

ATMD Bird & Bird

Singapore Personal Data Protection Policy

Contents

1.	PURPOSE	1
2.	SCOPE	1
3.	COMMITMENT TO COMPLY WITH DATA PROTECTION LAWS	1
4.	PERSONAL DATA PROTECTION SAFEGUARDS	3
5.	ATMDBB EXCEPTIONS:	6
6.	VIOLATIONS:	6
7.	QUERIES OR COMPLAINTS	6
8.	APPROVAL AND VARIATION	6
9.	GLOSSARY	7

ATMD Bird & Bird
SINGAPORE PERSONAL DATA PROTECTION POLICY
REQUIREMENTS FOR ALL STAFF

1. PURPOSE

This document sets out the policies and procedures that ATMD Bird & Bird LLP ("**ATMDBB**") has put in place, to comply with Singapore's personal data protection law as set out in the Personal Data Protection Act 2012 ("**PDPA**").

2. SCOPE

All employees (whether full-time, part-time, contract-based) and personnel, including interns, (collectively "**staff**") working in ATMDBB must comply with the policy. All new ATMDBB staff will receive training on personal data protection as part of their induction programme, while existing ATMDBB staff will receive training on personal data protection as part of their ongoing training and development. After completion of the training programme, staff will be required to sign an acknowledgement form to acknowledge that they have undergone the training programme, understand their obligations and responsibilities, and agree to protect any personal data with which they come into contact with in accordance with the PDPA.

ATMDBB's Data Protection Officer ("**DPO**"), is responsible for ensuring ATMDBB's compliance with the PDPA. The DPO may delegate his/her various tasks and responsibilities.

3. COMMITMENT TO COMPLY WITH DATA PROTECTION LAWS

3.1 ATMDBB staff must comply with the obligations under the PDPA whenever they are processing Personal Data. The Personal Data Protection Safeguards set out in Section 4 below set out what this means.

3.2 The PDPA applies when Personal Data of individuals in Singapore is processed by, or on behalf of, ATMDBB or when Personal Data of individuals out of Singapore is brought into Singapore and processed in Singapore.

3.3 "**Personal Data**" refers to data, whether true or not, about an individual who can be identified from that data, or from that data in combination with other information to which the organisation may have access. This includes data that would identify a person (e.g. name, residential address, personal email address, home telephone or employee number, etc), opinions and facts about individuals, and information about employees or clients. It is not confined to a person's personal (i.e. non-work) life: Mobile telephone numbers and personal details (e.g. IC number) may also be personal data. The fact that information is publicly available may prevent personal data protection laws from applying to it, but care must be taken to ensure the data is clearly publicly available. When in doubt, it is better to assume that the data is personal data.

3.4 "**Processing**" also has a broad meaning: for example, collecting, using, recording, holding, organisation, adaptation or alteration, retrieval, combination, transmission, erasure, obtaining, copying, amending, adding, deleting, extracting, storing, disclosing, transferring or destruction of personal data.

3.5 The PDPA requires that ATMDBB complies with the following obligations:

- **The Consent Obligation** (PDPA sections 13 to 17)

An organisation must obtain the consent of the individual before collecting, using or disclosing his personal data for a purpose.

Consent from minors

Consent may be granted by minors who are at least 13 years of age. However, ATMDBB should obtain consent from a minor's parent or legal guardian to provide consent on the minor's behalf where a minor is below the age of 18.

- **The Purpose Limitation Obligation** (PDPA section 18)

An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, where the individual concerned has been notified of the intended purposes.

- **The Notification Obligation** (PDPA section 20)

An organisation must notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before such collection, use or disclosure of the personal data.

- **The Access and Correction Obligation** (PDPA sections 21 and 22)

An organisation must, upon request:

- i. provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and
- ii. correct an error or omission in an individual's personal data that is in the possession or under the control of the organization.

- **The Accuracy Obligation** (PDPA section 23)

An organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data is likely to be –

- i. used by the organisation to make a decision that affects the individual concerned; or
- ii. disclosed by the organisation to another organisation.

- **The Protection Obligation** (PDPA section 24)

An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

- **The Retention Limitation Obligation** (PDPA section 25)

An organisation 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:

- i. the purpose for which the personal data was collected is no longer being served by retention of the personal data; and

ii. retention is no longer necessary for legal or business purposes.

