



T.S.K. FORGING CO.,LTD.

Personal Data Protection Policy

T.S.K. Forging Company Limited

Intent and Purpose of the Personal Data Protection Policy

In order to comply with the Personal Data Protection Act B.E. 2562 and other related laws, as well as any amended laws in the future (“the Personal Data Protection Laws”), T.S.K. Forging Company Limited (“the Company”) has therefore created this Privacy Policy (“the Policy”) to describe in detail regarding the collection, use and disclosure of personal information to our personnel and employees, or personnel and employees of third parties acting on or on behalf of the Company, in the processing of personal data in connection with the Company's business operations to be in accordance with the personal data protection law.

Key Definitions

“**Personal Data**” means information about an individual that enables oneself to be identified, either directly or indirectly, but does not include information of the deceased in particular.

“**Sensitive Personal Data**” means personal data regarding race, ethnicity, political opinions, cult, religion or philosophy, sexual preference, criminal records, health information, disability, union information, genetic data, biological data or any other data which may cause unfair discrimination against its subject or similarly affects the personal data owner as stipulated by the personal data protection law.

“**Personal data subject**” means a natural person whose personal data belongs to, i.e. customers, business partners, service providers, directors, employees, visitors and any other natural persons with whom the Company collects, uses or discloses personal data of that natural person.

“**Personal Data Controller**” means a natural person or a juristic person who has the authority to make decisions regarding the collection, use or disclosure of personal data.

“**Personal Data Processor**” means a natural person or juristic person who performs the collection, use or disclosure of Personal Data on the order or on behalf of the Personal Data Controller. However, such person is not considered as the Personal Data Controller.

“**Legal base**” means the grounds under which the Personal Data can be collected according to the Personal Data Protection Act.

Lawful Collection of Personal Information

To collect, use or disclose personal information, the Company shall act in accordance with the legal bases set out in the Personal Data Protection Act which has been regarded as a guideline in this policy as well as follows

1. **General personal information** The collection of personal data is authorized only when one of the seven legal bases is met:



T.S.K. FORGING CO.,LTD.

1.1 Consent of personal data subject (Consent Base)

In the event that data cannot be collected by other legal bases as set forth in Sections 1.2 – 1.7 of this Policy, the Company is obliged to obtain the expressed consent of the Personal Data Subject before or while collecting the Personal Data. No response or inaction does not constitute consent from the personal data subject. In addition, consent must be in writing, or through electronic systems which may contain forms and texts prepared by the Company (Letter of consent) or as required by law (if any), except for such consent is not possible. In this case, the data subject may provide verbal consent. However, the Company must record such consent in writing with details of the method of expressed consent and the date it has been given. The data subject may withdraw his consent at any time, unless there is a restriction by law or a contract deemed beneficial to the personal data subject.

However, the Company should keep in mind that it can seek consent only if the Personal Data Subject is able to provide his freely and completely voluntary consent.

Note: In the event that the Company has to obtain consent from a minor who is underage, an incompetent person or a quasi-incompetent person, the Company must seek to obtain such consent from their appointed guardians. In the case of a minor that is 10 years of age or older, consent may be given by himself/herself in regards of action that could be carried out by the minor independently.

1.2 For the collection of historical documents or archives for the public benefit, doing studies or statistics research(Archives/Research/Statistics)

The Company may collect personal information intended for preparation of historical documents or archives for public interest, or in regards to studies or statistics research which have put in place appropriate safeguards to protect the rights and freedoms of the personal data subject, as required by law.

1.3 To prevent or stop a danger to life, body or health of the person. (Basic benefits for life)

In some cases, it may be necessary for the Company to collect personal information in order to prevent or stop foreseeable hazards to life, body or health of any persons which is not only limited to the owner of the personal information, for example, in the event that the Company is required to collect personal information due to an emergency accident that occurs with the owner of the personal information, in this case, the Company does not need to ask for consent in order to collect such personal information.

