Mega International Commercial Bank Co. Ltd
Australia Branch

Privacy Policy

Approved By	AMC	SOOA	Approve No
Date of approval (V 1.0)	28 July 2011	29 August 2011	01714
Date of approval (V 1.1)	24 July 2012	22 August 2012	01772
Date of approval (V 1.2)	13 June 2013	30 July 2013	01695
Date of approval (V 1.3)	19 June 2014	7 August 2014	01620
Date of approval (V 1.4)	21 May 2015	3 August 2015	01162
Date of approval (2016.1)	16 August 2016	11 October 2016	00041

Version 2016.1

Policy Owner The Head of Risk and Compliance

Approved Australian Management Committee (AMC)

Senior Officer Outside Australia (SOOA)

Contents

Introduction

The Privacy Amendment (Private Sector) Act 2000 (Act) commenced on 21 December 2001 and extended the Privacy Act 1988 to the private section by introducing 10 National Privacy Principles (NPPs). The Privacy Act 1988 was further amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (the Reform Act). The Reform Act included a set of 13 new, harmonised, privacy principles for both the private and public sector, called the Australian Privacy Principles (APPs). The 13 APPs replaced the NPPs from 12 March 2014.

The APPs (The Principles) represent the minimum standards of privacy protection policy that must be adopted and regulate the collection, security, storage, use and disclosure of personal information for organisations.

Applicability

The Principles apply to "organisations". Mega International Commercial Bank Co., Ltd. Australia Branch（ hereinafter "the Branch"） holds an Australian Services Licence and therefore is identified as an "organisation" for the purposes of the Principles.

Personal and Sensitive Information

The Act protects personal information. This is information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information. Personal information includes names, age, gender, contact details and financial information. It also includes credit card details, information on credit history, credit reports from credit reporting agencies, information gathered on websites and mobile telephone numbers linked to user names and mailing lists.

There is extra protection for sensitive information. Sensitive information includes information about a person's racial or ethnic origin, political or religious belief, philosophical beliefs, membership of professional or trade associations or unions, sexual practices and criminal record. It also includes health and genetic information.

The Principles and Policy Codes

The Branch is bound either by the Principles or a registered policy code. The Principles set out the minimum standards required for the handling of personal information by organisations. They set the baseline standards for privacy protection. The Branch complies with the Principles. The Branch may at its absolute discretion adopt any other approved Privacy Policy in the future.

The Thirteen Australian Privacy Principles

The APPs mainly apply to personal information collected on or after 21 December 2001. However organisations such as the Branch will have some obligations under the APPs with respect to the:

- Accuracy and completeness;
- Security and disposal;
- Policies for management;
- Access and correction; and
- Transborder movement;

of personal information they hold after 21 December 2001, even if the information was collected before the commencement of the Act.

The following are guidelines to the APPs that are to be followed and adhered to by the Branch.

APP1 – Open and transparent management of personal information

The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

The Branch is required to have a clearly expressed and up to date policy about the management of personal information which contains the following information:

- The kinds of personal information that the Branch collects and hold and how the Branch does this;
- The purposes for which the Branch collects, holds, uses and discloses personal information;
- How an individual may access personal information about the individual held by the Branch and seek the correction of such information;
- How an individual may complain about a breach of the APPs and how the Branch will deal with that complaint; and
- Whether the Branch is likely to disclose personal information to overseas recipients and those countries where the recipients are located (where practical to specify).

The Branch's expressed policies on the management of personal information are set out in Appendix **A – Privacy and Spam Statement.** The Statement is made available to all prospective customers and to anyone who requests it free of charge and in the form that the individual or body requests it.

If requested, the Branch must take reasonable steps to let a person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses, and discloses that information.

APP2 – Anonymity and pseudonymity

Individuals must have the option of not identifying themselves or of using a pseudonym, when dealing with the Branch in relation to a particular matter.

This does not apply where the Branch is required or authorised by or under an Australian law (for example the AML/CTF Act), or a court/tribunal order, to deal with individuals who have identified themselves or where it is impracticable for the Branch to do so.

APP3 – Collection of solicited personal information

The Branch cannot collect personal information from an individual unless that information is reasonably necessary for one of the Branch's functions or activities. It is not acceptable for the Branch to collect information simply because the Branch would like to have, or might need to have, that information at some time in the future.

Information must be collected by lawful and fair means and not in an unreasonably intrusive way. If reasonable and practicable to do so, the Branch should always endeavour to collect personal information directly from the person concerned.

