
HUTCHMED (China) Limited

Policy on Personal Data Governance

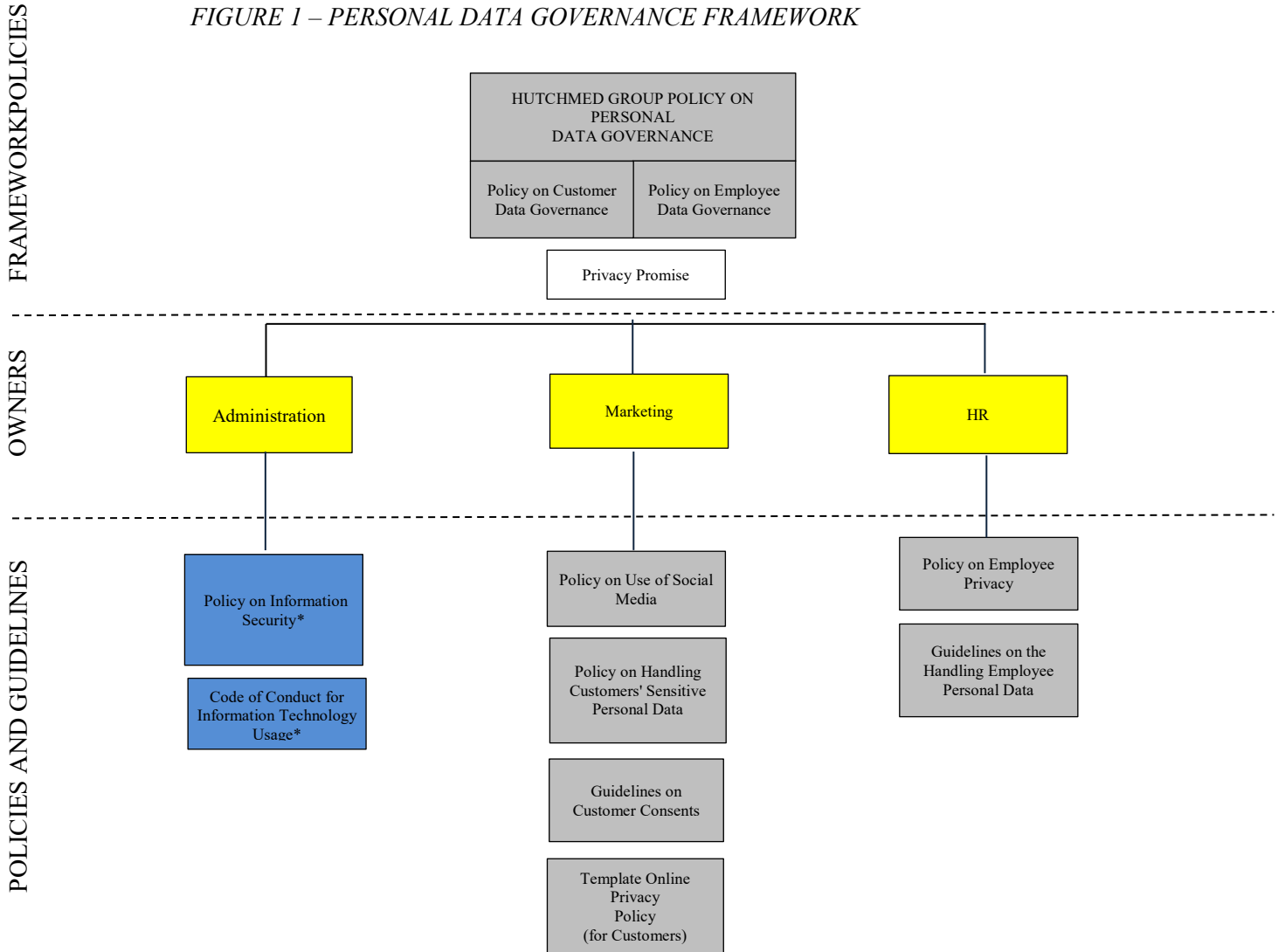
Adopted by the board of directors on 14 March 2017

1. PURPOSE AND SCOPE

- 1.1 This Policy sets out the framework of policies and procedures that HUTCHMED (China) Limited and its subsidiaries and controlled joint ventures (collectively the “HUTCHMED Group”) has implemented, or will implement, to ensure compliance with Data Protection Laws as part of the Personal Data Governance Framework (described in *Figure 1*, below). Where there is inconsistency between policies and procedures and this document, this document will take precedence.
- 1.2 The Personal Data Governance Framework is supported by the Privacy Working Group and the Data Privacy Officer.
- 1.3 Should you have any questions or need any support to understand the subject, please feel free to contact Group Legal or Group Marketing Department.
- 1.4 Appendix 1 sets out a summary of key concepts and a glossary of common terms used in this document and in the other documents forming part of the Personal Data Governance Framework.

