TM TECHNOLOGY SERVICES SDN BHD
CERTIFICATE AUTHORITY
(TMCA)
Privacy Plan
VERSION 1.0
TMTECH-PRV-001

DATE OF PUBLICATION: 3rd JULY 2024

Notice
This document and its contents are intended for public use. Reverse engineering of any part or all of the information in this document is strictly prohibited. The copyright notice does not indicate publication of this document.

Revision History

Date	Version	Modification Type	Item/ Ref.No.	Description	Author
3rd July, 2024	1	New		Approved for publication.	TMCA CPS Committee

Reviewed by

Name: Nazman Fariz Mohd Noh

Designation: AGM ESS CYDEC

Date: : 3rd July 2024

Approved by

Name: TMCA CP CPS Committee

Designation: TMCA CP CPS Committee

Date: : 3rd July 2024

TOC

Contents

1 Data Collection 5
2 Purpose of Data 5
2.1 Names, copy of NRIC/Military ID/Passport 5
2.2 Email Addresses 5
2.3 Telephone Number 5
2.4 Organizational Affiliations 5
2.5 Other Relevant Contact Information 6
2.6 CTC eInfo SSM (Company Search Report from Suruhanjaya Syarikat Malaysia) and Letter of Proxy on Company Letterhead 6
3 Use of Data 6
3.1 Verification of Identity 6
3.2 Communication 7
3.3 Authorization and Affiliation 7
3.4 Legal Compliance 7
4 Security and Trust 7
5 Data Retention 7
6 Data Security 8
6.1 Encryption 8
6.2 Access Controls 8
6.3 Secure Storage 8
6.4 Regular Security Audits 8
6.5 Incident Response 9
6.6 Employee Training 9
7 Compliance with Standards 9
8 TMCA Data Sharing Statement 9
8.1 General Principles 9
8.1.1 Service Providers 10
8.1.2 Law Enforcement and Regulatory Authorities 10
8.2 Your Rights 10
8.2.1 Changes to this Data Sharing Statement 10
8.2.2 Individual Rights 10
8.2.3 What Personal Data Do We Collect? 10
8.3 Your Rights Regarding Your Personal Data 11
8.3.1 Right to Access 11
8.3.2 Right to Rectification 11

8.3.3 Right to Erasure (Right to be Forgotten) 11
8.3.4 Right to Restrict Processing 11
8.3.5 Right to Data Portability 11
8.4 Exercising Your Rights 12
8.4.1 Verification Process 12
8.4.2 Exceptions to Your Rights 12
8.5 Changes to this Individual Rights Statement 12
9 Compliance with Malaysian Personal Data Protection Act (PDPA) 12
9.1 Data Protection Principles 12
9.2 Registration with PDPC 12
9.3 Limited Data Collection 13
9.4 Data Security Measures 13
9.5 Data Retention 13
9.6 Individual Rights 13
9.7 Changes to this Compliance Statement 13
10 Policy Updates 13
10.1 Policy Updates and Communication 13
10.1.1 Posting the updated CPS on our website 13
10.1.2 Direct notification 14
10.1.3 Public announcement 14
10.2 Frequency of Updates 14
10.2.1 Changes in Law or Regulations 14
10.2.2 Changes in Our Practices 14
10.2.3 New Technologies or Services 14
11 Your Continued Use of Our Services 14
12 Information Treated as Private 14
13 Information Not Deemed as Private 14
14 Responsibility to Protect Private Information 15
15 Notice and Consent to Use Private Information 15
16 Disclosure Pursuant to Judicial or Administrative Process 15
17 Contact Information 15

Privacy Plan

1 Data Collection

Details on what personal information is collected from certificate applicants. This may include

a) names,
b) copy of NRIC/MyTentera/passport and number
c) email addresses
d) telephone number
e) organizational affiliations
f) other relevant contact information.

2 Purpose of Data

2.1 Names, copy of NRIC/Military ID/Passport

The collection of names and copies of identification documents such as NRIC, Military ID, or Passport is essential to verify the identity of the certificate applicant. This information ensures that the certificate is issued to the correct individual or authorized representative of an organization, thereby enhancing the trustworthiness and security of digital transactions and communications.