The Branch must not collect sensitive information about an individual unless:

- The individual has consented and the information is reasonably necessary for one or more of the Branch's functions or activities; or
- The collection is required or authorised by or under an Australian law or a court/tribunal order; or

- The Branch reasonably believes that collection is necessary to lessen or prevent a serious threat to the life, health or safety of an individual and it is unreasonable or impracticable to obtain the individual's consent to the collection; or
- The Branch has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the Branch's functions or activities has been, is being or may be engaged in, and the Branch reasonably believes that the collection is necessary for it to take appropriate action in relation to the matter; or
- The Branch reasonably believes that the collection is reasonably necessary to assist the location of a person who has been reported as missing.

Most personal information will be collected from the Application Form provided to a customer. A statement as to the information collection and its purpose is included on each Application Form. A Privacy and Spam Statement (see Appendix A) is also included with the Application Form and provided to all prospective customers in order to provide information in relation to the Branch's Privacy Policies. The Privacy and Spam Statement is required to be signed by the customer and returned to the Branch.

APP4 – Dealing with unsolicited personal information

Unsolicited personal information (personal information the Branch receives but did not request) must be given the same protection by the Branch as solicited personal information.

Where the Branch receives unsolicited personal information:

- The Branch must determine whether it could have collected it under APP3
- If the information could have been collected, then APPs 5 to 13 will apply to the information
- If the Branch decides it couldn't have collected the information, then the Branch must destroy or de-identify the information as soon as practicable, but only if lawful and reasonable to do so, and only if the information is not contained in a commonwealth record.

APP5 – Notification of the collection of personal information

The Branch must take reasonable steps to ensure that individuals are aware of the following at or before the time of collecting the personal information:

- The Branch's identity and contact details;
- If collection is required or authorised under the law, then fact and details of requirement;
- The purpose of collection;
- Consequences of non-collection;
- The organisations to which the personal information of that kind is usually disclosed;
- The person's right to access the information after it has been collected and seek correction if necessary ;
- How the person may complain about a breach of the APPs and how the Branch will deal with such a complaint; and
- Whether the Branch is likely to disclose the information to overseas recipients and if so the countries in which the recipients are likely to be located.

If the Branch collects the personal information from someone other than the individual, then the Branch needs to take reasonable steps to ensure the individual is aware that the Branch has collected the information and the circumstances of the collection.

The Branch's Privacy and Spam Statement (Appendix A) contains all the above required information and should be provided to all prospective customers. The Privacy and Spam Statement is required to be signed by the customer and returned to the Branch.

APP6 –Use or disclosure of personal information

The Branch must not use or disclose personal information about a person for a purpose other than the primary purpose of collection unless:

- The secondary purpose is related to the primary purpose of collection and the individual would reasonably expect the Branch to use or disclose the information in that way; or
- The individual has consented to the use or disclosure; or
- The use or disclosure is authorised under Australian law or a court/tribunal order; or
- It is necessary to lessen or prevent a serious threat to the life, health or safety of an individual and it is unreasonable or impracticable to obtain the individual's consent to the collection; or
- It is necessary for the Branch to take action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to the Branch's functions or activities; or
- The Branch reasonably believes it is necessary to assist the location of a person who has been reported as missing; or
- The Branch reasonably believes it is necessary for enforcement related activities conducted by an enforcement body.

For the Branch, the sole use of the information is for further communications to customers, and for advising them of the availability of future products. The Branch's Privacy and Spam Statement (Appendix A) provides information to customers regarding disclosure of their personal information and is required to be signed by the customer and returned to the Branch.

APP7 –Direct Marketing

The Branch may only use or disclose personal information it has collected from an individual (other than sensitive information) for direct marketing purposes if the individual would reasonably expect that their personal information would be used or disclosed for direct marketing. In addition, the Branch needs to have provided a simple means by which the individual can request not to receive direct marketing and not have received such a request.

Where an individual would not reasonably expect their personal information (other than sensitive information) to be used for direct marketing, or the information has been collected from a third party, the Branch may only use or disclose the personal information for direct marketing if:

- The individual has consented to the use or disclosure for this purpose, or it is impracticable to seek this consent; and
- The Branch has provided a simple means by which the individual can opt out of direct marketing and the individual has not opted out; and
- In each direct marketing communication the Branch must include a prominent statement telling the individual that he or she may request to no longer receive direct marketing, and no request is made.

The Branch is required to obtain the consent of the individual before using or disclosing sensitive information for the purpose of direct marketing.