1.4 To perform the contract between the Company and the Personal Data Subject or to process the request of the Data Subject before entering into a contract with the Company (Contract base).

In the event that the Company needs to collect personal data in order to perform a contract to which the personal data subject is a direct party to the Company, or take action at the request of the personal data subject before entering into a contract with that company, the Company does not require consent for the collection of such personal data.



T.S.K. FORGING CO.,LTD.

1.5 To perform duties in carrying out missions for the public interest (Public benefit base)

In the event that the Company is required to collect personal data for the purpose of performing its duties in the public interest of the Personal Data Controller or perform the state authorized duties, the Company does not require consent for collection of such personal data.

1.6 It is necessary for our legitimate interest. (Base of legitimate interests)

The Company may collect personal data without obtaining the consent of the personal data subject. In the event that the Company is required to collect such information in order to carry out its legitimate interests of the Company or a third party who is not the owner of the Personal Data, i.e. the legitimate interest in the Company's and/or the third person's business operations, the legitimate interest in securing and protecting assets and persons within the Company's premises, lawful interests in the management of the Company's organization, etc. However, the Company must be careful in using this legal base when collecting personal information, and has it found that such legitimate interests are less important than the fundamental freedoms of the data subject or in cases where the fundamental freedoms of the personal data subject may be greatly affected, the Company will not collect personal information based on legitimate interests. However, the Company must obtain the consent of the Personal Data Subject if the Company wishes to proceed in collecting such Personal Data.

As a guideline for application of the legitimate interest base, the Company shall assess whether the collection of any personal information has met the following criteria in all respects.

- (1) Whether the Company or a third party has a legitimate interest from collecting such personal information.
- (2) If the collection of such personal data is necessary for the benefits under (1)
- (3) It is foreseeable to the Personal Data Subject to expect the collection of such Personal Data by the Company.
- (4) The collection of such information is of no less importance than the fundamental freedoms of the personal data subject, or it is not a case where the fundamental freedoms of the personal data subject may be greatly affected.
- (5) Whether the Company has provided appropriate measures to protect personal data storage.

1.7 To comply with the laws applicable to the Company (Base of legal duties)

In cases where the law requires the Company to collect, use or disclose personal information, the Company does not need the consent of the personal data subject. This may include processing personal data in accordance with court orders or government officials, for example, keeping personal data of employees for the purpose of complying with labor protection laws, maintaining accounting documents for a period of time as required by law, etc.

2. In case of sensitive personal data The Company may collect, use or disclose sensitive personal data **only with the expressed consent of the personal data subject.** (See Criteria and Procedures in Section 1.1) unless legal exceptions are applicable as follows:



T.S.K. FORGING CO.,LTD.

- Prevent or cease harm to the life, body or health of individuals for which the data subject is unable to give consent for whichever reason. This is often practiced in emergency.
- It is an information that is publicly available with the express consent of the personal data subject.
- It is necessary to comply with the law in order to achieve objectives relating to:
 - Preventive medicine or occupational medicine, employee competency assessment
 - Public health benefits.
 - Labor protection, social security, national health insurance, welfare related to medical treatment according to the rights of those entitled under the law which the collection is necessary for the performance of the rights or duties of the Company, or of the owner of the personal data.
 - Scientific research, studies in history or statistics, or other public interest
 - Other important public interests, such as collecting sensitive personal data for the purpose of preventing communicable diseases or epidemics. Collection and disclosure to government agencies of sensitive personal data for the purpose of anti-money laundering.

Note: Guidelines for considering and interpreting the term “Public interest” is subject to change in accordance with the guidelines for consideration and definition of the Personal Data Protection Committee, or as specified in the secondary law which may be promulgated in the future.

Details on the types, purposes and legal bases of the Company's collection of personal data are provided in the Privacy Notice for various types of personal data subjects.

3. Personal Data Collection Practices

Personal data must be collected only to the extent necessary to fulfill the purposes set forth by the Company. The Company shall consider and collect information as necessary to use and discard or destroy information that may be obtained unnecessarily, especially sensitive personal data. This is to reduce the risk of unlawful collection, use and disclosure of personal information by the Company.