2.2 Email Addresses

Email addresses are collected to facilitate communication with the certificate applicant throughout the certificate issuance process. They are used for sending notifications, updates, and verification requests related to the application, issuance, renewal, or revocation of digital certificates. This ensures timely and secure correspondence between the TMCA and the certificate applicant.

2.3 Telephone Number

The collection of telephone numbers enables the TMCA to contact the certificate applicant quickly and efficiently when necessary. It may be used to verify information provided during the application process, confirm identity, or address any issues that arise during certificate issuance or management. This enhances the security and reliability of the certificate issuance process.

2.4 Organizational Affiliations

Information regarding organizational affiliations is gathered to accurately attribute digital certificates to the respective organizations or entities. This helps in verifying the legitimacy and authority of the certificate applicant to act on behalf of their organization, ensuring that digital certificates are issued to authorized personnel and entities only.

2.5 Other Relevant Contact Information

Additional contact information, such as mailing addresses or secondary email addresses, may be collected to ensure comprehensive communication capabilities between the TMCA and the certificate applicant. This information supports efficient correspondence and facilitates the management of digital certificate-related inquiries, updates, and notifications.

2.6 CTC eInfo SSM (Company Search Report from Suruhanjaya Syarikat Malaysia) and Letter of Proxy on Company Letterhead

The collection of Certified True Copy (CTC) of eInfo SSM and Letter of Proxy on Company Letterhead is necessary to verify the legal status and authorization of the certificate applicant within their organization.

These documents help confirm that the applicant has the authority to request and manage digital certificates on behalf of the company, ensuring that certificates are issued to authorized personnel only and aligning with regulatory requirements.

These purposes collectively support the TMCA's commitment to verifying identities, ensuring the integrity of digital certificates, maintaining communication with certificate applicants, and upholding security standards in digital transactions and communications.

3 Use of Data

At TMCA, we collect various types of personal and company information from certificate applicants to facilitate the issuance, management, and verification of digital certificates. The data collected serves the following purposes:

3.1 Verification of Identity

Names and copies of identification documents such as NRIC, Military ID, or Passport are collected to verify the identity of the certificate applicant. This ensures that digital certificates are issued to the correct individual or authorized representative.

3.2 Communication

Email addresses and telephone numbers are used to communicate with certificate applicants throughout the certificate issuance process. This includes sending notifications, updates, and verification requests related to application status, certificate issuance, renewal, or revocation.

3.3 Authorization and Affiliation

Organizational affiliations and relevant contact information are collected to verify the affiliation of the certificate applicant with their organization or entity. This helps ensure that certificates are issued to authorized personnel and entities only, maintaining the integrity and authenticity of digital transactions.

3.4 Legal Compliance

Certified True Copy (CTC) of eInfo SSM and Letter of Proxy on Company Letterhead are collected to comply with regulatory requirements and to verify the legal status and authorization of the certificate applicant within their organization. This ensures that certificates are issued in accordance with applicable laws and regulations.

4 Security and Trust

The data collected is crucial for maintaining the security and trustworthiness of digital certificates issued by TMCA. By accurately verifying identities and affiliations, we help protect against fraudulent activities and unauthorized certificate issuance, thereby safeguarding digital transactions and communications.

Overall, the use of this data is fundamental to our commitment to providing secure and reliable digital certificates, enhancing trust in online interactions, and ensuring compliance with legal and regulatory standards.

5 Data Retention

At TMCA, we adhere to strict data protection practices to ensure the security and integrity of personal information collected during the certificate issuance process. In compliance with regulatory requirements, all data provided by certificate applicants, including names, identification documents (such as NRIC, Military ID, or Passport copies), email addresses, telephone numbers, organizational affiliations, and other relevant contact information, will be securely stored for a period of 10 years from the date of collection.

This data retention period is necessary to meet legal and regulatory obligations, including but not limited to auditing, compliance, and dispute resolution purposes. During this period, stringent measures are implemented to safeguard the confidentiality and integrity of stored data, including encryption, access controls, and regular security audits.

At the end of the retention period, data that is no longer required for legal, regulatory, or operational purposes will be securely and permanently deleted in accordance with our data retention and disposal policies.

By storing data for the specified period, TMCA ensures continued compliance with applicable laws and regulations, as well as maintaining the ability to verify identities, manage certificate lifecycles, and uphold the security and trustworthiness of our digital certificate services.