Individuals have the right to contact the Branch to request the following and the Branch needs to comply with the requests in a reasonable time and free of charge:

- Request not to receive direct marketing communications from the Branch;

- Request that the Branch does not disclose their personal information to other organisations for the purpose of direct marketing; or
- Request that the Branch provides the source for the individual's personal information (the Branch does not need to comply with this if it is unreasonable or impracticable).

The Branch's Privacy and Spam Statement (Appendix A) is required to be signed by the customer and states that:

- The Branch may disclose personal information of a customer to other organisations and their agents for the marketing of their products and services, unless a customer requests that the Branch does not do so; and
- A customer may, at any time, ask the Branch not to mail, telephone or send them information about products and services and not to disclose their personal information to other organisations for that purpose. A customer may do this by contacting one of the Branch's offices.

APP8 –Cross-border disclosure of personal information

If the Branch discloses personal information about an individual to an overseas recipient (i.e. a person not in Australia or an external territory) who is not the same entity as the Branch, then under APP 8.1 the Branch has to ensure that the overseas recipient doesn't breach the APPs.

The Branch may then only transfer personal information about an individual to a person in a foreign country if:

- The Branch reasonably believes that the recipient of the information is subject to a law or binding scheme in a way that, overall, is at least substantially similar to the way the APPs protect the information; and there are mechanisms available to the individual to enforce that protection or scheme; or
- The individual consents to cross-border disclosure, after the Branch informs them that APP 8.1 will no longer apply if they give their consent; or
- Where the cross border disclosure is required or authorised by or under an Australian law, or a court order; or
- Where the Branch reasonably believes the disclosure to be necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety; or
- Where the Branch reasonably believes that the disclosure is necessary to take action in relation to the suspicion of unlawful activity or misconduct of a serious nature that relates to its functions or activities; or
- Where the Branch reasonably believes that the disclosure is necessary to assist any APP entity, body or person to locate a person who has been reported as missing.

The Branch's Privacy and Spam Statement (Appendix A) is required to be signed by customers and states that:

- The Branch operates throughout Australia and overseas and that as a result, the customer agrees that some of the uses and disclosures of their personal information may occur overseas; and
- The customer agrees that the Branch may make such disclosures even if the disclosure is to an organisation overseas which is not subject to the privacy obligations which are equivalent to those which apply to the Branch.

APP9 –Adoption, use or disclosure of government related identifiers

An identifier is a number, letter or symbol (or combination) assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. An individual's name is not an identifier.

The Branch is prohibited from adopting as its own identifier of an individual a government related identifier, such as Tax File Numbers (TFNS),medicare and pension numbers, unless the adoption is required under the law.

Further, the Branch cannot use or disclose a government related identifier of an individual unless the use or disclosure is reasonably necessary for the Branch to verify the identity of the individual for the purposes of its activities or functions.

There are further exceptions which include where the use or disclosure is required or authorised by a court/tribunal order; or is reasonably necessary to fulfil the Branch's obligations to an agency or State/Territory Authority or for an enforcement related activity.

The Branch monitors compliance with this obligation on at least a quarterly basis and reports any findings to the Risk and Compliance Committee (RCC).

APP10 –Quality of personal information

The Branch must take reasonable steps to make sure that the personal information it collects is accurate, up-to-date and complete. If the Branch uses or discloses the personal information, the Branch must additionally ensure that the personal information is relevant to the purpose of the disclosure.

APP11– Security of personal information

The Branch must take reasonable steps to protect the personal information it holds from misuse, interference and loss and also from unauthorised access, modification or disclosure.

The Branch must also destroy or de-identify the information if it is no longer needed (unless it is required under an Australian law, or a court/tribunal order to retain the information).

The Branch monitors compliance with this obligation on at least a quarterly basis and reports any findings to the RCC.

APP12– Access to personal information

The Branch must provide individuals with access to and a copy of their personal information on request and within a reasonable period. This includes information collected from third parties, information received unsolicited and subsequently kept in records held, and opinions recorded about an individual.

The Branch may choose to charge for access to personal information. Those charges must not be excessive and must not apply to lodging a request for access.

The Branch does not have to give an individual access in a number of circumstances, which include:

- Giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
- Giving access would have an unreasonable impact on the privacy of other individuals; or

- The information relates to existing or anticipated legal proceedings between the Branch and the individual; or
- Giving access would reveal the Branch's intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- Giving access would be unlawful; or
- The Branch has reason to suspect that unlawful activity, or misconduct of a serious nature that relates to its functions or activities has been, is being or may be engaged in; and giving access would be likely to prejudice the taking of appropriate action; or
- Giving access would be likely to prejudice enforcement related activities; or
- Giving access would reveal evaluative information generated within the Branch in connection with a commercially sensitive decision making process.