In the event that the Company receives more personal information than is necessary, the Company shall seek to manage its collection of personal data only as necessary to achieve the purpose of the process, for example, in the event that the Company uses personal data to identify a partner or a representative of the Company's partner from a copy of national ID card. Normally, the Company only requires general personal information to identify such individuals (such as names and pictures). Therefore, in cases where sensitive personal information may appear on the identification card (e.g. religion), there should be a measure in prevention of such information from appearing on the card copy acquired in the possession of the Company. This could be, to cross out unnecessary information on the copy of the ID card that they received, leaving only representation of the information necessary for identification, for example.



T.S.K. FORGING CO.,LTD.

Privacy Notice for Personal Data Subjects

When the collection, use, or disclosure of personal information is being carried out, the Company will issue the Privacy Notice to the owners of various types of personal data, to clarify the details of data processing, definitions, personal data to be collected, purpose of collection, legal base of collection, collection period or expected duration, the type of person or entity to which personal information may be disclosed to, contact information of the Company, rights of the personal data subject, and other related details, in order for the owner of such personal data to acknowledge, understand and consider giving consent in the event that the collection is not legally enforced without such consent.

The Company shall notify or deliver a privacy notice to the Personal Data Subject before or while collecting the Personal Data. The notification or delivery of the privacy notice may not necessarily be repeated in the event that the Company has previously notified or delivered a privacy notice to the subject of such personal data. But in the event that the Company later amends the Privacy Notice, the Company shall notify or deliver the revised Privacy Notice to the data subject, again.

Source of Personal Information

In general, the Company must collect personal information directly from the owner of the personal data. However, if the Company collects personal data from a source other than the owner of the personal data directly, the Company will notify the personal data owner of the collection of personal data from other sources and issue the privacy notice to the personal data owner without delay, but not more than 30 days from the date of collection. The Company shall also request consent from the Personal Data Subject in the case of collecting Personal Data on the basis of consent, except in the case where the Company must use the Personal Data to contact the Personal Data Owner. The Company shall notify the owner of the information upon first contact, and in the event that the Company discloses personal information, the Company must notify the owner of the personal information before the disclosure of personal information for the first time.

However, in some cases, the Company may not be required to notify such collection and privacy notices to the personal data subject. If the Company can prove that the disclosure of such information is impracticable or would impede the Company's use or disclosure of personal information, or the owner of the personal data is already aware of the details, for example, the owner of the personal data has already received a privacy notice for certain transactions with the Company and wishes to do the same transaction with the Company, again.

In addition, if in the process of collecting, using or disclosing personal information, the Company has hired a personal data processor to act on behalf of the Company. The Company may employ a personal data processor to submit a privacy notice on its behalf. The Company shall also ensure that the processor of personal data complies with this Policy, and it is deemed that the Company has notified details of the collection, use or disclosure of personal data in accordance with the duties required by the Personal Data Protection Law as the Company's personal data controller.



T.S.K. FORGING CO.,LTD.

Rights of the Personal Data Subject

The Company should be aware that the owner of the personal data has the right to take any action on his/her personal data which is in the Company's possession, as required by the Personal Data Protection Law. Therefore, the Company must provide a request form to exercise the rights of the owner of the personal data, in order to facilitate the owner of the personal data to report the request to the Company. The Company shall keep record and notify the owner of the personal data of such refusal in writing.

1. Right to withdraw consent The owner of the personal data has the right to revoke the consent which has been previously given to the Company through a consent letter. Whether partial or complete revocation of consent, this can be done throughout the period that the Company maintains personal data. The Company must also notify the owner of the personal data upon revocation (if any). However, the revocation of consent will not affect any matters the Company has previously done as a result of obtaining the lawful consent of the personal data subject.

Reason for refusal: It is a case where there is a limitation of the right to withdraw consent by law, or the case of personal data relating to a contract rendering benefits to the personal data subject.