6 Data Security

At TMCA, we prioritize the protection of personal data to ensure confidentiality, integrity, and availability throughout its lifecycle. To achieve this, we have implemented robust data security measures, including:

6.1 Encryption

Personal data collected, processed, and stored TMCA is encrypted using strong encryption algorithms. This ensures that sensitive information remains protected against unauthorized access and breaches.

6.2 Access Controls

Access to personal data is strictly controlled and restricted to authorized personnel only. Role-based access controls (RBAC) are enforced to ensure that individuals have access only to the information necessary for their specific duties.

6.3 Secure Storage

Personal data is stored in secure environments that meet industry standards for physical and logical security. This includes data centers with access controls, surveillance, and environmental controls to prevent unauthorized access or physical theft.

6.4 Regular Security Audits

TMCA conduct regular security audits and assessments of our systems, infrastructure, and processes to identify and address potential vulnerabilities. These audits are performed by independent third-party security experts to ensure impartial evaluation and compliance with industry standards.

6.5 Incident Response

TMCA maintains a comprehensive incident response plan to promptly address and mitigate any security incidents or breaches. This includes procedures for incident detection, investigation, containment, and remediation to minimize impact and prevent recurrence.

6.6 Employee Training

All employees undergo regular training on data protection practices and security protocols to ensure awareness of their responsibilities in safeguarding personal data.

7 Compliance with Standards

TMCA adhere to relevant data protection laws and regulations, including but not limited to PDPA and industry-specific standards. Our data security measures are continuously updated to align with evolving legal requirements and best practices.

By implementing these data security measures, TMCA maintains a secure environment for handling personal data, thereby ensuring the trust, reliability, and integrity of our digital certificate services.

8 TMCA Data Sharing Statement

TMCA respects the privacy of its users and is committed to protecting their personal data. This Data Sharing Statement outlines the conditions under which TMCA may share personal data with third parties.

8.1 General Principles

TMCA will only share personal data with third parties when it is necessary to:

a. Deliver our services and fulfill our contractual obligations.
b. Comply with legal or regulatory requirements.
c. Protect the rights, property, or safety of TMCA, our users, or others.
d. Prevent or investigate fraud or other illegal activities.

TMCA will only share personal data with trusted third parties who have implemented appropriate technical and organizational measures to protect the data.

We will take steps to ensure that any third-party recipient of personal data uses the data only for the purposes for which it was disclosed and in accordance with applicable data protection laws.

8.1.1 Service Providers

TMCA may share personal data with service providers who assist us in operating our business and providing our services. These service providers may include data processing companies, customer support providers, and marketing agencies.

8.1.2 Law Enforcement and Regulatory Authorities

TMCA may share personal data with law enforcement or regulatory authorities if required by law or if we believe that such disclosure is necessary to protect the rights, property, or safety of TMCA, our users, or others.

8.2 Your Rights

Depending on your location, you may have certain rights with respect to your personal data, such as the right to access, rectify, erase, or restrict the processing of your personal data. For more information about your rights, please contact us.

8.2.1 Changes to this Data Sharing Statement

TMCA may update this Data Sharing Statement from time to time. We will post any changes on our website.

8.2.2 Individual Rights

At TMCA, we understand that you have rights regarding your personal data. This statement explains the rights you have under applicable data protection laws and regulations.

8.2.3 What Personal Data Do We Collect?

As a Certificate Authority (CA), TMCA typically collect the following types of personal data to issue and manage digital certificates:

8.2.3.1 Identification Information

Name, NRIC, Passport details, organization affiliation (if applicable), and contact details (e.g., email address).

8.2.3.2 Technical Data

Information about your device and interactions with our CA services, such as IP address and certificate issuance/renewal history.

8.3 Your Rights Regarding Your Personal Data

Depending on your location and applicable data protection laws, you may have the following rights:

8.3.1 Right to Access

You may request a copy of the personal data TMCA hold about you.

8.3.2 Right to Rectification

If you believe your personal data is inaccurate or incomplete, you may request that TMCA correct or update it.

8.3.3 Right to Erasure (Right to be Forgotten)

In certain circumstances, you may request that TMCA erase your personal data. However, this right may be limited in some situations, such as where we are required by law to retain your data.

8.3.4 Right to Restrict Processing

You may request that TMCA restrict the processing of your personal data, meaning we can no longer use it for certain purposes (e.g., marketing).

