Don Muang Tollway Public Company Limited

ISO 9001, ISO 14001, ISO 45001 & ISO/IEC27001 CERTIFIED

Announcement No. 52/2567

Office of the Managing Director

Privacy Policy

(Revised Edition 2/2567)

Don Muang Tollway Public Company Limited ("the Company") recognizes the importance of personal data protection, which is a fundamental right to privacy that must be protected in accordance with the Personal Data Protection Act B.E. 2562 (2019) and other related laws. To effectively protect personal data and provide remedies for violations of personal data rights, the Company has issued this policy as a principle for protecting personal data collected, used, or disclosed by the Company, as follows:

1. Definition

the Company	Don Mueang Tollway Public Company Limited
Employee	Director, personnel, staff, or employee of Don Mueang Tollway Public Company Limited.
Authorized Person	A person assigned by the Company to have the authority to grant any approval within the scope of authority received from the Company.
System Administrator	An agency or person assigned by the Company or the data subject to be responsible for overseeing a particular work system.
Data Subject	An individual who can be identified, directly or indirectly, by that personal data.
Personal Data	Information about an individual that enables the identification of that person, whether directly or indirectly, but does not include the information of a deceased person. For example, name, surname, email, photo,

	fingerprint, national ID number, which can directly identify a person, or can indirectly identify a person, such as address, gender, and age, which when combined can identify a person.
Special Category Personal Data	Personal data relating to race, ethnicity, political opinions, beliefs in a creed, religion or philosophy, sexual behavior, criminal records, health data, disability, labor union information, genetic data, biometric data, or any other data as announced by the Personal Data Protection Committee.
Public Data	Personal data that the data subject has disclosed to the public, such as social media profile information, when using social media credentials like Facebook, Twitter, or Line to connect to or access any of the Company's services. This includes Social Media Account ID, interests, likes, and the data subject's friend list, which the data subject can control the privacy of through the social media account settings provided by the respective social media provider.
Data Controller	A person or legal entity who has the authority to make decisions about the collection, use, or disclosure of personal data.
Data Protection Officer (DPO)	An officer appointed by the Data Controller to act as the Data Protection Officer in accordance with the Personal Data Protection Act B.E. 2562 (2019).
Data Processor	A person who processes the collection, use, or disclosure of personal data under the order or on behalf of the Data Controller. However, the person or legal entity carrying out such processing must not be the Data Controller.
Data Processing	Any operation performed on personal data or a set of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Business Partner	A counterparty who is a business partner of the Company or works with the Company.

2. Roles and Responsibilities

- 2.1 The Board of Directors is responsible for overseeing the protection of personal data in compliance with relevant laws and regulations.
- 2.2 Senior Management is responsible for managing and controlling operations related to the collection, use, and disclosure of personal data to be in accordance with the law and official regulations, ensuring effective data security, and assigning supervision of policy compliance, with the authority to approve amendments or reviews of this policy.
- 2.3 Employees have the duty to strictly comply with this policy, its guidelines, procedures, manuals, and the Company's orders, as well as all relevant laws and official regulations.

3. General Provisions

General Requirements

- 3.1 The protection of personal data under this policy covers all personal data collected by the Company, including the personal data of customers, partners, shareholders, and stakeholders of the Company as required by law, whether they are natural persons or legal entities, as well as the personal data of employees and external individuals who provide personal data to the Company for any operational purpose, such as recipients of the Company's scholarships.
- 3.2 The Company may update, review, or amend this policy, in whole or in part, from time to time to align with the Company's operational guidelines, good governance, and social responsibility. The Company and relevant departments will review this policy at least once a year, or when there are amendments to laws, rules, and regulations related to personal data protection law, or when there is a significant change in guidelines affecting the implementation of this policy. The Company will announce any changes on its website at https://www.tollway.co.th.
- 3.3 The Company will provide a privacy notice detailing the processing of personal data to the data subject before or at the time of collecting personal data, as required by law.
- 3.4 The Company will process personal data based on a lawful basis under Sections 24 and 26 of the Personal Data Protection Act, such as consent, legal obligation, legitimate interest, or contractual basis.

- 3.5 The Company will process personal data only as necessary for lawful purposes and within the period prescribed by law, for legitimate purposes consistent with the legal basis.
- 3.6 The Company will delete, destroy, or anonymize personal data when the retention period ends, when it is no longer necessary for the purpose for which it was collected, upon the data subject's request, or upon the data subject's withdrawal of consent, unless there is a legitimate legal or regulatory reason for the Company to retain such data.
- 3.7 The Company securely maintains personal data, taking into account the privacy of the data subject and the confidentiality of the personal data.
- 3.8 The Company will process personal data responsibly in accordance with the principles prescribed by law.

