

**Personal Information Collection Statement - Employees**

In compliance with the Personal Data Protection Act 2012 of Singapore (the "Act"), the Bank of East Asia, Limited, Singapore Branch ("the Bank") would like to inform you of the following:

- (1) It is necessary for prospective employees (job applicants) and employees of the Bank to supply the Bank with data about themselves for purpose in connection with their job application or employment.
- (2) The Bank may collect health data<sup>1</sup> of the employees and prospective employees (job applicants) for managing health and safety at work.
- (3) Failure to supply accurate and updated data about themselves and as stated in their declarations to the Bank will result in the Bank being unable to process employment or benefit applications or to develop and maintain the employment relationship (as the case may be).
- (4) During the recruitment process or after onboarding, various types of data may also be collected about prospective employees or employees up to leaving employment with the Bank. For example, the Bank may collect personal data of the employees in the course of their communications with customers of the Bank or any other third parties (as the case may be) by means of telephone recording system, internet access and email or other communications logging systems or platform and/or other available means wherever applicable.
- (5) The purposes for which data relating to employees (including former employees) and prospective employees (job applicants) may be used are as follows:
  - (i) processing employment applications;
  - (ii) determining and reviewing salaries, bonuses and other benefits;
  - (iii) conducting fit and proper assessment and performance assessment according to internal policy or regulatory requirements or consideration for promotion, training, secondment or transfer;
  - (iv) determining any disciplinary or rectifying action arising from employees' conduct or employees' ability to perform their job requirements;
  - (v) consideration of eligibility for and administration of staff loans, medical and other benefits and entitlements, and staff recreation and volunteer activities;
  - (vi) providing employee references;
  - (vii) registering employees as intermediaries or licensees with statutory authorities/ institutions for purposes directly related and/or associated to the employment;
  - (viii) monitoring compliance with regulatory requirements and internal governance, policies, procedures, guidelines or rules of the Bank;
  - (ix) meeting the requirements to make disclosure under the requirements/ obligations/ arrangements of any law binding on the Bank or under and for the purposes of any guidelines issued by regulatory or other authorities with which the Bank are expected to comply;
  - (x) detecting or conducting investigation regarding any cybersecurity matters, suspicious fraud cases, misconduct (e.g. fake sick leave) or criminal related activities;
  - (xi) public health protection, prevention of disease or control of pandemic;
  - (xii) assessing the suitability of the employee's continuance in employment; and
  - (xiii) for human resource management or purposes relating thereto.
- (6) Data held by the Bank relating to employees (including former employees) and prospective employees (job applicants) will be kept confidential but the Bank may provide such information to the following parties for the purposes set out in paragraph (5):
  - (i) any insurer, medical practitioner providing medical cover for the employees and their dependents (where applicable);
  - (ii) any administrator or manager of the Bank's retirement schemes or any relevant provident fund managers;
  - (iii) any agent, contractor, or third-party service provider (including data processors, cloud service providers or providers of Artificial Intelligence solution) or Bank's group companies) who provides administrative, telecommunications, computer, pre-employment screening, background checks or other services to the Bank in connection with the operation of its business;
  - (iv) any other person under a duty of confidentiality to the Bank including a group company of the Bank which has undertaken to keep such information confidential;
  - (v) any person to whom the Bank is under an obligation or otherwise required to make disclosure under the requirements of any law binding on or applying to the Bank or any disclosure under and for the purposes of any guidelines or guidance given or issued by any legal, regulatory, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations of financial services providers with which the Bank is expected to comply, all of which may be existing currently and in the future;
  - (vi) persons or companies seeking employee references in respect of employees with the prescribed consent of the employee concerned;