8.3.5 Right to Data Portability

You may have the right to receive your personal data in a structured and commonly

used format and to transmit it to another CA (where technically feasible).

8.4 Exercising Your Rights

If you wish to exercise any of your rights described above, please submit a written request to tmca.helpdesk@tm.com.my We will respond to your request within a reasonable timeframe, as required by law.

8.4.1 Verification Process

To protect your privacy and security, TMCA may require verification of your identity before processing your request. This may involve requesting additional information to confirm your identity.

8.4.2 Exceptions to Your Rights

In some cases, TMCA may not be able to fully comply with your request, for example, if it interferes with our legal obligations or the rights of others. However, we will always explain the reasons for any limitations.

8.5 Changes to this Individual Rights Statement

TMCA may update this Individual Rights Statement from time to time. We will post any changes on our website.

9 Compliance with Malaysian Personal Data Protection Act (PDPA)

TMCA are committed to complying with the Malaysian Personal Data Protection Act (PDPA) of 2010. We take the protection of your personal data seriously and strive to ensure its lawful and responsible processing. Here is how TMCA comply with the PDPA

9.1 Data Protection Principles

TMCA adhere to the seven data protection principles outlined in the PDPA, including: processing personal data for a lawful purpose, obtaining your consent, and ensuring the accuracy and security of your data.

9.2 Registration with PDPC

TM Technology Services Sdn Bhd is registered with the Personal Data Protection Commissioner (PDPC) as a data user.

9.3 Limited Data Collection

TMCA only collect the personal data necessary to fulfill our obligations as a CA, such as identification information for certificate issuance and technical data for service delivery.

9.4 Data Security Measures

TMCA implement robust technical and organizational measures to protect your personal data from unauthorized access, disclosure, alteration, or loss.

9.5 Data Retention

TMCA retain your personal data only for as long as necessary to fulfill the purposes for which it was collected or as required by law.

9.6 Individual Rights

TMCA respect your rights under the PDPA, including the right to access, rectify, erase, or restrict processing of your personal data. For more information about your rights, please see our Individual Rights Regarding Your Personal Data statement.

9.7 Changes to this Compliance Statement

TMCA may update this Compliance Statement to reflect changes in the PDPA or our data practices. We will post any changes on our website.

10 Policy Updates

10.1 Policy Updates and Communication

TMCA reserves the right to update this CPS from time to time. We will make reasonable efforts to communicate any material changes to the CPS to affected parties. This may include:

10.1.1 Posting the updated CPS on our website

TMCA will prominently display the revised CPS on our website with an effective date.

10.1.2 Direct notification

In some cases, TMCA may send direct notification (e.g., email) to users who have actively interacted with our CA services and provided contact information.

10.1.3 Public announcement

For significant changes, TMCA may issue a public announcement through industry channels or media outlets.

10.2 Frequency of Updates

TMCA may update the CPS for various reasons, including:

10.2.1 Changes in Law or Regulations

To comply with changes in applicable data protection laws or industry standards.

10.2.2 Changes in Our Practices

To reflect changes in our data collection, processing, or security practices.

10.2.3 New Technologies or Services

To accommodate the introduction of new technologies or services offered by our CA.

TMCA will strive to provide reasonable notice of any material changes to the CPS. However, we encourage you to periodically review the CPS on our website for the latest version.

11 Your Continued Use of Our Services

By continuing to use our TMCA services after the revised CPS becomes effective, you are deemed to have accepted the changes.

12 Information Treated as Private

Non-public Subscriber information is treated as private.

13 Information Not Deemed as Private

Subscriber information issued in the certificates, certificate directory, and online CRLs is not deemed private information, subject to applicable law.

14 Responsibility to Protect Private Information

No stipulation.

15 Notice and Consent to Use Private Information

No stipulation.

16 Disclosure Pursuant to Judicial or Administrative Process

TMCA shall be permitted to disclose confidential and/or private information if required to doso by law or regulation. This section is subject to applicable laws.

17 Contact Information

We understand that you may have questions or concerns about our privacy practices. For specific inquiries related to TMCA's data handling practices, you can contact the TMCA Manager at:

TMCA Manager:
Email: elia@tm.com.my
Phone: +6013 3999398

We strive to respond to all inquiries promptly and within the timeframes required by applicable data protection laws.