4. Collection and Processing of Personal Data

Sources of Personal Data

- 4.1 Personal data received directly from the data subject.
- 4.2 Personal data from third parties, such as the Department of Highways, the Expressway Authority of Thailand, the data subject's affiliated organization, or the Securities and Exchange Commission, etc.
- 4.3 Personal data received from website visits, such as the name of the internet service provider and IP Address used to access the internet, date and time of the website visit, pages visited on the site, and the address of the website that linked directly to the Company's website.
- 4.4 Personal data received from public and non-public records that the Company is legally entitled to collect.
- 4.5 Personal data received from government agencies and regulatory bodies exercising their legal authority.

Personal Data Processed

General personal data collected by the Company includes:

- General information of tollway users: Vehicle registration, vehicle image, vehicle information, name, surname, national ID number, address, phone number, still images, and moving images.
- General information about job applicants, employees, and interns: Name, surname, educational background, employee ID, job title, facial image, national ID number.
- Contact information: Email address, phone number, date of birth, gender.
- Information of business partners/contractors/service providers/shareholders/proxies: Copy of national ID card, copy of house registration, copy of passport, which does not contain sensitive personal data.
- Information of drivers violating the law: Name, surname, address, gender, vehicle/motorcycle registration, nationality, still images, moving images.

Sensitive personal data collected by the Company includes:

- Information on work-related/traffic accident reports on the tollway.
- Information of persons with disabilities supported by the Company's training grants: ID card for persons with disabilities, disability information, etc.

5. Main Purposes for Collecting, Using, or Disclosing Personal Data

The Company will collect your personal data only as necessary for its operations. The Company may have different purposes for processing personal data depending on the case, as follows:

1. To provide tollway services and carry out the Company's objectives.
2. For the purpose of communication or coordination in the Company's operations or missions with external parties.
3. To comply with laws related to the Company's operations and lawful orders of government agencies and relevant officials.
4. For auditing and security purposes, and to prevent illegal acts or fraud.
5. To serve as a database for the Company's business operations.

6. To be used as evidence in transactions and to comply with financial regulations, issuing invoices, tax invoices, making payments, as well as various financial transactions and the Company's accounting procedures.
7. For public relations to disseminate information, news, and activities of the Company, such as training, meetings, seminars, company projects, and social activities, to relevant parties.
8. To provide welfare for the Company's employees or personnel.
9. For the purpose of verifying or identifying you when accessing or using various services, entering into contracts, fulfilling contracts, and to ensure that all such service usage and communications with the Company are secure and confidential.
10. For debt collection, establishing legal claims, or defending against legal claims, such as investigations and/or inquiries by government officials, case preparation, legal proceedings, and/or litigation in court.
11. To serve as a record for the Company's operations.
12. To enter into or perform any contract of the Company.
13. For marketing purposes.

The personal data the Company collects for the above purposes is necessary for the performance of a contract or for compliance with applicable laws. If you do not provide the necessary personal data, it may be a violation of the law, or the Company may not be able to provide services, manage contracts, or facilitate various operations for you.

If there is a change in the purposes of collecting personal data in the future, the Company will notify you and take any other actions required by law, including keeping a record of the amendment as evidence.

6. Obtaining Consent from the Data Subject

6.1 The Company will obtain explicit consent for the collection, use, or disclosure of personal data from the data subject in writing or through an electronic system, unless the nature of the situation does not allow for consent to be obtained in such a manner.

6.2 The data subject will be informed of the purposes for collecting, use, or disclosure of personal data clearly, in an easily understandable manner, not deceptively or in a way that

misleads the data subject about the purpose, and with the utmost consideration for the data subject's freedom in giving consent.

6.3 If the data subject is a minor who has not reached legal age by marriage or does not have the status of a person who has become sui juris, the Company will obtain consent from the person exercising parental power who has the authority to act on behalf of the minor.

6.4 If the data subject is an incapacitated person, the Company will obtain consent from the guardian who has the authority to act on behalf of the incapacitated person.

6.5 If the data subject is a quasi-incompetent person, the Company will obtain consent from the curator who has the authority to act on behalf of the quasi-incompetent person.

6.6 If the data subject, or the authorized person under clauses 6.3, 6.4, and 6.5, wishes to withdraw previously given consent, they can do so as easily as giving consent. If the withdrawal of consent affects the data subject in any way, the Company will inform the data subject of the consequences of such withdrawal.