If the Branch refuses access on any of the above grounds, or refuses to give access in the manner requested, then it has to give the individual a written notice setting out the reasons for the refusal and how to complain about the refusal.

The Branch's Privacy and Spam Statement (Appendix A) notifies customers of their right of access to their personal information.

APP13 – Correction of personal information

If the Branch is satisfied that the personal information it holds for an individual is inaccurate, out-of-date, incomplete or irrelevant or misleading; or if the individual requests a correction, then the Branch needs to correct that personal information within a reasonable period of time. The Branch cannot charge the individual for making the correction.

If the Branch has disclosed the personal information to someone else, then the Branch needs to notify them of the correction if the individual requests.

If the Branch refuses to correct the personal information as requested by the individual, then it has to give the individual a written notice setting out the reasons for the refusal and how to complain about the refusal.

The Branch's Privacy and Spam Statement (Appendix A) notifies customers that the Branch will correct their personal information.

Appointment of Privacy Officer

Senior Officers outside Australia(SOOA) may at his/her absolute discretion appoint or employ any person to be the Privacy Officer of the Branch. The Privacy Officer would be the first point of contact in the Branch when privacy issues arise either internally or externally.

Until determined otherwise by SOOA, the Head of Risk and Compliance(HRC) is appointed as the Privacy Officer.

The Privacy Officer is responsible for:

- Developing and implementing a Privacy Policy that suits the Branch's business and complies with the law;
- Ensuring that the Branch's Privacy Policy and Procedures are fully implemented and working effectively; and
- Reporting to SOOA any breach of the Privacy Policy.

Complaints

An individual may make a complaint in writing by either asking to complete the Branch's complaint form detailing the problem or sending it a letter, email or facsimile. If they do not wish to make the complaint in writing, they may make the complaint in person, or the Branch will take down details of their complaint over the telephone.

The Branch will investigate, address and if necessary escalate the complaint as required under its Privacy Policy.

Policy Review

The Risk and Compliance Department will review this Policy annually and will update it, when required, between review dates to reflect legislative or regulatory changes.

This Policy is supported by further procedures and operational arrangements. If you have any questions regarding this Policy, then please contact the HRC.

The Policy will be communicated to all new members of staff by the Risk and Compliance Department during induction training sessions.

A breach of this Policy will be considered as professional misconduct and will be liable for disciplinary penalties. This could potentially include immediate dismissal and legal action. (Refer to the Branch's Risk Event and Breach Escalation Policy)

Appendix A. Privacy and Spam Statement

Privacy and Spam Statement 隱私同意書

This Statement explains how Mega International Commercial Bank Co., Ltd ("we/us/our") collects, uses and discloses Personal Information. For the purposes of this Privacy and Spam Statement, "Personal Information" is information which may be used to identify an individual, including name, age, gender, contact details and financial information such as credit history. By law, we are required to collect and store this information in accordance with prudent risk management, banking and anti-money laundering and counter terrorism financing legislation.

As well as dealing with our collection, use and disclosure of Personal Information, this Statement requests your consent to us sending you information about products and services, including by way of commercial electronic messages. Where you sign this Statement, you are providing your consent to the disclosures and contacts outlined in this Statement.

Purposes for which we collect and use Personal Information

(i) We may collect your Personal Information to allow us to assess and process your application for a product or facility, as well as to establish, provide and administer any product or facility we have agreed to provide to you.

(ii) We may also use your Personal Information to allow us to:

- comply with relevant state and federal legislative and regulatory requirements (such as customer identification);
- consider any other application you may make to us, including applications for commercial credit;
- perform our required business administration, including account keeping, risk management, record keeping, archiving, systems development and testing, credit scoring, fraud prevention and staff training;
- manage our rights and obligations in relation to external payment systems;
- conduct market or customer satisfaction research;
- develop, establish and administer alliances and other arrangements (including rewards programs) with other organisations in relation to the promotion, administration and use of our respective products and services;
- develop and identify products and services that may interest you; and
- tell you about products and services (unless you request that we not do so).

(iii) You agree that, in assessing an application for credit or in assessing whether to accept you as a guarantor to an application for credit, we may obtain a credit report about you or personal information about you in a credit report, from a credit reporting agency or organisation or a credit provider for the purpose of assessing whether to accept you as a borrower or guarantor.

(iv) If we do not collect Personal Information about you, we may not be able to provide you with our products or services.

(v) If you provide Personal Information to us about someone else, you agree that you will show them a copy of this Privacy and Spam Statement, to allow them to understand the manner in which their Personal Information may be used or disclosed by us in connection with your dealings with us.