- **The Transfer Limitation Obligation** (refer to PDPA section 26)

An organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA.

- **The Openness Obligation** (refer to PDPA sections 11 and 12)

An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available. Section 4 sets out the steps which ATMDBB has adopted and that staff **must follow** to ensure that these obligations are met.

4. PERSONAL DATA PROTECTION SAFEGUARDS

4.1 Process personal data with consent and notification for relevant purposes

- 4.1.1 In general ATMDBB only processes personal data where it has obtained consent, notified the individual of the relevant purpose of the processing and where such purpose is appropriate for a business or legal purpose, unless exempted by law.
- 4.1.2 For example, staff may process personal data (1) where this is for ATMDBB's business purposes (including verifying the identity of a client) and (2) where the individual has provided consent.
- 4.1.3 In some situations, ATMDBB may also process personal data without consent when permitted by law, such as for managing or terminating an employment relationship.
- 4.1.4 In other situations, staff should seek guidance from the DPO if they wish to collect, use or disclose personal data and are unsure if they are able to do so.
- 4.1.5 Where ATMDBB holds personal data for certain specific purposes, staff must be careful not to use the data in any other way which is incompatible with those purposes. If the relevant individuals would not expect this use of the data, it is likely to be 'inappropriate use'.
- 4.1.6 For example, staff may not access an individual's personal data records for their own purposes, or for friends or family. This is a breach of their employment obligations.
- 4.1.7 Disclosure of personal data should not be made unless such disclosure is legally acceptable and appropriate. If requested by a Government agency to disclose personal data, ATMDBB staff ensure that such disclosure can be made and if in doubt, should consult with the DPO prior to disclosure.
- 4.1.8 Use or disclosure of personal data for a new purpose may not be covered by the relevant notice and consent. Staff must therefore obtain consent from the individual or otherwise consult the DPO first, if they wish to use or disclose personal data for a new purpose.

4.2 Sensitive personal data

- 4.2.1 Sensitive personal data includes information about an individual's physical or mental health or condition, racial or ethnic origin, financial data, the commission or alleged commission of any criminal offence, criminal convictions, political opinions, trade union membership, religious or philosophical beliefs and sexual life.

- 4.2.2 Although the PDPA does not recognize or have special obligations in relation to sensitive personal data, ATMDBB staff should recognize that the handling of sensitive personal data requires special care, as the unauthorised disclosure or leakage of sensitive personal data is potentially damaging to ATMDBB.

4.3 Openness

- 4.3.1 ATMDBB is transparent about how it uses personal data: if the ATMDBB collects personal data about individuals, it must tell them how this information will be used. This means, for example, providing information about:
- the purposes for which ATMDBB processes personal data;
 - the general types of other companies or business to whom ATMDBB will disclose the personal data, and the purposes for which they will be disclosed;
 - the rights that individuals have to access and correct their personal data; and
 - whether personal data is transferred outside Singapore.
- 4.3.2 In general, notice must be provided to individuals before ATMDBB collects personal data from them.
- 4.3.3 It is not necessary to provide information on uses for business contact information provided by individuals, where it is evident from the context how the information will be used.

4.4 Accuracy and Retention

- 4.4.1 Staff should collect only personal data that is adequate, relevant and not excessive. Personal data may only be collected if there is a business need for the information and if the level of information so collected is proportionate to this.
- 4.4.2 Staff should use personal data that is accurate and, as far as possible, up to date. Staff should advise ATMDBB's Human Resources department promptly if their details change.
- 4.4.3 While client contact information will often be in the form of business contact information, this may not always be the case. If staff are told about a change in a client's personal data, they should change any local contact databases that they maintain and ensure central databases are updated accordingly.
- 4.4.4 ATMDBB must not retain personal data for longer than is necessary for the purposes for which the data was collected. Staff should comply with ATMDBB's records and document retention policies.

4.5 Security and Confidentiality

- 4.5.1 ATMDBB implements appropriate administrative, technical, organisational and physical measures to protect personal data. This requires appropriate IT and physical security and staff training and care in selection of third parties who process personal data on behalf of ATMDBB. Staff must comply with policies implementing these measures.
- 4.5.2 ATMDBB may, from time to time, use shared services and third party providers to process personal data, but has implemented policies and procedures to protect the personal data as required under the PDPA. Before Personal Data is disclosed to shared services and third party providers, ATMDBB staff should check whether there are contracts or other legally binding documents in place to ensure that the shared

services or third parties will comply with the PDPA. If in doubt, please approach the DPO.

