STRATEQ GROUP DATA PROTECTION POLICY
Include In Countries Local Guides

1. INTRODUCTION

1.1 Objective

Strateq is committed to compliance with data protection laws. This Group Data Protection Policy ("Policy") forms the basis of Strateq's data protection compliance program and applies to the Strateq group of companies worldwide ("Strateq"). All personnel must comply with this Policy when processing personal data in connection with Strateq's business and operations.

1.2 Policy Compliance

Laws around the world impose obligations on Strateq to protect and lawfully use personal data that we process in connection with our business. Failing to comply with such laws may expose Strateq to financial penalties, as well as damage to our reputation and customer confidence. Therefore, personal data must at all times be handled in accordance with this Policy and other related policies, procedures, notices, and standards which may be implemented from time to time. Personnel who fail to comply with this Policy may be subject to disciplinary action, up to and including dismissal.

1.3 Applicable of Local Laws

This Policy is based on generally accepted data protection principles and is intended to supplement local laws. To this end, this Policy should be read together with the relevant Local Guidelines for each country referenced herein, as well as the Data Retention and Disposal Policy and Data Breach Management Policy which supplement this Policy.

Where local laws conflict with or impose stricter requirements than those set out under this Policy, such local laws will take precedence; in such case, the relevant Strateq entity should work with the Group Data Protection Officer ("DPO") to find a practical solution that meets the purpose of this Policy.

Where local laws do not govern the processing of personal data, this Policy must still be complied with.

2. GLOSSARY

Personal Data	Information that relates directly or indirectly to individuals (e.g., patients, healthcare professionals, employees, individual representatives of customer and business partners, and other individuals) who are identified or identifiable from that information. This includes sensitive personal data, where applicable.

Sensitive Personal Data	Personal data that is subject to a higher standard of protection based on applicable data protection laws. Additional or differing definitions of "sensitive personal data" under local laws are set out in Section 2 of each country's Local Guidelines.
Processing	All activities involving the handling of personal data, such as collecting, recording, holding, storing, organizing, adapting, altering, retrieving, using, disclosing, transmitting, transferring, disseminating, making available, aligning, combining, correcting, erasing, destructing personal data.
Data Controller	A person who is either alone or jointly in common with other persons processes any personal data or has control over or authorizes the processing of any personal data but does not include a data processor.
Data Processor	A person, other than an employee of the data user, who processes the personal data solely on behalf of or at the instructions of the data controller and does not process personal data for any of his/her/its own purposes.
Data Subject	An individual who is the subject of the personal data and shall not include a deceased individual.

3. KEY PRINCIPLES

The following key data protection principles should be kept in mind when processing personal data.

Key principle	**Brief description**
General principle	Strateq must only process personal data, including sensitive personal data, lawfully where it has consent or can otherwise rely on a valid legal basis.
Notice and choice principle	Inform data subjects as soon as practicable the manner in which their personal data is processed.
Disclosure principle	Do not disclose personal data to third parties unless with consent of the data subjects or otherwise permitted by applicable laws.
Security principle	Protect personal data from any loss, misuse, modification, unauthorized, unlawful, or accidental access or disclosure, alteration or destruction.
Retention principle	Destroy or permanently delete personal data that is no longer required for its intended purpose(s) after the appropriate statutory retention time frames.
Data integrity principle	Take reasonable steps to ensure that personal data held by Strateq is accurate, complete, not misleading and kept up to date.

Access principle	Enable data subjects to access their personal data and to correct such data when it is inaccurate, incomplete, misleading or not up to date.

4. ROLES AND RESPONSIBILITIES

All Strateq employees must comply with this Policy.

The respective heads of Strateq's business units / departments (in Malaysia) and the country heads (outside Malaysia) (each a "Business Leader") are accountable for implementation and execution of this Policy.

The Group DPO is the owner of this Policy and will be responsible for the following:

a) supervising employees' compliance with this Policy;
b) advising and supporting Business Leaders on the application of this Policy;
c) monitoring developments in applicable data protection laws, and keeping Business Leaders and this Policy updated to reflect the same;
d) leading any investigations or inquiries by a regulator concerning any matters relating to this Policy; and
e) retaining external counsel where necessary to discharge any of the foregoing.

Details of the Group DPO can be located at Strateq Compliance Site and Learning Management System.

Strateq shall appoint a network of Data Protection Champions ("DPCs") group-wide representing different business units and functions to assist with the implementation of this Policy and the day-to-day running of the data protection program. DPCs will receive appropriate training and be adequately resourced to fulfil their responsibilities.

5. LAWFUL COLLECTION AND PROCESSING

5.1 Legal bases to process personal data

Employees must ensure Strateq is always processing personal data in a lawful manner. In most cases, this means obtaining the consent of data subjects to process their personal data. However, in some cases, other legal bases may apply e.g. where the processing is necessary for:

a) the performance of a contract to which the individual is a party;
b) the taking of steps at the request of the individual with a view to entering a contract;
c) compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;
d) order to protect the vital interests of the individual;
e) the administration of justice; or
f) the exercise of any functions conferred on any person by or under any law.

Additional or different guidelines may apply in some countries - see Section 1 of each country's Local Guidelines for details.

5.2 Sensitive personal data

Sensitive personal data may have separate requirements for consent or legal bases for processing - see Section 2 of each country's Local Guidelines for details.

6. PRIVACY NOTICES

Privacy notices should always reflect Strateq's practices and procedures when handling personal data. Strateq must provide an appropriate privacy notice when data subjects are first asked by Strateq to provide their personal data. A fresh or updated privacy notice must be given before Strateq uses the personal data for a purpose other than the purpose for which it was originally collected, or before Strateq discloses the personal data to a new class of third parties.

Employees should consult the DPO on the requirements and adequacy of privacy notices, which may differ from one use case to another - factors that will be taken into consideration include:

a) the types of personal data to be collected and processed;
b) the sources from which Strateq obtains such personal data;
c) the purposes for processing; and
d) the classes of third parties to whom personal data may be disclosed.

7. DISCLOSING PERSONAL DATA

Personal data should not be disclosed to or shared with any third parties other than those who are directly related to and necessary for the purposes as stated in the relevant privacy notices ("Purposes") which data subjects have been informed of and/or consented to.

7.1 Disclosures to third parties

If any situation arises which does not fall within any of the Purposes and/or requires the disclosure of personal data to any other third parties, please contact the DPO who will assess the following:

a) whether there is an exception under applicable data protection laws for Strateq to make such a disclosure;
b) whether consent of the data subjects may be obtained to allow such disclosure;
c) whether an agreement containing appropriate data protection clauses or a letter of undertaking must be entered into with or executed by the relevant third parties to protect the personal data; and
d) whether the disclosure must be recorded internally for tracking purposes.

Please be mindful that "disclosure" is interpreted very widely and includes a situation where a third-party service provider is granted access to Strateq's database, or where Strateq uses third-party services which may also access Strateq's database (e.g., cloud storage or IT maintenance).

Where Strateq is required to disclose personal data to any third parties, please ensure that the relevant agreement with such a third party contains appropriate data protection clauses which impose contractual obligations on the third party to process the disclosed

personal data in line with applicable laws and other safeguards imposed by Strateq. Employees should consult the DPO on the appropriate data protection clauses to use.

7.2 Cross-border data transfers

There may be further restrictions for personal data to be transferred from one country to another. Any cross-border transfer of personal data must be done in accordance with the applicable privacy laws. The local requirements to transfer personal data to another country are set out in Section 3 of each country's Local Guidelines - if in doubt, please consult the DPO.

8. STRATEQ AS DATA PROCESSOR

As an IT solution provider, transmission of personal data to Strateq by its clients will commonly occur. In respect of any personal data so received, Strateq will be the data processor and may only process such personal data in accordance with the instructions agreed with or received from the client (which may be recorded in the service agreement or other ancillary documents). These instructions may include restrictions on transfers to other parties (including other Strateq companies) or transfers to other countries as well as specific security requirements. Any such restrictions must be complied with. All such instructions must be properly reviewed by the DPO, documented in writing, and agreed before Strateq starts performing services for such clients, to ensure that Strateq is able to comply with any client-specific restrictions or requirements.