Disclosure of Personal Information

(i) You agree and acknowledge that we may disclose Personal Information we have collected about you to:

- credit reporting agencies for the purpose of obtaining a credit report or to allow the credit reporting agency to create or maintain a credit information file containing information about you;
- any credit provider for any purpose you have agreed to;
- our agents, contractors, service providers and external advisers;
- your agents and contractors, including your finance broker, builder, settlement agent and your legal or financial adviser;
- your executor, administrator, trustee, guardian or attorney;
- your referees;
- regulatory bodies, government agencies, law enforcement bodies and courts;
- debt collection agencies;
- any person or organisation who introduces you to us;
- anyone supplying goods or services to you in connection with a rewards program associated with a loan or facility you have (or have applied for) with us;
- other financial institutions and our related companies;
- other organisations with whom we have alliances or arrangements (including rewards programs) for the purpose of promoting our respective products and services (and any agents used by us and our business partners in administering such an arrangement or alliance);
- your franchisor (if applicable);
- external payment systems operators;
- any mortgage insurer used by us and reinsurer of such mortgage insurer;
- our insurers or prospective insurers and their underwriters;
- an intending guarantor, to enable that person to consider whether or not to act as guarantor, or offer property as security, for a loan you have (or have applied for) with us;
- your co-borrowers, sureties, guarantors and co-guarantors and prospective co-borrowers, sureties, guarantors and co-guarantors;
- any person considering purchasing your loan, guarantee or security, that person's advisers, persons involved in assessing the risks and funding of the purchase and, after purchase, the purchaser and any manager on an ongoing basis;
- any person to the extent necessary, in our view, in order to carry out any instruction you give us; and
- other organisations (including our related bodies corporate) and their agents for the marketing of their products and services (unless you request that we not do so).

(ii) You agree that we may make such disclosures even if the disclosure is to an organisation overseas which is not subject to the privacy obligations which are equivalent to those which apply to us, and we will not remain liable for the information once it is disclosed overseas.

(iii) We operate throughout Australia and in a number of countries overseas. As a result, you agree that some of these uses and disclosures may occur interstate or outside Australia. Please contact us if you wish for a list of the countries in which we operate.

Gaining access to and correction of your Personal Information

You may seek to gain access to your Personal Information held by us at any time by contacting one of our branches. We may charge an administration fee to allow access to this information.

If we are satisfied that your personal information held by us is inaccurate, incomplete or out of date then we will correct this. If you wish to request us to correct your information, please inform us as soon as practicable so that this can be updated. You may be required to provide new forms of evidence to support any requested changes to your Personal Information.

We will only deny you access to or refuse a correction of your Personal Information where we have a reason to do so or where required by law. In these circumstances, we will provide you with reasons (where possible) for denying your request. This may be because the information that you have requested access to is commercially sensitive, or we are prohibited or permitted to do so by law.

Complaints

If a matter is not or cannot be resolved immediately to your satisfaction and to our satisfaction, you may make a complaint in writing by either asking to complete our complaint form detailing the problem or sending us a letter, email or facsimile. If you do not wish to make the complaint in writing, you may make the complaint in person at one of our branches, or we will take down details of your complaint over the telephone. We will investigate and address your complaint within 10 Business Days. If you are not satisfied with the outcome, we will escalate your complaint internally and will inform you of the result of the escalation of your complaint.

If you are not satisfied with the outcome of the above process you may contact the Financial Services Ombudsman by completing and sending FOS a Dispute Form (available at www.fos.org.au) or by calling the Financial Services Ombudsman at 1300 78 08 08.

Receiving commercial electronic messages

(i) You consent to us sending commercial electronic messages, including messages about our products and services and the products and services of any third party that we think may be of interest to you, to each electronic address which you have provided to us. You warrant that you have authority either as or on behalf of the relevant electronic account holder to provide this consent.

(ii) In respect of each electronic address, you agree that until you provide written notice to withdraw your consent in respect of that electronic address or use an unsubscribe facility included within a commercial electronic message sent to that electronic address (to withdraw your consent), we may continue to send commercial electronic messages to that electronic address.

(iii) You may, at any time, ask us not to mail, telephone or send you information about products and services and not to disclose your Personal Information to any other organisations for that purpose. You may do this by contacting one of our branches.

For more information about the way in which we collect and use your Personal Information, please contact Mega International Commercial Bank Co., Ltd.

X			
Name of 1st Applicant 第一申請人姓名		**Date 日期**	
X			
Name of 2nd Applicant 第二申請人姓名		**Date 日期**	