect, use, and disclose personal information in accordance with the law and this policy, as well as attend training on the protection of personal information of the Company upon request.
- Notify the Company without delay in the event of a personal data breach.
- Support and assist the Company in responding to requests to exercise the rights of data subjects.

Violations of the law and this policy by employees may constitute disciplinary action, and violations of the law or this policy by contractors or service providers who process the Company's personal data may also be considered a breach of contract with the Company. If such a breach or non-compliance results in damage to the Company, the Company may consider it grounds for termination of employment or contract. There may also be criminal penalties, which are fines and imprisonment for those acting on behalf of the Company who violate or fail to comply with the law. Employees and related parties must therefore study the law on the protection of personal data and this policy and strictly comply with it.

Measures for the Personal Data Protection

The Company has implemented both policy and technical security measures to prevent the loss, unauthorized access, use, alteration, modification, or disclosure of personal data, and such measures are reviewed when necessary or when the technology changes in order to be effective in maintaining the security of personal information as required by law.

Recording, Collection, Use, and Disclosure of Personal Information

In order for the data subject to verify and exercise its rights, the Company has recorded, collected, used, and disclosed the personal information collected. The personal data to be collected must include at least the following items:

- Personal information collected
- Purposes of collecting personal information
- Information about the personal data controller
- Retention period of personal data
- Rights and methods of access to personal information, including conditions for exercising access to personal information
- Use or disclosure of personal information where personal information is collected based on a lawful basis other than consent
- Rejection of requests or objections to the exercise of the rights of the data subject

- Explanation of personal information security measures

Transmission or Transfer of Personal Information to Foreign Countries or International Organizations

1. The Company may transfer or send personal data to destination countries that have adequate data protection standards and comply with the laws.
2. In the case that the destination country has insufficient standards, the Company can transfer personal information in the following cases:
   - Consent has been obtained from the data subject, who is already aware of the inadequate standards of the destination country.
   - It is necessary to perform the contract to which the data subject is a party or to carry out the request before entering into the contract.
   - It is the performance of a contract between the Company and another person or legal entity for the benefit of the data subject.
   - To prevent or suppress harm to the life, body, or health of the data subject or other persons when the data subject is unable to give his or her consent at the time.
   - It is necessary to carry out the mission in the public interest.
3. In the case of sending or transferring personal data to the personal data controller or personal data processor who is abroad and affiliated with the same business, the Company has established a personal data protection policy for the transmission or transfer of data between each other in the same business that has been reviewed and certified by the Office of the Personal Data Protection Committee.

Actions for Personal Data Breach

When a personal data breach occurs within the company and that breach poses a risk to the rights and freedoms of the data subject, employees and related personnel must coordinate to take legal action. The Company will notify the Office of the Personal Data Protection Committee of the breach **within 72 hours** of becoming aware of the incident. In the event that the breach poses a high risk to the rights and freedoms of the data subject, the Company will immediately notify the data subject of the cause of the breach along with available remedies.

Amendments to the Personal Data Protection Policy

This personal data protection policy may be amended in response to changes in law and business suitability.

Additional Inquiries and Notifications of Personal Data Violations

For further inquiries or questions regarding personal data protection, or if you wish to report a personal data breach, please contact:

Data Protection Officer (DPO) at Telephone 0-3271-9920 or 0-3271-9900

E-mail: blc.dpo@bangkoklab.co.th