Response time: Without delay

2. Right to request access and obtain a copy of personal data The owner of the personal data has the right to request access and obtain a copy of his/her personal data which is under the Company's responsibility, or request to disclose the acquisition of such personal data that he/she did not give consent.

Reason for refusal: The Company may reject a request for enforcement of this right only in the following cases:

- It was done by law or court order, or
- When the Company considers that it will affect the fundamental rights and freedoms of other people

However, if there is a reason for refusing the request of the personal data subject according to the above rights, the Company will keep a record of such refusal of the request with its reasons in the Company archives.

Response time: In case the Company cannot refuse, the Company must process the request of the Personal Data Subject within 30 days from the date of receipt of the request.

3. Right to request to receive and request the transfer of personal data The owner of the personal information has the right to obtain personal information about him from the Company, or request the Company to transfer the information to another person or entity in a readable or generally usable format, including the right to receive personal information of their own that the Company or other person or organization has been transferred to collect. This request is applicable only in the event that the Company has collected, used or disclosed Personal Data with consent or to perform a contract or pre-contract request between the Personal Data Subject and the Company.



T.S.K. FORGING CO.,LTD.

Reason for refusal: The Company can refuse a request, if such personal data is used for public interest or to perform legal duties, or the exercise of such right infringes the rights and liberties of others, for example, if such information contains trade secret information or intellectual property information as part of

However, if there is a reason for refusing the request of the personal data subject according to the above rights, the Company shall maintain record on the refusal of the request with reasons in the Company archives.

Response time: 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 data in the following cases:

- (1) It is the collection, use or disclosure of personal information for lawful or public interest. This includes complying with the orders of government officials.

Ground of refusal (for Article 4 (1)): The Company can prove that there are legitimate grounds that are more important than the interests, rights or freedoms of the Personal Data Subject, or is collecting, using or disclosing personal information to establish, comply, use or defend legal claims;

However, if there is a reason for refusing the request of the personal data subject according to the above rights The Company shall maintain a record on the refusal of the request with reasons in the Company archives.

- (2) In Direct marketing case, the subject of personal data can object without any conditions.
- (3) For scientific, history or statistics research, unless it is deemed necessary for the public interests.

Response time: without delay, and in the event of no reason for refusal. the Company shall immediately separate the above personal data from other data as soon as its subject notifies on the objection.

5. Right to request deletion of personal data The owner of the personal data has the right to request that the Company delete, destroy or make the personal data non-identifiable, or render it irreversible when:

- (1) The personal data is no longer necessary to keep for its intended purpose, for the period of time that the data subject may be notified in the privacy notice;
- (2) The owner of the personal data has withdrawn his consent and the Company can no longer use other legal bases to collect the data.
- (3) The personal data subject has objected to the collection, use or disclosure of personal data, to which the Company cannot refuse to comply.
- (4) Personal information has been unlawfully collected, used or disclosed.

Reason for refusal of request: The Company has the right to reject the request in the event that personal data has been collected, used or disclosed in the following cases



T.S.K. FORGING CO.,LTD.

- It is preserved for the purpose of freedom of expression.
- For the achievement of objectives in relation to the preparation of historical or archival documents, research, statistics or public interest bases;
- It is the collection of sensitive personal data that is necessary to perform legal duties for preventive medicine purposes, occupational medicine, evaluation on the performance of employee, public benefit in relation to public health.
- Use for establishing legal claims, compliance, or the exercise of legal claims or raising the defense of legal claims
- Use to perform legal obligations

If the Personal Data is made public by the Company's actions or is transferred to another Personal Data Controller, and the owner of the personal data has a request to delete, destroy or make such information anonymous, the Company must take steps to delete, destroy or make such personal information identifiable, and must notify other personal data controllers to do the same.