- (vii) any actual or proposed purchaser of all or part of the business of the Bank or, in the case of any merger, acquisition or other public offering, the purchaser or subscriber for shares in the Bank; and
  - (viii) third parties in the form of directories of names and office telephone numbers of key officers of the Bank for promotional and administrative purposes.
- (7) Insofar as employees or prospective employees (job applicants) are also customers of the Bank, attention is drawn to the Bank's Personal Information Collection Statement as appropriate.
- (8) Under and in accordance with the terms of the Act, any individual has the right:
- (i) to check whether the Bank holds data about him/her and/or have access to such data;
  - (ii) to require the Bank to correct any data relating to him/her which is inaccurate; and
  - (iii) to ascertain the Bank's policies and practices in relation to data and to be informed of the kind of personal data held by the Bank.
- (9) In accordance with the terms of the Act, the Bank has the right to charge a reasonable fee for the processing of any data access request.
- (10) The person to whom requests from employees and prospective employees (job applicants) for access to personal data or correction of personal data or for information regarding the Bank's privacy policies and practices and kinds of personal data held are to be addressed is as follows:

Head, Human Resources & Administration	Tel: 6602 7992
The Bank of East Asia, Limited	Fax: 6324 9464
60 Robinson Road, BEA Building	
Singapore 068892	

The Bank generally relies on personal data provided by you (or your authorised representative). In order to ensure that your personal data is current, complete and accurate, please update the Bank if there are changes to your personal data by informing the Bank in writing.

#### **Personal Data Protection**

- (11) In accordance with the provisions in the Personal Data Protection Act 2012 of Singapore (the "Act"), you shall undertake that customer information, sensitive information and personal data<sup>2</sup> encountered during the course of work shall not in any way be disclosed to any other person except as expressly provided in the Act. You shall also undertake to comply with (i) the Do Not Call (DNC) registry provisions under Part 9 of the Act; and (ii) the provisions regarding prohibition on use of dictionary attacks and address-harvesting software under Part 9A of the Act.

In addition, I understand that Part 9B of the Act sets out offences that hold individuals accountable for egregious mishandling of personal data, including offences for knowing or reckless unauthorised (a) disclosure of personal data; (b) use of personal data for a wrongful gain or a wrongful loss to any person; and (c) re-identification of anonymised data. Pursuant to sections 48D, 48E and 48F of the Act, if an individual is guilty of an offence under Part 9B of the Act, the individual shall be liable on conviction to a fine not exceeding \$5,000 or to imprisonment for a term not exceeding 2 years or to both.

- (12) Pursuant to Section 48J(4) of the Act, for non-compliance with the Do Not Call (DNC) registry provisions under Part 9 of the Act, the PDPC may impose a financial penalty of up to \$200,000 in the case of an individual. Pursuant to Section 48J(4A) of the Act, for non-compliance with the provisions regarding prohibition on use of dictionary attacks and address-harvesting software under Part 9A of the Act, the PDPC may impose a financial penalty of up to \$200,000 in the case of an individual.
- (13) Pursuant to Sections 55 and 56, I understand that any person shall be subjected to a composition fine of any offence under Personal Data Protection Act (except Part 9 - DO NOT CALL REGISTRY) if a person is reasonably suspected of having committed the offence for a sum not exceeding the lower of the following sums:
- (i) one half of the amount of the maximum fine that is prescribed for the offence;
  - (ii) a sum of \$5,000.

AND a composition fine of any offence under Personal Data Protection Act under Part 9 - DO NOT CALL REGISTRY if a person is reasonably suspected of having committed the offence; a sum not exceeding \$1,000.

On payment of such sum of money, no further proceedings shall be taken against that person in respect of the offence.

Any person guilty of an offence under the Personal Data Protection Act for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a continuing offence, to a further fine not exceeding \$1,000 for every day or part thereof during which the offence continues after conviction shall apply.

(14) Nothing in this statement shall limit the rights of employees and prospective employees (job applicants) under the Act referred to herein above.

---

<sup>1</sup> "Health data" means data or information which reveals an individual's health status in relation to infectious disease may be collected by the Bank for deploying epidemic prevention and control measures in the workplace.

<sup>2</sup> "Personal data" means data, whether true or not, about an individual who can be identified —

a) from that data; or

b) from that data and other information to which the organisation has or is likely to have access.