Irrespective of any client requirements, as a rule, any personal data provided by a client must comply with the following:

a) processed only for the purpose they were provided for;
b) not kept for longer than is required for the purpose; and
c) at a minimum, subject to the same security requirements applicable to Strateq's own personal data.

In some countries, local data protection laws place direct obligations on Strateq as a data processor - see Section 4 of each country's Local Guidelines for details.

9. STRATEQ ENGAGING DATA PROCESSORS

Where Strateq uses data processors to process personal data on its behalf for Strateq's own purposes, personnel must ensure that the data processor:

a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and
b) takes reasonable steps to ensure compliance with those measures.

Therefore, when engaging third parties to process personal data for and on behalf of Strateq, the following should be carried out:

a) Assessment - assess whether such third parties can comply with Strateq's obligations under applicable data protection laws;
b) Contract - ensure that an agreement is carried out with the data processor to:
    i. limit the processing of personal data to that is strictly required to provide the relevant services;

ii. comply with all applicable data protection requirements whether legislative or regulatory;
iii. notify Strateq without undue delay once it has reason to believe that a data breach has occurred in relation to personal data it processes for or on behalf of Strateq;
iv. provide Strateq with the right to conduct spot checks to ensure that the data processor is compliant; and
v. indemnify Strateq for any loss which arise from their misuse of the personal data its breach of applicable laws or the terms of the agreement.

c) Monitoring - check periodically, after the execution of contract, in accordance with internal procedures to ensure that the data processor continues to satisfy Strateq's standards.

9.1 Cloud Computing Services

The following additional requirements apply where Strateq engages cloud computing vendors:

a) Transfer of personal data through cloud computing service must obtain written consent by an officer authorized by the top management of Strateq.
b) Any transfer of data through cloud computing service must be recorded.
c) Personal data transferred through cloud computing services must comply with applicable data protection laws.

10. DATA SECURITY

The data security measures set out below must be implemented and complied with to protect personal data from any loss, misuse, modification, unauthorized, unlawful, or accidental access or disclosure, alteration or destruction. If there are any circumstances which may affect Strateq's ability to comply, please consult the DPO.

10.1 Administrative measures (applicable to both electronic and non-electronic data)

a) Require all employees to be bound by confidentiality obligations, which may be provided for in the employees' employment contracts.
b) Set up a registration system which records each employee involved in the processing of personal data.
c) In respect of each employee involved in the processing of personal data:
i. provide them with a user ID and password;
ii. terminate their access rights to the personal data and/or delete the user ID and password provided immediately when they no longer manage personal data;
iii. revoke their access rights to the personal data and/or delete their user ID and password provided when they resign, are terminated, or where there have been changes in their role; and
iv. designate limits on their access to personal data for purpose of collection, processing and storage of personal data (e.g. certain employees may only be allowed rights to access and view personal data only, whereas other employees may have access and modification rights in relation to personal data).
d) Ensure that only employees registered in accordance with (b) and (c) above are allowed to process personal data.

e) Maintain database to record any access to personal data (i.e., who and when), and how such data are subsequently used, including whether such personal data were transferred to third parties (including within the Strateq group of companies) and the means (e.g. email, fax, hand delivery, mail, removable media devices, cloud computing services, etc.) used to transfer such data.
f) Conduct regular training sessions for employees to impart best practices in handling personal data and strengthen awareness of threats to security of personal data.
g) Implement robust policies and procedures regarding confidentiality (with disciplinary consequences for breaches).
h) Ensure that only the appropriate amount of personal data is held.
i) Implement a business continuity plan as a contingency measure in the event personal data is lost.

10.2 Technical measures (applicable to electronic data only)

a) Install appropriate computer security software and using suitable computer security settings including:
    i. update back up or recovery system and use the latest anti-virus software to protect personal data from any loss, misuse, modifications, unauthorized, unlawful, or accidental access, or disclosure, alteration or destruction; and
    ii. protect computer systems from malware threats to avoid attacks, e.g., by installing the latest anti-malware software.
b) Adopt appropriate access controls (e.g., stronger authentication measures).
c) Encrypt personal data to prevent unauthorized access.
d) Activate self-locking mechanisms if the computer is left unattended.
e) Use the right level of email security settings when sending or receiving highly confidential emails.
f) Update computer security and IT equipment regularly.
g) Ensure that IT service providers can provide the requisite standard of IT security.
h) Dispose of personal data in IT devices that are to be recycled, sold or disposed of.
i) Obtain authorization from top management of Strateq prior to use of any removable media devices and cloud services.
j) Record any transfer of data through removable media devices and cloud services.
k) Use of cloud services must follow applicable data protection laws.
l) Have in place the following physical security procedures:
    i. control access to the data storage area;
    ii. store the personal data in a suitable location which is safe from physical or natural threats and is not exposed.
    iii. provide close circuit security cameras (if necessary), and
    iv. provide 24-hour security control.

10.3 Physical measures (applicable to non-electronic data only)

a) Mark confidential documents clearly and prominently.
b) Restrict employee access to confidential documents on a need-to-know basis.
c) Use privacy filters to minimize unauthorized viewing on laptops.
d) Proper, careful and efficient disposal of confidential documents which contain personal data through shredding or similar means.

e) Ensure an appropriate level of security during delivery or transmission of personal data (e.g., prepaid A.R. registered post instead of normal post).
f) Provide a summary of the personal data contained in storage so that personal data is accessed only when necessary.
g) Confirm that the intended recipient is correct to avoid undue disclosure of personal data.
h) Adopt a clear-desk policy.
i) Ensure the following physical security procedures are in place:
    i. all personal data should be stored in files in an orderly manner;
    ii. all files that contain personal data to be stored in locked place;
    iii. all keys shall be kept in a safe place;
    iv. maintain a record on where the keys are kept; and
    v. store personal data shall be in an appropriate location which is safe from physical and natural threats and is not exposed.

11. RETENTION AND DISPOSAL

Generally, any personal data which is no longer required in connection with the purposes for which the data was collected should be permanently deleted or destroyed, unless required to be retained pursuant to applicable laws.

Please refer to the Strateq Group Data Retention and Disposal Policy for details.

12. DATA INTEGRITY, ACCESS, AND CORRECTION

12.1 Maintaining up-to-date data

Reasonable steps must be taken to ensure that personal data held by Strateq is accurate, complete, not misleading and kept-up-date. This is done by ensuring that data subjects are able to access and correct their data via Strateq's personal data update form.

12.2 Data subject requests

Data subjects may request to exercise certain rights under applicable data protection laws (e.g., access to or correction of their personal data) - see Section 5 of each country's Local Guidelines for details.

If Strateq receives such a request, please refer to the DPO immediately who will advise on the next steps, the relevant requirements, and timelines to be complied with.

Records of all such requests received from individuals or the relevant persons must be retained.

13. RECORDS OF PROCESSING

Generally, Strateq must keep and maintain a record of any application, notice, request or any other information relating to the personal data that is being processed.

Where consent is the legal basis relied upon by Strateq for the lawful processing of personal data, records of data subjects providing consent must be properly recorded and maintained by Strateq.

13.1 Personal data systems

Strateq may deploy systems, whether automated or otherwise, which are used by Strateq for the processing of personal data ("personal data systems").

Where Strateq maintains such personal data systems, the following must be properly recorded and retained:

a) the record of the consent from a data subject maintained in respect of the processing of personal data by Strateq;
b) the record of use or disclosure of personal data without the consent from a data subject (e.g. by relying on another legal basis);
c) the record of a written privacy notice issued by Strateq to the data subject;
d) the personal data collected and the purpose for the collection of each category of personal data;
e) the list of disclosures to third parties in respect of personal data that has been or is being processed by Strateq;
f) the retention period of the personal data and the record of compliance to demonstrate compliance with the Retention principle in this Policy;
g) the record of compliance in accordance with the Integrity principle in this Policy;
h) the record of rejection or objection according to certain data subject rights;
i) the rights and methods for accessing personal data, including the conditions for personnel entitled to such access and the conditions to access such personal data;
j) details of Strateq's data security measures; and
k) such other related information.

The personal data system should be maintained in a manner which is organized and easily accessible, in the event an inspection is carried out by the regulators and/or data subjects exercise their rights under applicable law and request certain records of processing.

