TOM Group Limited

Policy on Personal Data Governance

(If there is any inconsistency or conflict between the English and the Chinese versions, the English version shall prevail.)

Table of Contents

1. Policy Statement

TOM Group Limited (the "Company"), its subsidiaries and controlled affiliates (collectively, the "Group") recognises that the protection of personal data is fundamental to preserving the trust of customers and employees. the group is committed to the safeguard and protection of their personal data in compliance with applicable data protection laws.

This Policy sets out the Group governance framework for the safeguard of Personal Data of Employees and Customers. This Policy should be read in conjunction with the TOM Group Information Security Policy and the TOM Group Code of Conduct, as well as the local policies and procedures of Business Units ("BU").

This Policy applies to the Group, and to all directors, officers and Employees in the Group.

Please contact the head of the relevant BUs and the Legal Department of BUs for any questions in relation to this Policy.

Appendix 1 and 2 set out a glossary of common terms and a summary of key concepts used in this Policy.

2. Governance Framework

The senior management of each BU is accountable for the effective implementation of this Policy (including the Data Privacy Principles and Procedures set out below). Senior management is to ensure that this Policy is incorporated and embedded into local policies and procedures, subject to (and in compliance with) Applicable Data Protection Laws.

As the "Data Controller" of its Customer and Employee Personal Data, each BU must implement its local policies and procedures in such a manner that it can demonstrate compliance with its Applicable Data Protection Laws including (where required):

(a) ensuring that the legislative and regulatory requirements are embedded in all activities involving the processing of Personal Data (e.g. ensuring 'privacy by design' for all new projects involving processing Personal Data);

(b) implementing appropriate technical and organisational measures which are designed to implement the Data Privacy Principles in an effective manner and to integrate necessary safeguards into processing activities, and to protect the rights of data subjects as required in the jurisdictions in which they operate;

(c) conducting privacy and data protection awareness training for Employees to ensure awareness and understanding of this Policy and their responsibilities in data protection management and privacy;

(d) conducting regular privacy risk assessments of its business to assess the privacy risk (including with respect to third party vendors) and the adequacy of mitigating controls;

(e) ensuring Personal Data is classified and handled according to its sensitivity, and access is restricted on a need-to-know-basis; and

(f) designating appropriate privacy and IT security specialists to support the business in managing its data privacy risks (e.g. the appointment of a data protection officer if required).

All Employees involved in Personal Data processing should understand and comply with this Policy, as well as any related policies, procedures and guidelines implemented by their BU. Failure to process Personal Data in accordance with this Policy may lead to disciplinary action. Serious and/or deliberate non-compliance with this Policy could result in dismissal for Employees.

3. Data Privacy Principles

The Group shall at all times process Personal Data in line with the following Data Privacy Principles.

3.1 Lawful, Fair and Transparent Processing

(a) Personal Data will only be used in a way that is lawful, fair and transparent.

(b) Use of Personal Data should be in compliance with Applicable Data Protection Laws within each of the jurisdictions in which the Group operates. BUs are to be transparent about when, how and for what purpose the Personal Data of Customers and Employees is processed, and what choices and rights individuals have in that jurisdiction in relation to the processing of their Personal Data.

(c) Access to Personal Data should be restricted to Employees who need to know the information to fulfil their role within the company and Sensitive Personal Data (including access thereto) requires the highest level of protection.

3.2 Purpose and Use

Personal Data should only be collected for specified, clear and legitimate purposes and only to the extent needed to achieve those purposes. Use of

Personal Data helps improve the services offered by the Group, but use of such data should be proportionate to clear purposes.

3.3 Data Accuracy

Reasonable steps should be taken to ensure that any Personal Data held is accurate and up to date.

3.4 Data Retention

Personal Data should only be kept for as long as is necessary for the purposes for which it is being used. Guidelines around document retention periods should be issued by each BU to relevant management and staff.

3.5 Rights of the Individuals

(a) Personal Data should be processed in accordance with the rights of individuals under the Applicable Data Protection Laws within each of the jurisdictions in which the Group operates.

(b) All requests from individuals to access, amend, delete or otherwise relating to their Personal Data should be handled in a manner compliant with Applicable Data Protection Laws with appropriate processes for receiving and responding to such requests.

3.6 Information Security

(a) Appropriate technical and organisational security measures should be adopted to safeguard the Personal Data the Group is entrusted with against unauthorised or unlawful processing and against accidental loss, destruction or damage to ensure a level of security appropriate to the risk (e.g. the pseudonymisation and encryption of Personal Data and/or other security measures as appropriate).