6.7 The Company will collect, use, or disclose personal data only for the purposes notified to the data subject. The collection, use, or disclosure of personal data for purposes different from those notified is not permitted, unless additional purposes have been notified in accordance with the rules and conditions prescribed by law that allow the Company to do so for legal and litigation benefits in cases where the data subject is a stakeholder of the Company, and it shall be deemed that the data subject has been informed and has consented.

7. Access to and Use of Personal Data

7.1 The Company will authorize employees to access or use personal data only as necessary for their job performance and according to the rights specified by the Company. If an authorized employee needs to access personal data beyond the specified rights for their work, they must seek approval only from the Company's authorized person.

7.2 The Company will ensure that authorized employees use personal data only for the purposes for which it was collected or as consented to by the data subject, unless supported by a lawful basis.

7.3 The Company will ensure that the system administrator allows authorized employees to access personal data only according to their specified rights or with approval from the Company's authorized person.

8. Disclosure and Receipt of Personal Data

8.1 The Company will seek consent from the data subject for the disclosure of personal data to external individuals or organizations, unless it is in compliance with other laws. The Company will disclose personal data to third parties and/or external organizations or agencies only in the following cases:

8.1.1 Business partners and/or external service providers to offer benefits and other services of the Company to the data subject, including the development and improvement of the Company's products or services, such as data analysis, data processing, information technology services and related infrastructure preparation, platform development for customer service, sending emails/SMS, website development, mobile application development, satisfaction surveys and research, and customer relationship management. A Data Processing Agreement (DPA) and a Non-Disclosure Agreement will be established to ensure security and confidentiality. In the case of legal entities, they must have acceptable personal data protection standards.

8.1.2 Government agencies, government bodies, officials with legal authority in civil, criminal, and administrative matters, as well as any other organization established by law, to comply with laws, orders, and requests, and for coordination with various agencies on matters related to legal compliance.

8.2 The Company will ensure that personal data received from external individuals or organizations has a lawful basis, unless it is for compliance with the law. The Company will collect data that the data subject has provided directly to the Company or personal data that the

Company has received from its services or operations through all channels, including the following:

8.2.1 Information received when the data subject registers or fills out an application to participate in the Company's activities or use other services, such as name, surname, national ID number or other identification card numbers, phone number, date of birth, address, email, etc.

8.2.2 Data from membership registration or participation in activities, data for creating a user account profile containing personal details provided to the Company to access services through the Company's service channels, such as mobile applications and/or through the Company's website, including online accounts or application accounts providing the Company's services, as well as personal data provided for various registrations, such as joining activities and/or contacting the Company via the website or other channels specified by the Company.

8.2.3 Data from subscribing to newsletters, participating in surveys, or information from joining various activities, such as satisfaction, interests, or consumption behavior.

8.2.4 Information about transactions with the Company or about legal obligations between the Company and third parties, such as job application data, agent application data, information for bidding, which includes credit or debit card information, bank account numbers, or other banking or payment information, including the date and time of payment, depending on the type of transaction of the data subject.

8.2.5 Data from visiting or using the Company's website or applications operated by or for the Company, data from social media use and interaction with the Company's online advertisements, model and type of web browser used, type of device used to access services (such as personal computers, laptops, or smartphones), operating system and platform information, IP address of the device or terminal equipment, location data, and information about the services and products that the data subject viewed or searched for.

8.2.6 Data from records of the data subject's contact with the Company, which is stored in the form of service user's message logs, satisfaction assessments, research and

statistics, or voice or video recordings via CCTV when the data subject contacts the Company, such as the Company's customer service center, as well as information provided through various research media such as SMS, Social Media, applications, or email.

8.2.7 Social media profile data when using social media credentials such as Facebook, Twitter, and Line to connect or log in to any of the Company's services, such as Social Media Account ID, interests, likes, and the data subject's friend list, which the data subject can control the privacy of through the social media account settings provided by the respective social media provider.

8.3 In cases where the Company engages an external person or organization to collect, use, or disclose personal data on behalf of the Company (a data processor), the Company will use a data processor that has appropriate and equivalent security measures to the Company's standards. The Company will establish an agreement between the parties to control the data processor's operations to be in accordance with the law, clearly defining the purpose or instructions for collecting, using, or disclosing personal data to the data processor, and setting measures to prevent the data processor from collecting, using, or disclosing personal data received from the Company for purposes other than those specified or instructed by the Company.

9. Sending or Transferring Personal Data Abroad

In the event the Company sends or transfers personal data abroad, the Company will establish standards for agreements and/or business contracts with individuals or entities. The individual or organization receiving the personal data must have an accepted standard of personal data protection that is consistent with relevant laws to ensure that the personal data is securely protected, for instance:

9.1 In cases where the Company needs to store and/or transfer personal data for storage.

9.2 For processing in the cloud, the Company will consider individuals or organizations with international security standards and will store personal data in an encrypted format or by other methods that cannot identify the data subject.