2. GOVERNANCE FRAMEWORK AND STRUCTURE

FIGURE 1 – PERSONAL DATA GOVERNANCE FRAMEWORK



* Existing Policies

New Policies

3. GOVERNANCE PRINCIPLES

3.1 We will always process Personal Data fairly and lawfully and will comply with local Data Protection Laws within each of the jurisdictions in which we operate. We are committed to cooperating with enquiries and investigations of the Privacy Authorities, particularly if they have concerns regarding the Privacy of our Employees, Customers or users of our Websites.

Any communications from Privacy Authorities should be referred to the Legal Department without delay.

3.2 We are committed to being open and transparent about how we use, collect and protect Personal Data. Each BU should implement Privacy Policies to protect the Personal Data of the Customers and Employees and regularly review the Privacy Policies to ensure that they contain an accurate description of the Personal Data we process and the purposes for which we process it.

3.3 As a Group we will, and each BU is expected to, adopt appropriate technical and organisational security measures to safeguard the Personal Data we are entrusted with. The security measures in place will be regularly reviewed to ensure that they offer the appropriate level of protection.

3.4 Where we engage third party service providers as part of our normal business operations to perform certain tasks, it is important to select such third party service providers carefully and contracts must be put in place requiring them to implement similar data governance standards to our own.

3.5 All the Personal Data that we process should be necessary and proportionate for the effective operation of our business and to comply with our legal and regulatory obligations. We will take steps to ensure that the data we hold is accurate and up-to-date.

3.6 Our organisation is a multi-city business and as such we are required to transfer information among countries. When we transfer information it is essential that there are adequate safeguards in place to protect the Personal Data we transfer, especially in countries that do not have adequate Data Protection Laws.

3.7 We will hold data only for so long as is necessary for our business purposes. Guidelines around document retention periods will be issued from time to time.

4. HANDLING PERSONAL DATA

4.1 All Personal Data is strictly confidential and will be handled according to its sensitive nature. All Personal Data is for internal use only unless we are required to disclose it in accordance with any of our policies or procedures or applicable law.

4.2 Sensitive Personal Data requires the highest level of protection.

4.3 Access to Personal Data will be restricted to Employees who need to know the information to fulfil their role within the company and access to Sensitive Personal Data must be authorised by the relevant authorised person within the HUTCHMED Group.

5. THE PRIVACY PROMISE OF THE HUTCHMED GROUP

As part of the commitment of the HUTCHMED Group to protect and value Personal Data, the HUTCHMED Group will publicly commit to its Customers and Employees to comply with certain principles in its 'Privacy Promise'. The Privacy Promise is as follows:

"At HUTCHMED (China) Limited, we are committed to protecting your personal data. We promise that we will:

- protect your personal data;
- always explain to you what personal data we collect;
- never sell any of your personal data to third parties; and
- comply with all relevant data protection laws."

6. CUSTOMER PERSONAL DATA

6.1 The HUTCHMED Group recognises the value of Customer Personal Data and is adapting to the evolving customer privacy landscape. The HUTCHMED Group is moving towards owning increasing amounts of Customer Personal Data across markets and, in line with our strategic direction, seeking to maximize the benefits from utilizing this Customer Personal Data.

6.2 The prudent use of Customer Personal Data represents a tremendous business opportunity. This data represents a very significant asset for the HUTCHMED Group and the way we process this Personal Data is critical to creating and maintaining the value in this asset.

6.3 Detailed policy statements regarding the processing of Customer Personal Data are set out in the Policy on Customer Data Governance.

7. EMPLOYEE PERSONAL DATA

7.1 We recognise that our Employees are central to our growth and we aim to protect their Personal Data to the highest standards. We recognise the valuable contribution of Employee capital and realise that Employees are placing their trust in us when they provide us with their Personal Data. We, in turn, are committed to protecting their Personal Data. To that end we have established a Policy on Employee Data Governance.

7.2 As a Group we will, and each BU is expected to, ensure that Employees are made aware of both their rights in relation to the Personal Data that the HUTCHMED Group holds about them and the Personal Data that they handle in the course of their employment. The detailed requirements are set out in the Policy on Employee Privacy.