14. DIRECT MARKETING

Marketing and other promotional material or similar communications may only be sent to data subjects who have consented to receiving the same. At any time, data subjects may withdraw their consent (e.g., unsubscribe) and Strateq must cease sending any such materials upon receiving such withdrawal.

Save for Singapore, consent for direct marketing may be obtained as part of the data subject's consent to the processing of personal data by Strateq, where direct marketing must be noted as one of the purposes in the privacy notice. To the extent that Strateq relies on a legal basis other than consent to process the data subject's personal data, consent to process personal data for direct marketing should be separately obtained.

Once data subjects inform Strateq by written notice to cease processing their personal data for purposes of direct marketing, Strateq must comply with such notice and ensure that such marketing materials are no longer directed at these data subjects.

Additional or different guidelines may apply in some jurisdictions - see Section 6 of each country's Local Guidelines for details.

15. DATA BREACH

Any known, suspected, or potential threat to the security of personal data, including unauthorized or unlawful access, acquisition, disclosure, alteration, modification, loss, or use of the personal data ("Data Breach Incidents") must be reported to the DPO immediately. This includes Data Breach Incidents notified by any third-party service providers, business partners or other individuals.

Please refer to the Strateq Group Data Breach Management Policy for details.

16. LOCAL GUIDELINES MALAYSIA

Section 1
Additional guidelines on legal bases for processing personal data

Refer section 5.1 of the Policy. Other relevant guidelines as mandated by the Commissioner are as follows:

- Personal Data Protection Act 2010 (Act709)
- Personal Data Protection (Amendment) Act 2024 (Act A1727)
- Data Protection Officer Guideline (effective 01 June 2025)
- Data Breach Notification Guideline (effective 01 June 2025)
- Data Portability Guideline (effective date to be advised)
- Cross-Border Data Transfer Guideline (effective date to be advised)
- Data Protection Impact Assessment Guideline (effective date to be advised)
- Privacy by Design Guideline (effective date to be advised)
- Profiling and Automated Decision-Making Guideline (effective date to be advised)

Section 2
Sensitive personal data

Definition of "sensitive personal data"
Any personal data consisting of information in relation to data subjects as to:

(a) their physical or mental health or condition;
(b) their political opinions;
(c) their religious beliefs or other beliefs of a similar nature; and
(d) the commission or alleged commission by them of any offence, biometric data or any other personal data as the Miniter may determine by order published in the Gazette.

Consent requirements or other legal bases for processing
Sensitive personal data can only be processed if:

(a) data subjects have given their explicit consent to such processing;
(b) the information contained in the personal data has been made public because of steps deliberately taken by the data subjects; or
(c) processing is necessary:
    i. for the purposes of exercising or performing any legal right or obligation on Strateq in connection with employment;
    ii. to protect the vital interests of the data subjects or another person, in a case where consent cannot be given by or on behalf of the data subjects or Strateq cannot be reasonably expected to obtain the data subjects' consent;
    iii. to protect the vital interests of another person, in a case where consent by or on behalf of the data subjects has been unreasonably withheld;
    iv. for medical purposes and is undertaken by a healthcare professional or any person who owes a duty of confidentiality equivalent to that of a healthcare professional;
    v. for the purposes of legal proceedings, obtaining legal advice, or establishing, exercising, or defending legal rights; or

vi. for the administration of justice or exercise of any statutory functions.

Section 3
Local requirements for cross-border data transfers

Personal data can only be transferred to a place outside Malaysia if:

(a) there is in that place in force any law which is substantially similar to the Malaysia Personal Data Protection Act 2010 and Personal Data Protection (Amendment) Act 2024;
(b) that place ensures and adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the Malaysia Personal Data Protection Act 2010 and Personal Data Protection (Amendment) Act 2024;
(c) the data subjects have given their consent to the transfer;
(d) the transfer is necessary for the performance of a contract between the data subjects and Strateq;
(e) the transfer is necessary for the conclusion or performance of a contract between Strateq and a third party which is entered into at the request of the data subjects or is in the interest of the data subjects;
(f) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
(g) Strateq has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would a contravention of the Malaysia Personal Data Protection Act 2010 and Personal Data Protection (Amendment) Act 2024;
(h) transfer is necessary in order to protect the vital interests of the data subjects;
(i) Strateq has reasonable grounds to believe that in all circumstances of the case:
   i. the transfer is for the avoidance or mitigation of adverse action against the data subjects;
   ii. it is not practicable to obtain consent in writing of the data subjects to that transfer; and
   iii. if it was practicable to obtain such consent, the data subjects would have given their consent.

Section 4
Direct obligations on Strateq as data processor under local laws

Refer Malaysia Personal Data Protection Act 2010 and Personal Data Protection (Amendment) Act 2024, section 5 and section 9.

Section 5
Dealing with data subjects' requests

Data Access Request

A data subject has the right to:
a) be informed of details of his/her personal data that is being processed by or on behalf of Strateq; and
b) request for information on his/her personal data and have a copy of the same.

21 Days	Upon receipt of the data access request, Strateq should within 21 days of receipt of such request: a) Acknowledge and record receipt of request;

	b) Establish the identity of the requestor and confirm that he/she is legally entitled to data access; c) Locate the personal data requested; d) Identify and address any related issues, such as: • The existence of a relevant court order against granting access; • The application of other law other than the Malaysian Personal Data Protection Act 2010 and Personal Data Protection (Amendment) Act 2024; • Divulgement of any confidential information; or • Disclosure of personal information of other data subjects; and e) Provide the requestor with a copy of the data requested. Where Strateq cannot fully comply within the 21-day period, it should prior to its expiry notify the requestor of the delay (providing reasons) and comply as far as possible. However, in certain circumstances, Strateq may refuse a data access request by informing the requestor and providing reasons within the 21-day period.
14 Days	Strateq is under an obligation to comply with the whole data access request within 14 days after the expiry of the initial 21-day period.

EXCEPTIONS

Strateq may refuse a data access request where:

a) insufficient data is supplied to identify the requestor or the data subject, or that the requestor is the relevant person in relation to the data subject;
b) insufficient data is supplied to locate the requested personal data;
c) the burden of expense of providing access is disproportionate to the risks to the data subject's privacy;
d) Strateq cannot comply with the request without disclosing personal data of another individual. In such a situation, the consent of the individual is required;
e) another data controller controls the processing of the data and prohibits access;
f) providing access is against an order of a court;
g) providing access would disclose confidential commercial information; or
h) access to the data is regulated by another law.

Data Correct Request

A data subject has the right to:

a) correct the personal data; and
b) supply the requestor with a copy of the corrected personal data.

21 Days	Upon receipt of the data access request, Strateq should within 21 days of receipt of such request: a) Acknowledge and record receipt of request; b) Establish the identity of the requestor and confirm that he/she is legally entitled to data access; c) Locate the personal data requested; d) Identify and address any related issues, such as: • The existence of a relevant court order against granting access; • The application of other law other than the Malaysian Personal Data Protection Act 2010 and Personal Data Protection (Amendment) Act 2024; • Divulgement of any confidential information; or • Disclosure of personal information of other data subjects; and e) Provide the requestor with a copy of the data requested. Where Strateq cannot fully comply within the 21-day period, it should prior to its expiry notify the requestor of the delay (providing reasons) and comply as far as possible. However, in certain circumstances, Strateq may refuse a data access request by informing the requestor and providing reasons within the 21-day period.
14 Days	Strateq is under an obligation to comply with the whole data access request within 14 days after the expiry of the initial 21-day period.

EXCEPTIONS

Strateq may refuse a data access request where:

a) insufficient data is supplied to identify the requestor or the data subject, or that the requestor is the relevant person in relation to the data subject;
b) insufficient data is supplied to locate the requested personal data;
c) the burden of expense of providing access is disproportionate to the risks to the data subject's privacy;
d) Strateq cannot comply with the request without disclosing personal data of another individual. In such a situation, the consent of the individual is required;
e) another data controller controls the processing of the data and prohibits access;
f) providing access is against an order of a court;
g) providing access would disclose confidential commercial information; or

h) access to the data is regulated by another law.

Section 6
Additional guidelines on direct marketing

Refer Section 14 of the Policy.