Response time: without delay

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

- (1) A request has been made to the Company to correct the accuracy of the Personal Data and is in the process of verification. However, the Company may abort the suspension of such personal data, if it has verified the accuracy of the information by notifying the owner of the personal data before the cancellation with the reason.
- (2) It is an unlawful use of information, but the owner of the personal data asks to suspend the use instead of deletion.
- (3) The personal data is no longer necessary to maintain, but the data subject has asked the Company to retain the data because it is necessary to use, establish, comply with or raise the legal claim of the personal data owner himself.
- (4) The Company is in the process of proving to reject the objection of personal data. However, the Company may consider canceling the suspension of the use of personal data, if the Company deems it has the right to continue using such data on the grounds of the refusal to the right to object to the personal data mentioned above

Response time: without delay

7. Right to request correction of personal data The Personal Data Subject may request the Company to ensure that the Personal Data is accurate, current, complete and does not cause misunderstandings.

However, if there is a reason for refusing the request of the personal data subject according to the above rights, the Company shall continue to record the refusal of the request with reasons in the Company archives.



T.S.K. FORGING CO.,LTD.

Response time: without delay

8. The right to report The owner of the personal data has the right to lodge a complaint to a panel of experts appointed by the Personal Data Protection Committee when it is apparent that the Company or the processor of personal data, including employees or contractors of the Company or personal data processors, violate or fail to comply with personal data protection laws.

Obligations and Responsibilities of Personnel

All employees and personnel including persons employed and employees of persons employed by the Company is responsible for compliance with the law and this privacy policy. They must strictly maintain the confidentiality of personal information and do not use personal information obtained during the performance of work duties in an improper way used for personal gain or unlawful. The duties may be divided according to the following steps:

1. Positions of Managing Director and Executive Personnel

It is responsible for overseeing all personal data protection processes of the Company as follows:

- Promote and support the serious and concrete implementation of this Policy and Guidelines.
- Establish measures and practices relating to personal data within the Company in accordance with the law, this Policy and Guidelines including relevant international standards.
- Designate a person responsible for the implementation of this Policy and Guidelines, such as an agency or person, to determine the relevant guidelines or manuals and/or supervise the implementation of this policies and guidelines
- Provide a process to control, monitor and verify compliance with this policy and guidelines, as well as relevant instruction and operating manuals.

2. Human Resources Department

The Company has assigned the Human Resources Department (HR) to be responsible and coordinator regarding the protection of personal information of the Company. In the event that the owner of the personal data has any questions or wishes to exercise his or her rights as stipulated by law

- Prepare and update the Personal Data Protection Policy, regulations, and procedures in accordance with the Personal Data Protection Law.
- Training to educate employees at all levels to understand the protection of personal data as a personal data subject and as a collection, use or disclose the personal information of others in accordance with the law.
- Provide a confidentiality contract or the addition of information in the employment contract to contain information about the confidentiality of personal information and a letter of consent from the owner of the personal data.



T.S.K. FORGING CO.,LTD.

- Execute the request to exercise the rights of the personal data subject such as correcting, changing, destroying, deleting of personal data, as requested by the owner of the personal data along with recording the transaction according to the form specified by the Company, as well as keeping all evidence of such transaction.

3. Department manager level

It is responsible for overseeing the collection, use or disclosure of personal information within its departments, which may vary from department to department. The duties may be described as follows:

- Receive reports from subordinates in case of notification of personal data breaches, consider whether such violations may risk affecting the rights and freedoms of the personal data subject, including consulting with the person responsible for the protection of personal information of the Company, and executives to consider an order to take any action appropriate under this policy.
- Store, maintain and prevent use or disclosure of personal information for the purposes that the Company has notified the owner of the personal information, or where the owner of the personal data has given consent as set forth in this Policy and Guidelines, as well as relevant instructions and operating manuals.
- Provide measures to protect the security of personal data that are responsible for with access checks, setting a password, separate each segment of information by level of confidentiality, and the necessary to access information to use disclosure personal information in accordance with this policy.
- Clarify and encourage employees in the work unit to comply with personal data protection policies and practices, and warnings of disciplinary action in case of inappropriate conduct.
- Supervise employees in the department to strictly comply with personal data protection policies and practices.