7.3 For further guidance please refer to our Guidelines on Handling Employee Personal Data.

8. REPORTING

8.1 Please review your current practice immediately to ensure that this Policy is complied with in your BU. Should you have any questions or need any support to understand the subject, please feel free to contact the Administration Department or the Legal Department.

8.2 If you would like to report any breach of this Policy, please report either by email to report@hutch-med.com or by post to the General Manager, Group Management Services, 48th Floor, Cheung Kong Center, 2 Queen's Road Central, Hong Kong.

Appendix 1:

Glossary of Terms

Term	Definition
CKHH Group	means the group of CK Hutchison Holdings Limited and its controlled affiliated companies.
Customer Personal Data	means all Personal Data relating to Customers of the HUTCHMED Group.
Customers	means all customers of the goods and services provided by the HUTCHMED Group, whether online and/or offline, including members of relevant customer loyalty schemes.
Data Controller	means the natural or legal person which alone or jointly with others determines the purposes and means of processing of Personal Data.
Data Privacy Officer(s)	means the Employee(s) or service provider(s) responsible for managing compliance with Data Protection Laws within the HUTCHMED Group.
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 a natural or legal person 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 Protection Laws	means the applicable laws and regulations in the relevant countries ensuring the protection of Personal Data.
Data Security Incident (DSI)	means any actual or suspected event where the security, confidentiality, integrity or availability of HUTCHMED Data has been or could be compromised. For example: loss or theft of data or equipment on which HUTCHMED Data is stored; sharing or inappropriate use of passwords allowing unauthorised access to HUTCHMED Data; IT systems failure; human error; unforeseen circumstances such as a fire or flood; hacking attack on any IT systems held by the HUTCHMED Group; improper handling or disposing of HUTCHMED Data; and offences where HUTCHMED Data is obtained by deceiving the HUTCHMED Group.
Data Subject(s)	means an Individual about whom the HUTCHMED Group holds Personal Data.
Employee(s)	means all who work for the HUTCHMED Group or any of its business entities, including employees with temporary, fixed term and permanent employment contracts.
Employee Personal Data	means all Personal Data relating to current and former Employees of the HUTCHMED Group.

HUTCHMED Group Policy on Personal Data Governance

Term	Definition
Individuals	means all Employees, Customers and users of the websites held by the HUTCHMED Group.
Personal Data	means information that directly or indirectly identifies an Individual, whether a Customer, Employee or user of the websites held by the HUTCHMED Group.
Privacy Authorities	means the information commissioners or equivalent regulatory authorities in the relevant countries responsible for administering and enforcing the relevant Data Protection Laws.
Privacy Policy(ies)	means, in respect of Customers, the online privacy policy used on the websites held by the HUTCHMED Group and, in respect of Employees, the Policy on Employee Privacy.
Sensitive Personal Data (SPD)	means any Personal Data which, due to its sensitive nature, is subject to additional legal controls over processing. This includes data concerning the racial or ethnic origin, ideology or political opinions, religious beliefs, membership of a trade union, physical or mental health condition, sexual life, criminal convictions or alleged commission of any offence of an individual.

KEY CONCEPTS

Key definitions and concepts

What is "Processing"?

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. 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 our possession, or is likely to come into our possession. The concept of Personal Data is therefore extremely broad.

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 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 HUTCHMED Group 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 the 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 of an individual. 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 HUTCHMED Group relies 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 "consent"?

For consent to be valid, Individuals must be fully informed about the processing activities related to their Personal Data and give their consent freely. The HUTCHMED Group informs Individuals about our processing activities in the HUTCHMED Group Privacy Policies. Customers and Employees will be informed of any data processing activities held by the HUTCHMED Group as soon as practicable and users of the websites held by the HUTCHMED Group indicate their consent by their continued use of the site and may consent to further processing if they register as a member. Customers also

consent to any data processing conducted by the HUTCHMED Group in different ways depending on the channel.

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 HUTCHMED Group will be a Data Controller in relation to data relating to its Employees or Customers, even if the data is held by a third party, which acts on behalf of the HUTCHMED Group (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 HUTCHMED Group together with another party controls the manner and purposes of the processing the two parties can be joint Data Controllers.

Example: The HUTCHMED Group runs a marketing campaign which it wishes to collect public views. A third party agency is to undertake the processing (e.g. operating a website) on behalf of and under the instructions made by the HUTCHMED Group. The HUTCHMED Group is the Data Controller and the agency will be a Data Processor.