Refer to new section 43A in Personal Data Protection (Amendment) Act 2024 on Rights to Data Portability.
(1) Subject to Section 43 subsection (2), a data subject may request the data controller to transmit his personal data to another data controller of his choice directly by giving a notice in writing by way of electronic means to the data controller.
(2) The request for data portability referred to in Section 43 subsection (1) is subject to technical feasibility and compatibility of the data format.
(3) Upon receiving the request for data portability under Section 43 subsection (1), the data controller shall complete the transmission of personal data within the period as may be prescribed.

17. LOCAL GUIDELINES UNITED STATES

These Local Guidelines for United States should be read together with Strateq's HIPAA Policies. In the event of any conflict between the two, the HIPAA Policies will prevail.

Section 1 Additional guidelines on legal bases for processing personal data.
None under federal law. Please refer to applicable state laws for additional data processing obligations.
Section 2 Sensitive personal data
Definition of "sensitive personal data" Under the Health Insurance Portability and Accountability Act ("HIPAA"), "Personal Health Information" ("PHI") is generally defined as health data created, received, stored, or transmitted by HIPAA-covered entities and other business associates in relation to the provision of healthcare, healthcare operations and payment for healthcare services that relates to the past, present, or future physical or mental health or condition of the individual, or the past, present, or future, payment of health care to that individual that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Examples include demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide health services or healthcare coverage. Additional state laws apply to personally identifiable information, education records, and other personal information. Enhanced protections typically exist for sexually transmitted diseases, substance abuse, HIV status, and mental health treatment records. **Consent requirements or other legal bases for processing** A covered entity (e.g., health plans, healthcare clearinghouses and healthcare providers) is permitted to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: a) To the individual (unless required for access or accounting of disclosures); b) Treatment, payment, and health care operations; c) Opportunity to agree or object; d) Incident to an otherwise permitted use and disclosure; e) Public interest and benefit activities; and f) Limited data set for the purposes of research, public health, or health care operations. Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.
Section 3 Local requirements for cross-border data transfers

None under federal law. Please refer to applicable state laws and/or commercial relationships/contract entered into by Strateq and other third parties.
Section 4 Direct obligations on Strateq as data processor under local laws
Implement appropriate physical, technical, and administrative safeguards to maintain the privacy and integrity of the data.

Section 5
Dealing with data subjects' requests

Data Access Request

A data subject has the right to:

a) be informed of details of his/her personal health information that is being processed by Strateq on behalf of a covered entity; and
b) request for information on his/her personal data and have a copy of the same pursuant to 45 CFR Part 164.524.

30 Days	Upon receipt of the data access request, Strateq should within 30 days of receipt of such request: a) Acknowledge and record receipt of request; b) Establish the identity of the requestor and confirm that he/she is legally entitled to data access; c) Locate the personal data requested (whether in paper or electronic form); d) Identify and address any related issues, such as: • The existence of a relevant court order against granting access; • The application of other law other than HIPAA; • Divulgement of any confidential information; or • Disclosure of personal information of other data subjects; and e) Provide the requestor with a copy of the data requested. Where Strateq cannot fully comply within the 30-day period, it should prior to its expiry notify the requestor of the delay (providing reasons) and comply as far as possible. A 30-day extension is permissible. refuse a data access request by informing the requestor and providing reasons within the 21-day period.

EXCEPTIONS

Strateq may refuse a data access request where it provides a written denial letter where:

a) insufficient data is supplied to identify the requestor or the data subject, or that the requestor is the relevant person in relation to the data subject;
b) insufficient data is supplied to locate the requested personal data;
c) the information relates to an individual's psychotherapy notes or information compiled for legal proceedings;
d) Strateq cannot comply with the request without disclosing personal data of another individual. In such a situation, the consent of the individual is required;
e) another data user controls the processing of the data and prohibits access;
f) providing access is against an order of a court;
g) providing access would disclose confidential commercial information;
h) the individual refuses to pay a "reasonable, cost-based fee" for copying and processing the record; or
i) access to the data is regulated by another law.

Data Correct Request

A data subject has the right to:

a) correct the personal data; and
b) supply the requestor with a copy of the corrected personal data.

30 Days	Upon receipt of the data access request, Strateq should within 21 days of receipt of such request: a) Acknowledge and record receipt of request; b) Establish the identity of the requestor and confirm that he/she is legally entitled to data access; c) Locate the personal data requested; d) Identify and address any related issues, such as: • The existence of a relevant court order against granting access; • The application of other law other than the Malaysian Personal Data Protection Act 2010; • Divulgement of any confidential information; or • Disclosure of personal information of other data subjects; and e) Provide the requestor with a copy of the data requested. Upon receipt of the data correction request, Strateq should within 30 days of receipt of such request: a) Acknowledge and record receipt of request; b) Establish the identity of the requestor and confirm that he/she is legally entitled to correct the data; c) Identify and address any related issues such as: • The existence of a relevant court order; • The application of other law other HIPAA; • Divulgement of any confidential information; • Disclosure of personal information of other data subjects; d) Confirm that the correction provided will make the data more accurate, complete or updated; e) Locate the data requested and correct the same as requested; f) Provide the requestor with a copy of the corrected data; and g) If the personal data has been disclosed to a third party in the preceding 12 months from the date of correction and there is no reason to believe that such third party has ceased using the personal data, Strateq must take all practicable steps to supply such third party with the corrected personal data and provide reasons for the same. Where Strateq cannot fully comply within the 30-day period, it should notify the requestor of the delay (providing reasons) and comply as far as possible.

EXCEPTIONS

Strateq may refuse a data correction request where:

a) insufficient information was supplied to identify the requestor (if a relevant person) or the data subject;
b) the covered entity did not create the record, or the information is not part of the designated record set;
c) insufficient information was supplied to ascertain in what way the personal data to which the data correction request relates is inaccurate, incomplete, misleading or not up to date;
d) Strateq is not satisfied that the personal data to which the data correction request relates is inaccurate, incomplete, misleading or not up to date;
e) Strateq is not satisfied that the correction which is the subject of the data correction request is accurate, complete, not misleading or up to date; or
f) another data user controls the processing of the personal data to which the data correction request relates in such a way as to prohibit Strateq from complying, whether in whole or in part, with the data correction request.

Additional protections may apply to non-PHI but other sensitive and individually identifiable information where set forth under applicable state laws. Also refer to Strateq's HIPAA Policies (including the PHI Uses and Disclosures Policy).

Section 6
Additional guidelines on direct marketing

The HIPAA Privacy Rule provides patients with important controls over how and whether their protected health information may be used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of PHI is permissible. Marketing communications are distinguished under the law from other communications about goods and services that are for quality health care.

18. LOCAL GUIDELINES CHINA

Section 1
Additional guidelines on legal bases for processing personal data.

Consent of data subjects is, by statute, the main legal basis ground for collection of personal data.

The following non-consent legal bases are currently recognized by data protection law of the People's Republic of China ("PRC"):

a) Processing of personal data disclosed by a data subject him/herself or through other legitimate manners within the reasonable scope, unless the data subject explicitly rejects such processing activities, or the processing activities would severely infringe legitimate interests of such data subject;
b) Other reasonable processing activities for the purpose of safeguarding public interests or legitimate rights of data subjects.

There are other non-consent legal bases recognized under the recommended national standards (i.e., Personal Information Security Specification), including processing of personal data is:

a) in connection with the fulfilment of obligations under laws and regulations;
b) directly related to national security or national defense;
c) directly related to public security, public health or major public interests;
d) directly related to criminal investigations, prosecutions, trials or execution of court decisions;
e) essential to the signing and performing of a contract requested by data subjects;
f) essential to maintaining safe and stable operation of the product or service provided, such as the discovery and handling of product or service failures;
g) essential for news agencies to carry out legitimate news reporting; or
h) essential for academic research institutions to carry out statistics or academic research for public interests, provided that the personal data contained in the results is de-identified when it makes the academic research or the descriptive results available

Please note that PRC data protection law does not allow for the collection and processing of personal data on the basis of the "legitimate interests" of corporate entities.

Section 2
Sensitive personal data

Definition of "sensitive personal data"
Sensitive personal data is not statutorily recognized and categorized under currently effective PRC data protection law. Under the recommended national standards (i.e., Personal Information Security Specification), sensitive personal data is defined as personal data that may lead to bodily harm, property damage, reputational harm, harm to personal health, or discriminative treatment of an individual if such data is disclosed, leaked, or abused.