(b) Security measures should be implemented and reviewed regularly to ensure that they offer the appropriate level of protection.

(c) The same level of security should be used to protect the Personal Data that is processed on behalf of third parties (e.g. where the BU acts as "Data Processor").

3.7 International Transfers of Personal Data

The Group is a global business and as such is required to transfer information internationally. Personal Data should not be transferred to a country or territory that does not provide adequate data protection without appropriate safeguards.

4. Procedures

Each BU is to implement appropriate procedures to ensure that Personal Data is processed fairly and lawfully in accordance with the Data Privacy Principles and Applicable Data Protection Laws.

4.1 Records of Processing

Each BU should maintain records of processing activities, and documentation related to data protection compliance, if required by Applicable Data Protection Laws.

4.2 Privacy Impact Assessments

Privacy impact assessments should be performed with respect to new products, technologies and business operations, where required by Applicable Data Protection Laws or where appropriate to manage the privacy risk. For instance, if the project involves one or more of the following: processing large amounts of Personal Data or where the processing affects a large number of individuals; using existing Personal Data for a new and/or more intrusive purpose; processing Sensitive Personal Data and/or genetic or biometric data (e.g. fingerprint scanning, face recognition); introducing new and intrusive technology (e.g. CCTV cameras, locator technologies); or engaging in any type of employee monitoring (including any recording and/or reviewing of employees' communications or activities, including phone calls, emails and computer files).

4.3 Privacy Notices

Each BU should implement appropriate privacy policies / notices ("Privacy Notices") where required by Applicable Data Protection Laws including to explain to Customers and Employees what Personal Data is processed and for what purposes. These Privacy Notices should be readily accessible and kept up to date, with simple mechanisms for individuals to opt-out of, or not to agree to, processing of Personal Data when the law requires.

4.4 Data Subject Requests

All requests from individuals to access, amend, delete or otherwise relating to their Personal Data should be handled according to procedures which are compliant with Applicable Data Protection Laws.

4.5 Disclosure of Personal Data to Law Enforcement Authorities / Other Regulatory Authorities

The Group may have a duty to disclose Personal Data to law enforcement authorities or other regulatory authorities in certain specified and limited

circumstances. Responding to official requests for Personal Data should be balanced against the obligation to protect Personal Data. All Employees must follow the relevant procedures and if they are in doubt they must consult with the head of the relevant BUs and the Legal Department of their BU.

4.6 Cooperation with Privacy Authorities

The Group is committed to cooperating with enquiries and investigations of the Privacy Authorities, particularly if they have concerns regarding the privacy of the Employees, Customers or users of websites of the Group. Communications from Privacy Authorities should be referred to the head of the relevant BUs and the Legal Department of the BUs without delay.

4.7 Data Security Incidents

When a Data Security Incident ("DSI") occurs which involves Personal Data, BUs should aim to mitigate the potential consequences and to secure Personal Data from further unauthorised access, use or damage as quickly as possible. BUs should respond rapidly and in accordance with applicable DSI procedures, which may include notifying the Privacy Authorities and/or affected individuals if required. In the event of a DSI involving Personal Data, the Chief Executive Officer of the Group, the head of the relevant BUs, the Corporate Systems & IT Department and the relevant BU Legal Department should be alerted immediately. Further guidance on notification and handling of DSIs should be issued from time to time.

4.8 Use of CCTV

The use of CCTV may involve processing identifiable images of individuals. Where used, BUs must consider the potentially sensitive nature of the images captured when using CCTV and processing the data gathered. Employees involved in the use of CCTV should be trained in respect of its use to ensure compliance with Applicable Data Protection Laws.

4.9 Third Party Processors

Where third party service providers are engaged as part of business operations which involve the Data Processing of Personal Data, it is important to ensure that:

(a) appropriate diligence is conducted in the selection of such vendors, with ongoing monitoring and review of third party vendors;

(b) the third party implements adequate privacy and security safeguards in accordance with this Policy;

(c) a contract including data privacy clauses is in place and approved by the relevant BU Legal Department before the processing starts; and

(d) any recommendations arising from the privacy impact assessment (if applicable) relating to the use of the third party are implemented.