4. Employee level position

are obliged to strictly comply with the laws and this Privacy Policy, especially in the part that is the procedure at the operational level as follows:

- Collect, use and disclose personal data in accordance with the law and this policy, including attending training on the protection of personal information of the Company
- To perform the duties assigned to the protection of personal data; In regards to the handling of personal information such as security, transfer, disclosure or recording of various information, etc.
- Notify the supervisor in the event that the collection, use or disclosure of any personal information in the Company or the order to do any such act is unlawful, or in the opinion that the collection, use or disclosure of any personal data may pose a risk of infringement of the fundamental rights and freedoms of the personal data subject.
- Notify supervisors for approval in the event of a request to exercise the rights of the personal data subject.



T.S.K. FORGING CO.,LTD.

- Immediately notify supervisors in the event of a personal data breach, whether the violation is due to the willful or negligent nature of any person; and whether the infringement may or may not have a risk of affecting the rights and freedoms of the personal data subject.

5. Contractors and service providers who process personal data of the Company

It is obligated to strictly comply with the data protection laws and this policy. It is also subject to a personal data processing contract with the Company (if any) with the following functions:

- Collect, use and disclose personal data in accordance with the law and this policy, including attending training on the protection of personal information of the Company upon request.
- Notify the Company without delay of any personal data breach. Within 24 hours of being aware of the violation
- Support and assist the Company in responding to requests for the exercise of rights of personal data subjects.

An employee's violation of the law and this policy may result in disciplinary action, and violations of the law or this policy of the contractor or service provider who processes personal data of the Company may be considered a breach of contract with the Company as well. If the violation or non-compliance with the said effect causes damage to the Company, it may regard such as grounds for termination of employment or termination of the contract. There may also be criminal penalties, including fines and jail terms, for those acting on behalf of companies that violate or fail to comply with the law. Employees and related parties are required to study the Personal Data Protection Law and this Policy, and strictly follow.

Measures to Protect Personal Information

The Company must provide appropriate policy and technical security measures to prevent the loss, access, use, alteration, alteration or disclosure of personal data without authorization or abuse, and such measures must be reviewed when necessary or when technology changes in order to be effective in maintaining appropriate security, according to the standards prescribed by law as follows:

1. Policy measures

- 1.1 The Company shall supervise, inspect, assign, monitor the collection, use or disclosure of personal information in accordance with the requirements of the law, and security of information personal in terms of secrecy Accuracy and Availability of Personal Data.
- 1.2 The Company shall assign access rights and enter into confidentiality agreements with persons who need to know personal information.
- 1.3 The Company shall annually train and educate employees on personal data protection.
- 1.4 The Company shall regularly review the consistency of personal data security measures, in accordance with the standards of the Personal Data Protection Law.



T.S.K. FORGING CO.,LTD.

- 1.5 Use and Disclosure of Sensitive Personal Information both within and outside the Company must be approved by the Human Resources Manager only.
- 1.6 The Company shall conduct an internal audit (Internal audit) of the employees' performance in accordance with this manual / policy on personal data protection, at least on a yearly basis.

2. Practical measures for users of personal data

Persons who have the right to access, use, modify, change, disclose personal information providing the scope of the use of the information according to the position, duties or terms of the contract and under the permission of the Company, such as permanent employees, temporary employees, contractors, etc. Users of personal data are obliged to secure information from access, modify, alter, disclose or destroy information unlawfully or without authority;

- 2.1 Able to collect, use and disclose personal information according to duties and responsibilities or as assigned by the Company only.
- 2.2 Access, use and disclose personal information according to the Company or set by the administrator only.
- 2.3 Perform its duties by taking various actions to prevent the loss, unauthorized access, use, disclosure, correction, alteration of personal data.
- 2.4 When not in use or in continuous use, personal data must be stored securely, such as locking drawers, desks, or room locks.