Consent requirements or other legal bases for processing

Under the current PRC data protection law, sensitive personal data is treated similarly as personal data, and the legal bases for processing of personal data shall be equally applicable to processing of sensitive personal data.

While the current PRC data protection law is silent on whether consent to processing of sensitive personal data should be made in an explicit or in an implied manner, according to the recommended national standards (i.e., Personal Information Security Specification), the recommended best practice is to obtain an explicit consent from the data subject to process his/her sensitive personal data.

Section 3
Local requirements for cross-border data transfers

Under currently-effective PRC data protection law, there are no restrictions on cross-border data transfer of personal data as a general matter, provided that the consent of the data subjects with respect to such transfer has been obtained and the entity conducting the cross-border transfer is not an operator of "Critical Information Infrastructure" ("CIIO").

According to Article 31 of the Cybersecurity Law ("CSL"), the term "Critical Information Infrastructure" or "CII" is defined to include "the infrastructure used for public communication, information services, energy, transport, water conservancy, finance, public services, e-government affairs, and other important industries and fields and other critical information infrastructure that will result in serious damage to the national security, national economy, and people's livelihood and public interests if they are destroyed, there are lost functions or they are subject to data leakage."

However, the exact scope of CII is not entirely clear under the CSL and is expected to be further clarified in implementation regulations issued by the PRC authorities. As a general legal requirement, an entity that is classified as a CIIO needs to store and process in China personal data collected and generated in the course of operations conducted in China, unless it is truly necessary for the CIIO to transfer such personal data abroad, in which case it needs to obtain clearance from a competent Chinese regulator.

Section 4
Direct obligations on Strateq as data processor under local laws

The current PRC data protection law does not distinguish the concept of data controller and data processor. This means that the relevant requirements and obligations under PRC data protection law will be equally applicable to Strateq if it only processes personal data on behalf of its clients.

Section 5
Dealing with data subjects' requests

Data Access Request
A data subject has the right to:

a) be informed of details of his/her personal data that is being processed by or on behalf of Strateq; and
b) request for information on his/her personal data and have a copy of the same.

Data Correction Request
A data subject has the right to:
a) correct the personal data; and
b) supply the requestor with a copy of the corrected personal data.

Data Deletion Request
A data subject has the right to:
a) delete any personal data processed in violation of the laws and regulations or agreement between the data subject and Strateq.

Upon receipt of the data access request, Strateq should promptly respond to such a request:
a) Acknowledge and record receipt of request;
b) Establish the identity of the requestor and confirm that he/she is legally entitled to data access;
c) Locate the personal data requested;
d) Identify and address any related issues, such as:
    - The existence of a relevant court order against granting access;
    - The application of other law other than the PRC data protection law;
    - Divulgement of any confidential information; or
    - Disclosure of personal data of other data subjects; and
e) Provide the solution to the request brought by the requestor

However, in certain circumstances, Strateq may refuse a data access request by informing the requestor and providing reasons.

EXCEPTIONS
Strateq may refuse a data access request where:
a) the processing activities are in connection with the fulfilment of obligations under laws and regulations by Strateq;
b) the processing activities are directly related to national security or national defense;
c) the processing activities are directly related to public security, public health or major public interests;
d) the processing activities are directly related to criminal investigations, prosecutions, trials or execution of court decisions;
e) where Strateq has sufficient evidence to show that the data subject has malicious intent or abuses his/her rights;
f) the processing activities are for the purpose of protecting the life, property or other significant legal rights and interests of a data subject or other individuals, and it is difficult to obtain consent from such data subject;

g) responding to a data subject's request will bring about grave harm to the legitimate rights and interests of such data subject, other individuals, or organizations; or
h) trade secrets are involved.

Section 6
Additional guidelines on direct marketing

None in addition to Section 14 of the Policy.

19. LOCAL GUIDELINES HONG KONG

Section 1 Additional guidelines on legal bases for processing personal data.
Under the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"), there is no concept of "legal bases" for the purposes of processing personal data. Generally, Data Protection Principle ("DPP") 1 of the PDPO provides that personal data shall not be collected unless the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data. DPP 1 further provides that personal data shall be collected by means which are lawful and fair in the circumstances of the case.
Section 2 Sensitive personal data
Definition of "sensitive personal data" There is no definition of "sensitive personal data" under the PDPO. However, there are specific Codes of Practices that set out requirements with respect to certain types of personal data which are more sensitive in nature. Examples of such personal data include: a) Identity Card Number and other Personal Identifiers; b) Consumer Credit Data c) Biometric Data d) Health Records **Consent requirements or other legal bases for processing** Personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user who is using the data. Personal data shall be collected by means which are lawful and fair in the circumstances of the case. Generally, the following principles and factors should be taken into consideration before collecting data which are more sensitive in nature: 1) necessity and proportionality; 2) data minimization; and 3) providing transparency to the data subject from whom data is being collected. Where a Code of Practice is applicable to a specific type of personal data, such Code of Practice should be adhered to.
Section 3 Local requirements for cross-border data transfers
There are requirements in Hong Kong that regulate the transfer of personal data outside of Hong Kong, however, these requirements are not currently in force and therefore do not need to be strictly complied with. For reference, under local law (which is not in force), it provides that a data user shall not transfer personal data to a place outside of Hong Kong unless one of the following conditions is met:

a) The place is specified by the Privacy Commissioner in a whitelist - no such whitelist gazetted to date;
b) Strateq has reasonable grounds for believing that the place has laws substantially similar or servers a similar purpose to Hong Kong's data privacy laws;
    - The data subject has consented in writing to the transfer;
    - Strateq has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; and it is not practicable to obtain the consent in writing of the data subject to that transfer; but if it was practicable, such consent would be given;
    - The data transfer is an exempted transfer from under law;
    - The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not be collected, held, processed, or used in any manner in which, if that place were Hong Kong, would be a contravention of Hong Kong law.

Section 4
Direct obligations on Strateq as data processor under local laws

None.

Section 5
Dealing with data subjects' requests

Data Access Request

A data subject has the right to:

a) be informed in writing that Strateq holds data concerning the data subject (if Strateq does in fact hold such data); and
b) request for information on his/her personal data and have a copy of the same.

40 Days	Upon receipt of the data access request, Strateq should within 40 days of receipt of such request: a) acknowledge and record receipt of request; b) establish the identity of the requestor and confirm that he/she is legally entitled to data access; c) locate the personal data requested; d) identify and address any related issues, such as: • the existence of a relevant court order against granting access; • the application of other law other than the Personal Data (Privacy) Ordinance (Cap. 486); • divulgement of any confidential information; or • disclosure of personal information of other data subjects; and e) provide the requestor with a copy of the data requested or where Strateq does not hold such a record, informing the requestor that no such data is held. Where Strateq cannot fully comply within the 40-day period, it should prior to its expiry notify the requestor in writing of the situation with reasons and comply with the data access request to the extent that Strateq is able to comply with the request (i.e., comply partially). Strateq is required to comply fully with the data access request as soon as practicable thereafter.

EXCEPTIONS

Strateq may refuse a data access request where it provides a written denial letter where:

j) insufficient data is supplied to identify the requestor or the data subject, or that the requestor is the relevant person in relation to the data subject;
k) insufficient data is supplied to locate the requested personal data;
l) the information relates to an individual's psychotherapy notes or information compiled for legal proceedings;
m) Strateq cannot comply with the request without disclosing personal data of another individual. In such a situation, the consent of the individual is required;
n) another data user controls the processing of the data and prohibits access;
o) providing access is against an order of a court;
p) providing access would disclose confidential commercial information;
q) the individual refuses to pay a "reasonable, cost-based fee" for copying and processing the record; or

r) access to the data is regulated by another law.

Strateq shall refuse a data access request where:

a) insufficient data is supplied to identify the requestor or the data subject, or that the requestor is the relevant person in relation to the data subject;
b) Strateq cannot comply with the request without disclosing the personal data of a third party; or
c) compliance with the request is prohibited under the PDPO or any other ordinance.