Furthermore, the data subject can check the list of third parties to whom the Company will disclose personal data at www.tollway.co.th. This list of third parties may increase or decrease, and the Company will keep the information updated.

10. Personal Data Security Measures

Protecting the security of your personal data is important. The Company agrees to retain your personal data for as long as necessary for the purposes specified in this privacy policy, in a secure storage location, and will take necessary measures to protect the stored personal data from misuse, loss, unauthorized access, alteration, or disclosure.

Overall, the Company has established internal practices to define rights to access or use the data subject's personal data to maintain confidentiality and security. The Company will review these measures periodically for appropriateness, in line with industry standards and relevant laws.

The measures to prevent access or control the use of personal data will consist of at least the following actions:

1. Security measures must cover the collection, use, and disclosure of personal data in accordance with the Personal Data Protection Act, whether such personal data is in paper, electronic, or any other format.
2. Security measures consisting of appropriate organizational measures, technical measures, and, where necessary, physical measures.
3. Actions regarding the identification of significant risks that may arise with information assets, the prevention of significant potential risks, the monitoring and surveillance of threats and personal data breaches, incident response upon detection of threats and personal data breaches, and the restoration of damage caused by threats or personal data breaches as necessary, appropriate, and feasible according to the level of risk.
4. Security measures that must take into account the ability to maintain the confidentiality, integrity, and availability of personal data appropriately according to the level of risk, considering technological factors, context, environment, accepted standards for entities or businesses of the same or similar type, the nature and purpose of the collection, use, and disclosure of personal data, and the resources required.

5. For the processing of personal data in electronic form, security measures must cover the various components of the information system involved in the collection, use, and disclosure of personal data, such as systems and equipment for storing personal data and various devices used appropriately according to the level of risk, considering the principle of defense in depth, which should consist of multiple layers of security controls.
6. Security measures related to accessing, using, altering, amending, deleting, or disclosing personal data shall consider the necessity of access and use according to the nature and purpose of the collection, use, and disclosure of personal data, security according to the level of risk, and the resources required. Such security measures must, at a minimum, consist of the following actions as appropriate to the level of risk: a) Access control to personal data and critical information system components, with identity proofing and authentication, and appropriate authorization or assignment of rights to access and use, considering the need-to-know basis and the principle of least privilege. b) Appropriate user access management, which may include user registration and de-registration, user access provisioning, management of privileged access rights, management of secret authentication information of users, review of user access rights, and removal or adjustment of access rights. c) Defining user responsibilities to prevent unauthorized or unlawful access, use, alteration, amendment, deletion, or disclosure of personal data, including actions outside their assigned roles, as well as unauthorized or unlawful copying of personal data and theft of devices for storing or processing personal data. d) Providing methods to allow for retrospective auditing of access, alteration, deletion, or transfer of personal data, consistent and appropriate with the methods and media used for collecting, using, or disclosing personal data.
7. Security measures must include raising awareness of the importance of personal data protection and security (privacy and security awareness), and appropriately communicating policies, practices, and measures for personal data protection and security to individuals who are users or are involved in accessing, collecting, using, altering, amending, deleting, or disclosing personal data, for their knowledge and compliance, including when there are updates or amendments to such policies, practices, and measures, taking into account the nature and purpose of the collection, use, and disclosure of personal data, the level of risk, the resources required, and the feasibility of implementation.

Third parties acting as data processors for the Company must act on the Company's instructions and agree to maintain the security of the personal data.

11. Rights of the Data Subject

The data subject has the following rights:

- The right to be informed of the existence, nature, and purpose of the use of their personal data by the Company.
- The right to access and request a copy of their personal data, for which the Company will have appropriate procedures for you to verify your identity with the Company first.
- The right to request correction or changes to their personal data to be accurate, current, complete, and not misleading.
- The right to object to the collection, use, or disclosure of personal data concerning them, including the right to object to the processing of personal data.
- The right to request the temporary or permanent suspension of the use or disclosure of personal data concerning them, by providing written notice to the Company.
- The right to request the deletion or destruction of personal data concerning them, or to have the personal data be made unidentifiable to the data subject.
- The right to request disclosure of the acquisition of personal data concerning them, in cases where the data was collected or stored without the user's consent.
- The right to withdraw consent previously given to the Company for the collection, use, or disclosure of personal data, which must be notified in writing to the Company. The withdrawal of consent will not affect the collection, use, or disclosure of the data subject's personal data for which consent has already been given, nor will it affect the collection, use, or disclosure of personal data in cases where the Company can proceed for legal and litigation benefits as prescribed by law, or for reasons of necessity under clauses 3.3 and 3.4.
- The right to lodge a complaint with the relevant government agency for personal data protection if you believe that the Company's collection, use, and/or disclosure of personal data is unlawful.