3. Guidelines on Information Systems/Other Relevant Issues

- 3.1 Personal data must be stored in secure and encrypted storage devices, **especially sensitive personal data**. The personal data document must specify the place of storage. Storage period is appropriate including designated key collectors to access storage locations.
- 3.2 When personal data is no longer used or there is no legal ground to keep it, must be deleted or destroyed by means of shredding or destruction according to the nature of the device. If documented personal data must be destroyed using a shredder, as for digital data, files that are in trash or formatted must be deleted so that data cannot be recovered. In the case of digital devices that can no longer be used, it has to be broken or placed in the grinder so that it cannot be used again.
- 3.3 Employees who use portable computers or movable equipment must not be left unattended, unless these devices are tethered to a desk, or stored in a locked cupboard or drawer.
- 3.4 The Company does not allow employees to use the recording device, unless the device is authorized by the Human Resources Department. And whenever personal data is stored on an external hard disk, thumb drive, these storage devices must be stored securely and locked in a locked archive.



T.S.K. FORGING CO.,LTD.

- 3.5 Employees must be careful not to inadvertently disclose personal information to persons who do not need to use it. All employees must store sensitive information in a work area where there is no third party, or unauthorized persons in the area. In the event that an unauthorized person is in an area where the computer screen or display device can be seen, Data users must use Screen Saver, log-off, or take any action with the same effect. And computers that store important data must have a password to use to access the data.
- 3.6 For the right to access personal data from outside, such as working from home, this must be considered by the Human Resources Manager before employees can initiate external use, and in off-site work Employees must exercise caution to protect the Company's assets, both hardware and software, from being stolen, lost, etc., including using only devices that are authorized by the Company.
- 3.7 Employees are prohibited from bringing personal computer equipment or devices that are not the Company's property to work on the Company premises unless approved by the Company.
- 3.8 Employees are prohibited from using personal email such as GMAIL or Outlook to use instead of the Company's email for sending and receiving information in the Company's work, or used to communicate within and outside the Company except when authorized by IT and personnel departments.
- 3.9 The Company will record video from CCTV in various areas of the Company, in case of an unforeseen incident. It will continuously record, if the data is full, it will overwrite the oldest. The storage period is 6 months, the administrator must collect information from the CCTV, keep it a secret and will not disclose, transfer or modify such information to anyone, except subsidiary affiliates we carefully select, third parties now and in the future.
- 3.10 Access to the various systems must be made using personally identifiable User-IDs and Passwords. To prevent unauthorized use and prohibit employees from sharing their own password to others.
- 3.11 In the event that employees do not use computers, they must log-off out of the system, which will prevent unauthorized persons from seeing the information on the screen.
- 3.12 After printing, personal data must not be left on the printer.
- 3.13 Attempting to access the system, any unauthorized hacking, attempting to guess a password, attempting to decrypt (file decryption), hacking a copy of the data, or any compromising on system security is a serious disciplinary offense.
- 3.14 Employees who wish to request User IDs or modify the right to use must submit documents/forms for approval from the Human Resources Manager.
- 3.15 Administrators must not grant access rights to employees or anyone, if the procedure is not allowed.
- 3.16 If there is a change in the position of the employee, the right to access the various systems must be changed according to the new position of the employee in the event of a transfer or change of position.



T.S.K. FORGING CO.,LTD.

- 3.17 In the event that the employee terminates the employment contract for any reason, all assets of the Company must be returned, and the right to access the various systems will be terminated immediately.
- 3.18 Employees' computers must install Anti-Virus program and employees must update the version regularly according to the Company's regulations.
- 3.19 The use of various information technology systems must be protected through the use of Firewall at all times when connected on the Internet as specified by the Company.
- 3.20 Third parties (Visitor) who are allowed to enter the storage room must register according to the system of the Company, and must be supervised by IT staff at all times.
- 3.21 There shall be a record of the details of the deletion or destruction of personal data such as methods of destruction, amount of data destroyed, destructive effect check. This ensures that personal data that has been destroyed will not be accessed and can be recovered.
- 3.22 Request for use and disclosure of sensitive information requires MD approval to proceed.
- 3.23 The internal audit unit shall conduct an audit that must at least cover the requirements specified in the above measures at least once a year.