Appendix 1: Glossary of Terms

Term	Definition
Applicable Data Protection Laws	means the applicable laws and regulations in the relevant countries ensuring the protection of Personal Data.
Customers	means all customers of a BU's goods and services, whether online and/or offline, including members of customer loyalty schemes.
Data Controller	means the entity which alone or jointly with others determines the purposes and means of processing of Personal Data.
Data Processing	means any operation performed upon Personal Data whether or not by automatic means, including collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Personal Data.
Data Processor	means the entity which processes Personal Data on behalf of the Data Controller (and the meaning of Data Processing shall be construed in accordance with this definition).
Data Security Incident (DSI)	means any actual or suspected event where the security, confidentiality, integrity or availability of Personal Data has been or could be compromised. For example: loss or theft of data or equipment on which Personal Data is stored; sharing or inappropriate use of passwords allowing unauthorised access to Personal Data; IT systems failure; human error; unforeseen circumstances such as a fire or flood; hacking attacks on IT systems; improper handling or disposing of Personal Data; and offences where Personal Data is obtained through deception.
Employee(s)	means all persons who work for the Group including employees with temporary, fixed term and permanent employment contracts.
Personal Data	means information that directly or indirectly identifies an individual person, whether a Customer, Employee or user of the Company or a BU website.
Privacy Authorities	means the information commissioners or equivalent regulatory authorities in the relevant countries responsible for administering and enforcing the relevant Applicable Data Protection Laws.
Sensitive Personal Data (SPD)	means any Personal Data which, due to its sensitive nature, is subject to additional legal controls over processing, including the following special categories of Personal Data: data concerning an individual's racial or ethnic origin, ideology or political opinions, religious or philosophical beliefs, membership of a trade union, physical or mental health, sexual life or orientation, criminal convictions or alleged commission of any offence, as well as any genetic or biometric data.

Appendix 2: Key Concepts

What is "Processing"?

Applicable Data Protection Laws regulate the "processing" (i.e. handling) of Personal Data. Processing is *very* broadly defined and covers a range of activities including receiving, holding, storing, collecting, deleting, amending, editing, selling, analysing or reporting Personal Data. The rules apply to holding data on computer databases, word processed documents and audio tape, or images identifying a person on video tape, CD, DVD or stored as a digital image. Applicable Data Protection Laws also regulate paper-based information held in filing systems.

What is "Personal Data"?

Data is Personal Data if it relates to a living individual who can be "identified" or who is "identifiable" (a) from those data, or (b) from those data and other information which is in the Group's possession, or is likely to come into its possession. The concept of Personal Data is therefore extremely broad. In some countries, information relating to a corporate entity is treated as Personal Data.

Examples: a telephone number on its own may be Personal Data if it is capable of identifying a living individual. The information contained on a credit card constitutes Personal Data because it contains the name of the card holder. Customer Loyalty card number by itself is regarded as Personal Data under Applicable Data Protection Laws because the loyalty card issuer can identify the individual person behind the number. Footage from a video camera can be Personal Data to the extent individuals are recognisable. Telephone or email log data contain Personal Data because it is possible to directly or indirectly identify the individuals who communicated.

Personal Data also includes any expression of opinion about the individual and any indication of the intentions of the Company or BUs or any other person in respect of the individual.

What is Sensitive Personal Data or SPD?

Sensitive Personal Data refers to various categories of data that are subject to additional legal controls over processing and include data concerning an individual's racial or ethnic origin, ideology or political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health condition, sexual life, criminal convictions or alleged commission of any offence. Please note that the definition may be broader in some jurisdictions and that in some jurisdictions information relating to offences and proceedings will constitute "judicial data" and be subject to specific rules. More stringent rules apply in many countries to processing of Sensitive Personal Data and judicial data. Where the Company or

BUs rely on consent to process Sensitive Personal Data, such consent must be "explicit" - i.e. the individual needs to take some positive step to indicate their acceptance.

What is the difference between a Data Controller and Data Processor?

A **Data Controller** is the entity which controls the manner in which and purposes for which the data is collected, even if it does not physically hold the data itself. As such, the Company and BUs will be Data Controllers in relation to data relating to their Employees or Customers, even if the data is held by a third party, which acts on behalf of the Company and BU (e.g. payroll administration is outsourced to a third party). A party which holds and processes Personal Data on behalf of a Data Controller is a **Data Processor**. Where the Company or BUs together with another party control the manner and purposes of the processing, the two parties can be joint Data Controllers.

Example: BU has certain marketing material which it wishes to distribute to all its loyalty card members. A third party agency is to undertake the processing (e.g. sending direct marketing communications) on behalf of and under the BU's instructions. The BU is the Data Controller and the agency will be a Data Processor.