Strateq may refuse a data access request where:

a) the request is not in Chinese or English;
b) insufficient data is supplied to locate the requested personal data. Where the description of the requested data is too generic, it is reasonable for Strateq to seek clarification from the requestor. If requestor fails to supply information reasonably requested, Strateq may refuse to comply with request;
c) the request is not made in the designated form set out by the Privacy Commissioner (however, it is recommended that requests in other formats should be in any event be responded to);
d) the request follows two or more similar requests, and it is unreasonable for the data user to comply with the request in the circumstances;
e) another party controls the use of the requested data in a way that prohibits the data user from complying with the request;
f) Strateq is entitled under the PDPO or any other ordinance not to comply with the request; or
g) there is an applicable exemption provided in the PDPO from complying with the request;

Strateq should erase any personal data relating to a third party from the copy of the requested data unless Strateq is satisfied that the third party has consented to the disclosure.

Data Correct Request

A data subject has the right to request that Strateq make the necessary corrections to their data where the data subject considers that data held by Strateq about them is inaccurate.

40 Days	Upon receipt of the data access request, Strateq should within 40 days of receipt of such request: a) acknowledge and record receipt of request; b) assess whether request is a data correction request as defined under the PDPO; c) establish the identity and authority of requestor and confirm that he/she is legally entitled to correct the data; d) assess the content of the data correction request; e) identify and address any related issues, such as the application of other law other than the Personal Data (Privacy) Ordinance (Cap. 486);

	f) consider accuracy of each and every item in the data correct request; g) correct the inaccurate data without a fee; and h) provide the requestor with a copy of the corrected data. Where Strateq cannot fully comply within the 40-day period, it should comply with the data correction request to the extent that Strateq is able to comply and notify requestor in writing reasons for non-compliance within the 40-day period. Strateq is required to comply fully with the data correction request as soon as practicable thereafter.

EXCEPTIONS

Strateq may refuse a data correction request where:

a) the data correction request is not made in Chinese or English writing;
b) it is unable to verify the identity and authority of the requestor;
c) it is not satisfied that the personal data to which the data correction request relates is inaccurate;
d) it is not provided with sufficient information to ascertain that the data is inaccurate; or
e) it is not satisfied that the correction provided in the data correction request is accurate.

If Strateq decides to refuse to comply with a data correction request, a data user is obliged to give written notice and reasons for the refusal to the requestor of the receipt of the data correction request. The PDPO does not allow a refusal to be delayed.

Section 6

Additional guidelines on direct marketing

Consent for the purposes of direct marketing includes an indication of no objection to the use or provision. Further, where Strateq intends to conduct direct marketing, the privacy policy should further include the following information:

a) the intention to use data for direct marketing purposes;
b) that Strateq may not use the data unless the data user has received the data subject's consent to the intended use;
c) the kinds of personal data to be used; and
d) the classes of marketing subjects in relation to which the data is to be used.

Where Strateq intends to provide personal data to another person for use by that other person in direct marketing, the privacy policy should further include the following information:

a) the intention to use data for direct marketing purposes;
b) that the data user may not use the data unless the data user has received the data subject's written consent to the intended use;
c) if the data is to be provided for gain, that the data is to be so provided;
d) the kinds of personal data to be used;
e) the classes of persons to which the data is to be provided; and

f) the classes of marketing subjects in relation to which the data is to be used.

20. LOCAL GUIDELINES SINGAPORE

Section 1
Additional guidelines on legal bases for processing personal data.

In addition to section 5.1 of the Policy, the legal bases to collect, use and disclose personal data in Singapore without consent are specified under the First and Second Schedules of the Personal Data Protection Act 2012 ("SG PDPA") and include:

1. Vital interests of the individuals: purposes that are clearly in the interests of the data subject or is necessary to respond to an emergency that threatens the life, health, or safety of the individual or another individual.
2. Matters affecting the public: the information is publicly available; the personal data is collected, used, or disclosed for national interest, solely for artistic or literary purposes, solely for archival or historical purposes or solely for news activity by a news organization.
3. Legitimate interests: before relying on this exception, an assessment of the adverse must be conducted to ensure the legitimate interests outweigh any adverse effect. Examples of legitimate interests include: for evaluative purposes; for any investigation or proceedings; for recovery or payment of debt owed; for the purposes of managing or terminating an employment relationship with or appointment of an individual.
4. Business asset transactions: transactions involving the sale, purchase, lease, merger or amalgamation or any other acquisition disposal or financing of Strateq for its interests.
5. Business improvement: purposes include improving goods and services, developing new methods for operations, understanding the behavior of individuals in relation to providing goods and services, and personalizing goods and services for individuals.

For further information, refer to the summary of the relevant legal bases here issued by the Personal Data Protection Commission ("PDPC").

Strateq must notify data subjects of the purposes and manner in which their personal data is processed, and to obtain an indication of their choice, on or before any collection of personal data takes place.

Section 2
Sensitive personal data

Definition of "sensitive personal data"
Singapore does not have a separate category of sensitive personal data. The SG PDPA neither defines the term "sensitive personal data" nor distinguishes between "sensitive personal data" and "non-sensitive personal data". However, the concept of "sensitive personal data" is recognized by the PDPC through its guidance and enforcement decisions, and refer to data such as medical data, financial data, and bankruptcy status.

Consent requirements or other legal bases for processing
The requirements for processing personal data are the same for all types of personal data including personal data of a more sensitive nature. For completeness, please note

that the PDPC has taken the view in its enforcement decisions that personal data of a sensitive nature should be subjected to a higher standard of protection.

Section 3
Local requirements for cross-border data transfers

For personal data to be transferred outside of Singapore, Strateq should:

a) take appropriate steps to ensure that it will comply with the obligations under the SG PDPA in respect of the transferred personal data, while such data remains under its possession or control; and
b) take appropriate steps to ascertain and ensure that the recipient is bound by legally enforceable obligations to provide the transferred personal data a standard of protection that is at least comparable to that under the PDPA. These "legally enforceable obligations" include:
    - those imposed under law;
    - contract;
    - binding corporate rules (for intra-corporate transfers only); or
    - any other legally binding instruments.

Strateq may also satisfy the requirement to transfer personal data outside of Singapore if personal data is transferred to a recipient organization holding certifications to the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System and the Asia-Pacific Economic Cooperation Privacy Recognition for Processors System.

Section 4
Direct obligations on Strateq as data processor under local laws

As a data intermediary/processor, Strateq will be subject to the following obligations under the SG PDPA:

a) Protection obligation: Strateq must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks.
b) Retention limitation obligation: Strateq must cease to retain documents containing personal data or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the retention of such personal data no longer serves the purpose for which it was collected, and is no longer necessary for legal or business purposes.
c) Data breach notification obligation: Strateq (as a data intermediary/processor) must notify the organization or public agency that it is processing personal data on behalf of without undue delay from the time it has credible grounds to believe that a data breach has occurred.

Section 5
Dealing with data subjects' requests

Data Access Request

A data subject has the right to have access to:

a) his/her personal data that is in the possession or under the control of Strateq; and
b) information about the ways in which the personal data referred to above has been or may have been used or disclosed by the organisation within a year before the date of the request.

30 Days	Upon receipt of the data access request, Strateq should within 30 days of receipt of such request: a) Acknowledge and record receipt of request; b) Establish the identity of requestor and confirm that he/she is legally entitled to data access; c) Locate the personal data requested; d) Identify and address any related issues, such as: • The existence of a relevant court order against granting access; • The application of other law other than the SG PDPA; • Divulgement of any confidential information; or • Disclosure of personal information of other data subjects; and e) Provide requestor with a copy of the data requested. Where Strateq cannot fully comply within the 30-day period, it should prior to its expiry notify the requestor of the delay (providing reasons) and the time by which it will be able to respond to the request.

EXCEPTIONS

Strateq may refuse a data access request in the following matters (See Fifth Schedule of the SG PDPA):

a) opinion data kept solely for an evaluative purpose;
b) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
c) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;
d) a document related to a prosecution if all proceedings related to the prosecution have not been completed;
e) personal data which is subject to legal privilege;
f) personal data which is disclosed would reveal personal data about another individual, other than any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual;
g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of Strateq;
h) any request that would unreasonably interfere with the operations of Strateq because of the repetitious or systematic nature of the requests;
i) any request that is frivolous or vexatious; or

j) any request for information that is trivial.