- 4.5.3 Any suspected or actual breach, unauthorised disclosure of, damage to or loss of any personal data (including loss of or damage to equipment containing personal data or hard copies of personal data) should be promptly reported in accordance with the relevant IT Security policies as well as to the DPO.
- 4.5.4 Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the individual and the legitimacy of any request for personal data. Unless essential, avoid releasing Personal Data over the telephone. If in doubt, please contact the DPO.

4.6 Restriction on transfers of Personal Data out of Singapore

- 4.6.1 A "**transfer**" under the PDPA refers to the transfer of Personal Data outside of Singapore, whether the Personal Data is transferred electronically (e.g. cloud storage, email, etc) or physically (e.g. shipping physical files).
- 4.6.2 The PDPA restricts transfers of personal data to other countries unless prescribed steps are taken to ensure that the personal data is protected. ATMDBB may, from time to time, use various shared services, outsourcing vendors and agencies outside Singapore to process personal data for administrative, business and legal purposes, or share employee personal data with other Bird & Bird offices around the world. ATMDBB may transfer Personal Data outside Singapore to these companies and to Bird & Bird offices in other countries for various business and legal purposes.
- 4.6.3 ATMDBB has put in place agreements to regulate the transfers of data to third parties outside of Singapore under binding legal agreements.
- 4.6.4 Staff must seek the clearance of a DPO or the Legal department if they wish to transfer personal data to a new supplier or vendor outside Singapore, to ensure that a data transfer agreement is already in place.

4.7 Rights of Individuals

- 4.7.1 ATMDBB will honour individuals rights under personal data protection laws:
 - to access and correct information relating to them;
 - to prevent direct telemarketing to them; or
 - to withdraw consent to processing of their personal data.
- 4.7.2 Any requests by staff for access to Personal Data should be made to the HR department or to the DPO.
- 4.7.3 Access and correction requests may be submitted through standard forms available from the DPO. However, ATMDBB must accept all requests made in writing and sent to the business contact information of its DPO, or left at or sent (by pre-paid post) to its Singapore office.
- 4.7.4 If ATMDBB staff receive any requests from individuals in relation to their Personal Data, such as access, correction or withdrawal of consent requests, such requests should be forwarded immediately to the DPO. ATMDBB should respond to access and correction requests within 30 days. If ATMDBB is unable to respond within 30 days, it must within that time inform the applicant in writing of the time by which it will respond to the request. It would also be good practice to specify the reasons why ATMDBB is unable to respond within 30 days of the request. If ATMDBB wishes to impose an administrative fee for access requests, it should also set out the fee amount, payment methods and other related details.

5. ATMDBB EXCEPTIONS:

Any request to deviate from this policy must be approved by the DPO.

6. VIOLATIONS:

Failure to comply with this policy is a disciplinary offence and will be handled in accordance with ATMDBB's disciplinary procedures.

7. QUERIES OR COMPLAINTS

If you have any queries or complaints in relation to this policy or data protection generally, you should contact ATMDBB's DPO at dposingapore@twobirds.com. The DPO or a person to whom he or she has delegated certain responsibilities, will respond to your query or complaint, investigate the complaint or request additional information in order to do so.

8. APPROVAL AND VARIATION

This policy has been approved by ATMDBB's HR department. This policy may be updated from time to time. Please ensure that you refer to the latest version of the policy made available to all staff.

9. GLOSSARY

"Personal Data" refers to data, whether true or not, about an individual who can be identified from that data, or from that data in combination with other information to which the organisation may have access;

"Processing" includes recording, holding, organisation, adaptation or alteration, retrieval, combination, transmission, erasure, obtaining, copying, amending, adding, deleting, extracting, storing, disclosing, transferring or destruction of personal data;

"Sensitive personal data" includes information about an individual's physical or mental health or condition, racial or ethnic origin, financial data, the commission or alleged commission of any criminal offence, criminal convictions, political opinions, trade union membership, religious or philosophical beliefs and sexual life;

"Transfer" under the PDPA refers to the transfer of Personal Data outside of Singapore, whether the Personal Data is transferred electronically (e.g. cloud storage, email, etc) or physically (e.g. shipping physical files).