

**SS 714:2025**  
(ICS 35.030)

**SINGAPORE STANDARD**  
**Data protection trustmark**



**SS 714:2025**

(ICS 35.030)

---

SINGAPORE STANDARD

**Data protection trustmark**

---

Published by Enterprise Singapore

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilming, without permission in writing from Enterprise Singapore. Request for permission can be sent to: [standards@enterprisesg.gov.sg](mailto:standards@enterprisesg.gov.sg).

© Enterprise Singapore 2025

ISBN 978-981-5338-67-6

**Contents**

	<b>Page</b>
Foreword _____	3
0 Introduction _____	4
1 Scope _____	4
2 Normative reference _____	4
3 Terms and definitions _____	5
4 Abbreviations _____	6
5 Overview of the standard _____	6
6 Governance and transparency _____	7
7 Management of personal data _____	11
8 Care of personal data _____	14
9 Safeguarding individual rights _____	20
Bibliography _____	23

## Foreword

This Singapore Standard was prepared by the Working Group on Data Protection Trustmark set up by the Technical Committee on Security and Privacy Standards under the purview of the Information Technology Standards Committee.

This standard describes provisions for achieving a data protection trustmark (DPTM). The DPTM supports digital economy strategies and is intended to encourage organisations to strengthen their accountability and conformance to generally accepted personal data protection standards and best practices.

The DPTM is a mark of distinction for an organisation's accountable data protection practices. Companies are able to easily identify partners with DPTM, facilitating more data exchanges to improve business outcomes.

It is presupposed that in the course of their work, users will comply with all relevant regulatory and statutory requirements. An example of a relevant act is listed in the Bibliography. The Singapore Standards Council and Enterprise Singapore shall not be responsible for identifying all of such legal obligations.

In preparing this standard, reference was made to the Personal Data Protection Act.

Acknowledgement is made for the use of information from the above publication.

Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

### NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as "mature standards". Mature standards will not be subject to further review unless there are requests to review such standards.*
2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*
3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

## **Data protection trustmark**

### **0 Introduction**

Globalisation in the 21st century is increasingly defined by flows of data and information. The growing digital economy has created high demand for cross-border data transactions. Robust protective measures allow overseas businesses and customers to exchange data with the assurance that the exchanged data are protected and used responsibly.

Developing strong consumer confidence in digital transactions encourages participation and contributes to the growth of the digital economy. This standard aims to provide assurance to businesses and their customers that their personal data is properly managed by organisations that adopt these data protection practices.

Specifically, this standard aims to:

- a) strengthen and demonstrate compliance with regulatory and statutory requirements for the protection of personal data and promote accountability by organisations;
- b) enhance and promote consistency in data protection standards across all sectors;
- c) provide a competitive advantage for businesses that are certified; and
- d) encourage organisations to be transparent and accountable in their data protection practices and boost consumer confidence in their management of personal data.

As consumers and organisations in both public and private sectors increasingly demand accountable data protection practices, organisations have the impetus to adopt robust data governance regimes. This fosters an environment of trust among businesses and customers, contributing to a vibrant digital economy.

### **1 Scope**

This standard covers the following data protection principles that are applicable to organisations that manage personal data:

- a) Governance and transparency: Appropriate data protection policies and practices (e.g., risk assessment, data breach management plan) for managing personal data, and the communication of these policies and practices to stakeholders.
- b) Management of personal data: Appropriate procedures for obtaining consent to collect, use, and disclose data for appropriate purposes, including required notifications.
- c) Care of personal data: Appropriate procedures for ensuring the security, accuracy, completeness, retention, and disposal of personal data.
- d) Safeguarding individuals' rights: Procedures enabling individuals to withdraw consent, access their personal data, and request corrections.

### **2 Normative references**

There are no normative references in this document.