If Strateq refuses any data access request, Strateq would have to keep a copy of the personal data requested for, as the individual that has requested for this would be able to seek help from the PDPC or the courts, and this data has to be maintained during the process.

Data Correct Request

A data subject has the right to request for Strateq to correct an error or omission in the personal data about the individual that is in the possession or under the control of Strateq.

30 Days	Upon receipt of the data correction request, Strateq should within 30 days of receipt of such request: a) Acknowledge and record receipt of request; b) Establish the identity of requestor and confirm that he/she is legally entitled to correct the data; c) Identify and address any related issues such as: • The existence of a relevant court order; • The application of other law other than the SG PDPA; • Divulgement of any confidential information; • Disclosure of personal information of other data subjects; d) Confirm that the correction provided will make the data more accurate, complete or updated; e) Locate the data requested and correct the same as requested; f) Provide the requestor with a copy of the corrected data; and g) If the personal data has been disclosed to a third party in the preceding 12 months from the date of correction and there is no reason to believe that such third party has ceased using the personal data, Strateq must take all practicable steps to supply such third party with the corrected personal data and provide reasons for the same. Where Strateq cannot fully comply within the 30-day period, it should prior to its expiry notify the requestor of the delay (providing reasons) and the time by which it will be able to respond to the request.

EXCEPTIONS

Strateq may refuse a data correction request where (See Sixth Schedule of the SG PDPA):

a) opinion data kept solely for an evaluative purpose;
b) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
c) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;

d) a document related to a prosecution if all proceedings related to the prosecution have not been completed; or
e) in the case of derived personal data.

Section 6
Additional guidelines on direct marketing

Consent for direct marketing should be separately obtained from the data subject's consent to the processing of personal data by Strateq.

21. LOCAL GUIDELINES THAILAND

Section 1
Additional guidelines on legal bases for processing personal data.

All Strateq employees must ensure Strateq is always processing personal data in a lawful manner. Lawful basis is necessary in support of the rights for Strateq to process personal data. In certain cases, this means obtaining the lawful consent from data subjects to process their personal data. Here below are other legal bases that may apply e.g. where the processing is:

a) for the achievement of the purpose relating to the preparation of the historical documents or the archives for public interest, or relating to research or statistics in which the suitable measures to safeguard the data subject's rights and freedoms are put in place and in accordance with the sub-regulation as to be prescribed by the Personal Data Protection Committee (historical, research or statistics basis);
b) for preventing or suppressing a danger to a person's life, body or health (vital interest basis);
c) necessary for the performance of a contract to which the data subject is a party or for taking steps at the request of the data subject prior to entering into a contract (contractual basis);
d) necessary for the performance of a task carried out in the public interest by the data user or for the exercising of official authority vested in the data user (public interest or official authority power basis);
e) necessary for legitimate interests of the data user, or any other persons or legal persons other than the data user, except where such interests are overridden by the fundamental rights of the data subject of his/her personal data (legitimate interest basis); or
f) for compliance with any legal obligation to which the data user is subject (legal obligation basis).

Section 2
Sensitive personal data

Definition of "sensitive personal data"

Any personal data consisting of information in relation to data subjects as to:

a) their racial or ethnic origin;
b) their political opinions;
c) their cult, religious or philosophical beliefs;
d) their sexual behavior;
e) their criminal records;
f) their health data;
g) their disability;
h) their trade union data;
i) their genetic data;
j) their biometric data; and
k) any other data which may affect the data subjects in the same manner, as further prescribed by the Personal Data Protection Committee.

Consent requirements or other legal bases for processing

Sensitive personal data can only be processed if:

a) data subjects have given their explicit consent to such processing;
b) it is to prevent or suppress danger to life, body or health of the person where the data subject is incapable of giving consent by whatever reason;
c) it is carried out in the course of legitimate activities with appropriate safeguards by the foundations, associations or any other not-for-profit bodies with a political, religious, philosophical, or trade union purposes for their members, former members of the bodies, or persons having regular contact with such foundations, associations or not-for-profit bodies in connection with their purposes, without disclosing the personal data to outside of such foundations, associations or not-for-profit bodies;
d) the information has been made public with the explicit consent of the data subject;
e) it is necessary for establishing, complying, exercising or defending legal claims; or
f) the processing is necessary for compliance with legal obligation to achieve the purposes with respect to:
    - preventive medicine or occupational medicine, the assessment of working capacity of the employee, medical diagnosis, the provision of health or social care, medical treatment, the management of health or social care systems and services. In the event that it is not for compliance with legal obligation and such personal data is under the responsibility of the occupational or profession practitioner or person having the duty to keep such personal data as confidential under the law, it must be for compliance with the contract between the data subject and the medical practitioner;
    - public interest in healthcare such as protecting against cross-border dangerous contagious disease or epidemics which may be contagious or pestilent or ensuring standards or quality of medicines, medicinal products or medical devices, on the basis that there is a provision of suitable and specific measures to safeguard the rights and freedom of the data subject, in particular maintaining the secrecy of personal data in accordance with the duties or professional ethics;
    - employment protection, social security or national health security, social health welfare of the entitled person by law, the road accident victim's protection, or social protection in which the collection of personal data is necessary for exercising the rights or carrying out the obligations of the data user or the data subject and the suitable measures have been provided to protect the fundamental rights and interest of the data subject;
    - it is for the scientific, historical or statistic research purposes or other public interests which must be carried out only to the extent necessary to achieve such purposes, and the suitable measures have been provided to protect the fundamental rights and interest of the data subject to be prescribed by the Personal Data Protection Committee; or
    - the substantial public interest and the suitable measures have been provided to protect the fundamental rights and interest of the data subject.

Section 3

Local requirements for cross-border data transfers
Personal data can only be transferred to a place outside Thailand if: a) such place falls under a whitelist gazetted by the Personal Data Protection Committee and is carried out in accordance with the rules for the protection of personal data as to be prescribed by the Personal Data Protection Committee - no such whitelist gazetted to date; b) in the absence of the whitelist, personal data can be transferred to a place outside Thailand if: • for legal compliance; • the data subjects have given their consent to the transfer provided that the data subjects have been informed of the inadequate personal data protection standards of the destination country; • the transfer is necessary for the performance of a contract between the data subjects and Strateq or for taking steps at the request of the data subjects prior to entering into a contract; • it is for compliance with a contract between Strateq and a third party, which is for the interests of the data subjects; • it is to prevent or suppress danger to life, body or health of data subjects or other person, where the data subject is incapable of giving consent by whatever reason; or • the transfer is necessary for carrying out the activities in relation to substantial public interest. c) Strateq has a policy for cross-border transfer of personal data to another data user or data processor which is (i) located in a foreign country, and (ii) in the same affiliated business or the same group undertaking to jointly operate the business or group undertaking ("Binding Corporate Rules"), and (a) the policy of which is certified by the Office of the Personal Data Protection Committee, and (b) personal data is transferred overseas pursuant to such certified policy - no such sub-regulation on Binding Corporate Rules to date; or d) Strateq provides suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures according to the rules and methods as to be prescribed and announced by the Personal Data Protection Committee - no such sub-regulation on suitable protection measures to date.
Section 4 Direct obligations on Strateq as data processor under local laws
Apart from the general rule as mentioned in section 8 of the Policy, Strateq as a data processor must comply with the following: a) process only for the purpose they were instructed for, except where such instruction is illegal or is in breach of any provisions regarding personal data protection under the Personal Data Protection Act, B.E. 2562 (2019) ("TH PDPA"); b) maintain appropriate security measures for prevention of unauthorized or unlawful loss, access, use, alteration, modification or disclosure of personal data; c) notify the data user of any relevant Data Breach Incidents;

d) prepare and maintain a record of processing activities in accordance with the rules and methods set forth by the Personal Data Protection Committee - no such sub-regulation on record of processing activities to date;
e) This obligation may be exempted if the data processor is a small organization as prescribed by the Personal Data Protection Committee (no such sub-regulation on the definition of small organization to date) unless:
    - the processing of such personal data is likely to result in a risk to the rights and freedoms of data subjects;
    - not a business where the processing of personal data is occasional; or
    - involve in the processing of sensitive personal data.
f) enter into a contract with the data user to control the activities carried out in accordance with Strateq's obligation for compliance with the TH PDPA, in which such contract shall be in accordance with the requirements to be prescribed by the Personal Data Protection Committee. - no such sub-regulation on the detailed requirements of data processing agreement to date; and
g) designate a DPO and/or representative (where applicable).