The Company has established contact channels for you to exercise your rights as detailed in Section 17. The Company will process and consider the data subject's request within 30 days from

the date of receiving such a request. The rights mentioned above are as prescribed by the Personal Data Protection Act. However, the Company may refuse to act on the data subject's rights as permitted by law or by the contract made with the Company, in cases where it would cause the data subject to lose various benefits.

Furthermore, the deletion or destruction, or the rendering of personal data into a form that cannot identify the data subject, or the withdrawal of consent by the data subject, can only be done under the provisions of the law and the contract made with the Company. Exercising such rights may affect the performance of contracts made with the Company or the provision of other services, as it will not be possible to identify the data subject, which may lead to limitations in providing certain services that require personal data and may result in the data subject no longer receiving benefits, services, and news from the Company.

12. Retention Period and Location of Personal Data

The Company will retain personal data for as long as is necessary for the purposes of collection, use, and disclosure of personal data as specified in this privacy policy or in each specific privacy notice. The criteria used to determine the retention period include the period during which the Company still has a relationship with you as a customer of the Company and may continue to store it for the period necessary to comply with the law or legal statute of limitations, for the establishment of legal claims, compliance with the law or the exercise of legal claims, or to defend against legal claims, or for other reasons according to the Company's internal policies and regulations. The Company will store and have security measures in place to protect the data in an appropriate storage location according to the type of personal data. The Company will retain personal data for a period that you can reasonably expect according to the standards of collection, for example, not exceeding the general legal statute of limitations of 10 years.

13. Use of Personal Data for Marketing Purposes

Subject to the provisions of the law, the Company will use personal data for marketing purposes, such as sending documents about various promotions by post, email, and by any other means, including direct marketing, to enhance the benefits that the data subject will receive from being a customer of the Company through the recommendation of relevant services.

The data subject can choose not to receive communications for marketing purposes from the Company, except for communications related to the data subject and/or services that the Company has provided to the data subject, such as receipts, tax invoices, withholding tax certificates, etc.

14. Cookies

The Company will use cookies or similar technologies to collect information about the use of the website and applications by the data subject to store data and compile statistics, conduct research, analyze trends, and to improve the quality and control the operation of the website and/or application for more convenient visits to the Company's website. The Company will provide further details in its Cookie Policy.

15. Links to External Websites

The Company's website will contain links to third-party websites, which may have privacy policies different from the Company's. Data subjects are encouraged to study the personal data policies of those websites to understand the details of personal data protection and to decide on the disclosure of personal data. The Company will not be responsible for the content, policies, damages, or actions caused by third-party websites.

16. Data Protection Officer (DPO)

The Company has appointed a Data Protection Officer to inspect and provide advice on the processing of personal data, as well as to coordinate and cooperate with the Personal Data Protection office to comply with the Personal Data Protection Act B.E. 2562 (2019).

17. Penalties

Employees and personnel of the Company who are responsible for carrying out any matter according to their duties, if they violate the personal data protection policy, practices regarding personal data, and as stipulated by the Personal Data Protection Act B.E. 2562 (2019), may be subject to the Company's disciplinary action.

Furthermore, if such actions cause damage to the Company and/or any other person, the Company may consider taking further legal action.

18. Contact Channels

If the data subject wishes to contact, has questions, or wants to inquire about the details of the collection, use, and/or disclosure of personal data, including the rights and the exercise of the data subject's rights under this privacy policy, or wishes to withdraw consent for the collection, use, and/or disclosure of personal data, or if it is found that the data subject's personal data has been used unlawfully, you can contact Don Mueang Tollway Public Company Limited or the Company's Data Protection Officer at the following details:

18.1 Data Controller

Don Mueang Tollway Public Company Limited

Address: 40/40 Vibhavadi Rangsit Road, Sanambin Sub-district, Don Mueang District, Bangkok 10210

Website: www.tollway.co.th

Call Center: 1233

18.2 Data Protection Officer

Address: 40/40 Vibhavadi Rangsit Road, Sanambin Sub-district, Don Mueang District, Bangkok 10210

Email: dpo@tollway.co.th

Phone Number: 02-792-6500 ext. 6331

The Company hereby announces this for general acknowledgment.

This shall be effective from July 17, 2024.

Announced on July 17, 2024.