4. Measures for managing the risks of personal data

Where there may be a high risk of personal data breach, such as a breach of sensitive information. The Company may assess the risks and provide protective measures on a case-by-case basis.

Recording, Use and Disclosure of Personal Information

The Company must keep a record of the use and disclosure of the information collected with at least the following items:

- Personal data collected including the purpose and duration of storage.
- Use or disclosure of personal data in the event of collecting data on a legal basis other than obtaining consent.
- Rights and methods and conditions for the right of access to the data of the personal data subject.
- Refusal or objection to various types of exercise requests with the reasons stated in this Policy; and
- Description of the security measures provided by the Company.

In order for the owner of the personal data to be able to verify and can enforce the rights that the owner of the personal data informs or requests to the Company



T.S.K. FORGING CO.,LTD.

Transfer of Personal Data to Foreign Countries or International Organizations

The Company can transfer personal data abroad in the following cases:

1. The destination country has been certified to have adequate personal data protection standards.
2. In case the destination country has insufficient standards, the transfer of personal data is subject to legal exceptions,

including:

- It is a legal practice.
- Consent of the personal data subject has been informed of the insufficient standards of the destination country or organization.
- It is necessary to perform the contract to which the Personal Data Subject is a party, or to proceed with the request before entering into the contract.
- It is the performance of a contract between the Company and another person or entity for the benefit of the Personal Data Owner.
- To prevent or cease harm to the life, body or health of the personal data subject or other persons when the owner of the personal data is unable to give consent at that time.
- It is necessary to carry out missions for the benefit of the public.

3. In the case of transfer of information between foreign persons or juristic persons who are in the same business group The Company may transfer personal information between each other without having to perform the actions set out above. The Company must have a personal data protection policy for the transmission or transfer of information between the same business group that has been audited and certified by the Office of the Personal Data Protection Commission. (Currently, the Company does not have a policy on the transmission of personal information between its affiliates.)

At present, the committee has not yet established a country with sufficient standards and has not adopted a policy on the transfer of personal data among its affiliates. However, the Company can still transmit personal data abroad or international organizations. If the Company has put in place appropriate personal data protection measures, the rights of the personal data subject can be enforced, as well as having effective legal remedy measures in accordance with the standards prescribed by the law. At present, the law has not set any such standards, therefore, the Company can proceed with the transfer of personal data in accordance with the conditions set forth in Article 2 until further laws are promulgated in such matters.

Employees, managers or executives of the Company that wish to send or transfer personal data abroad must be considered by the Human Resources Department for approval before proceeding.



T.S.K. FORGING CO.,LTD.

Actions on a Personal Data Breach

When a personal data breach occurs within the Company where there is a risk of infringement that affects the rights and freedoms of the personal data subject. All employees and personnel must coordinate with each other to ensure compliance with the law. The Company shall notify such violation to the Office of the Personal Data Protection Commission without delay within 72 hours from the moment of knowing the cause as far as practicable. In the event of infringement that present a high risk of affecting the rights and freedoms of the personal data subject, the Company shall notify the incident to the owner of the personal data with the remedy without delay.

Amendments to the Privacy Policy

This Privacy Policy may be amended as appropriate, according to the changes in the law and business suitability.

Note: This Privacy Policy was last revised on [June 1st, 2022]

Inquiry and Report of Personal Data Breach

In case of inquiries relating to the protection of personal data or if you wish to report a breach of personal data, kindly contact:

Human Resources Department, T. S. K. Forging Company Limited

Address: 700/61 Moo 6, Tambol Bankao, Amphur Phanthong, Chonburi 20160

Telephone: 038-214238-9 extension 113-4,

Administrative and Personnel Department, Email: hr@tskgroup.net