Section 5
Dealing with data subjects' requests

Consent Withdrawal Request

a) A data subject has the right to request withdrawal of consent that the data subject has consented earlier.
    - Strateq must allow the data subject to withdraw their consent as equally easily as giving consent to Strateq.
    - If consent is withdrawn, all data processing activities carried out by Strateq that were based on consent and took place before the withdrawal remain lawful.
    - If withdrawal of consent affects the data subject in any aspect, Strateq must notify the data subject the effects of the withdrawal.
b) Exceptions
    - Strateq may refuse a consent withdrawal request where:
        - there is a restriction as imposed by law; or
        - there is a restriction as imposed by contract which gives benefit to the data subjects.

Data Access Request

a) A data subject has the right to:
    - request for access to information on his/her personal data and have a copy of the same. Strateq is required to provide the information within 30 days; and
    - be informed of details of the acquisition of his/her personal data that is being processed without his/her consent.
b) Exceptions
    - Strateq may refuse an access request where:
        - permitted by a legal obligation or order of a court; and
        - such access and obtaining a copy would adversely affect the rights and freedoms of others.

Data Portability Request

a) A data subject has the right to:
   - obtain a copy of certain personal data processed by Strateq in a structured, commonly used and machine-readable format by automated means;
   - request such personal data to be sent or transferred to another data user if it can be done by automated means;
   - request to directly obtain personal data in a format that Strateq sends or transfers to another data user, unless it is impossible to do so because of the technical circumstances.

b) The request shall be based on the condition that:
   - the personal data concerns the data subject;
   - the processing is based on the data subject's consent, or for the performance of a contract (contractual basis), or other lawful basis as determined in the future by the Personal Data Protection Committee; and
   - when processing is carried out by automated means.

c) Exceptions
   - Strateq may refuse a data portability request where:
     - the processing of personal data by Strateq is a performance carried out in the public interest or for compliance with a legal obligation; or
     - the exercise of right per the request would violate the rights and freedoms of others.

Objection Request

a) A data subject has the right to:
   - object to the processing based on legitimate interest basis or the performance of a task in the public interest / exercise of official authority basis;
   - object to direct marketing; and
   - object to the processing for the purpose of scientific / historical research and statistics basis.

b) In the event the data subject exercises his/her right to object, Strateq shall no longer be able to process such personal data and Strateq shall immediately distinguish such personal data clearly from other matters at the time the data subject gives the notice of objection to Strateq.

c) Exceptions
   - Where Strateq processes personal data on the basis of its legitimate interest basis or the performance of a task in the public interest / exercise of official authority basis and an objection is received, Strateq must stop processing personal data unless:
     - Strateq can demonstrate compelling legitimate ground for the processing of such personal data; or
     - the processing is for the establishment, compliance or exercise or defense of legal claims by Strateq.
   - Where Strateq processes personal data for the purpose of scientific / historical research and statistics basis and an objection is received, Strateq must stop processing personal data unless:
     - It is necessary of a task carried out in the public interest.

Data Deletion Request

a) A data subject has the right to request Strateq to delete, destroy or anonymize personal data.
b) The request will only apply when:
    - personal data is no longer necessary in relation to the purpose for which it was originally collected / processed;
    - the data subject withdraws consent and there is no other lawful basis applicable;
    - the data subject objects to the processing and there is no ground to refuse the objection request; or
    - the personal data was unlawfully processed.
c) Where Strateq made the relevant personal data publicly available, Strateq must take reasonable steps, including technical measures and be responsible for the expenses that may occur, to inform other data user which processes the personal data that the data subject has requested the deletion and obtain their response to comply with the request.
d) Exceptions
    - Strateq may refuse a deletion request where personal data is processed for the following reasons:
        - to exercise the right to freedom of expression and information;
        - archiving purposes in the public interest, scientific / historical research or statistical purposes;
        - necessary for the performance of a public task or exercise of official authority;
        - necessary for compliance with legal obligation to achieve the purposes with respect to preventive medicine or occupational medicine, assessment of working capacity, medical diagnosis, provision of health or social care, medical treatment and management of health or social care systems and services;
        - necessary for compliance with legal obligation to achieve the purposes with respect to public interest in the public health;
        - the establishment, compliance or exercise or defense of legal claims by Strateq; or
        - for compliance with a legal obligation.

Restriction Request

a) A data subject has the right to request Strateq to restrict the use of certain of their personal data.
b) The request will only apply when:
    - the personal data is pending verification for accuracy per the correction request;
    - the data subject requested the restriction instead of deletion;
    - the personal data is no longer necessary to be retained but the data subject requested the restriction for the establishment, compliance, exercise or defense of legal claims; or
    - the personal data is pending verification by Strateq whether Strateq can oppose an individual's objection request.

Data Correction Request

a) A data subject has the right to request Strateq to rectify personal data where the personal data held about the data subject is inaccurate, incomplete, not updated, or misleading.

Lodge a Complaint

a) A data subject has the right to lodge a complaint to the Expert Committee in cases where Strateq, its employees or contractors violates or fails to comply with the TH PDPA and/or its sub-regulations or does not fulfill the data subject's request.

Data Subject Rights Management Procedure

On a Continuing Basis	To manage the data subject request, Strateq should take the following steps: a) Inform the data subjects of their rights, and how they can exercise their rights; b) Establish and maintain a mechanism for data subjects to exercise their rights; c) Implement a mechanism for complying with the request; d) Keep up to date with training on what to do when a request is received, including who to contact and how to update any relevant database; e) Put in place a contractual obligation for vendors and suppliers to address promptly and effectively any request dealing with the exercise of a data subject request. In addition, require its vendors and suppliers to promptly communicate to Strateq any such request that they may receive from individuals.

1-30 DAYS (Depending on the request)	Depending on the data subject right, Strateq may consider the following time frames: a) Data Access Request: within 30 days of receipt of such request • The 30-day period is prescribed in the TH PDPA. b) Objection Request: within 3-5 days of receipt of such request • The TH PDPA requires data user to comply with the request immediately. However, in practice, verification of relevant personal data and the request could take some time. Hence, a 3–5-day period to comply with such request should be reasonable period of time to proceed with a request based on the legal requirement and practical perspective. c) Other Request: within 30 days of receipt of such request • Although the TH PDPA has not prescribed the timeframe for other data subject rights, recently, there was a public hearing on the draft sub-regulation regarding data subject rights. We therefore foresee that the timeframe in responding to other data subject right request should be in line with the Data Access Request. As such, we recommend a 30-day period while pending the official issuance of the sub-regulation. d) Upon receipt of the data subject request, Strateq should: • analyze the request and identify whether any further clarification is required; • acknowledge, record receipt of request and request for further information (if necessary); • establish the identity of requestor and confirm that he/she is legally entitled to exercise the data subject request; • consider whether the request is valid; • consider whether any exemptions apply. Apart from the exceptions listed above, Strateq may refuse a data subject request where: • insufficient data is supplied to identify the requestor or the data subject, or that the requestor is not the relevant person in relation to the data subject; • insufficient data is supplied to locate the requested personal data; • locate the data which is relevant to the request; • consider whether immediate action needs to be taken in relation to the personal data; • identify the responsible person to fulfill the request; • notify the relevant third party data processor of the request (if necessary) and seek cooperation in acting on the request; and • respond to the request explaining the actions taken or explaining why the request has been rejected.

60 DAYS	The criteria to extend the period for responding to the data subject request is subject to the sub-regulation - no such sub-regulation to date. Strateq may be able to extend the period for compliance by a further 60 days where there is a necessity, by taking into account the complexity and numbers of the requests, provided that Strateq informs the requestor of such extension within 30 days of receipt of such request and explains the reasons of such extension.
Post-Action	Record and document the details of the compliance or rejection, including explanation of why such request has been rejected (e.g., in the records of processing activities).

Section 6
Additional guidelines on direct marketing

None in addition to Section 14 of the Policy.