FORTIFIRE

DEFEND AGAINST DISASTER

Fortifire Pty Ltd
T/A
Fortifire

ABN: 44 152 787 034

Privacy Policy Manual

 © Copyright – EC Credit Control 1999-2020 #**40979**

Table of Contents

DISCLAIMER: Subject to any applicable law which cannot be excluded and to all provision implied by statute which cannot be excluded, EC Credit Control (Aust) Pty Ltd accepts no responsibility for any loss, damage, cost or expense (whether direct or implied) incurred by you as a result of any error, omission or misrepresentation in any information in this manual.

This manual has been prepared by EC Credit Control (Aust) Pty Ltd
www.eccreditcontrol.com.au | info@eccreditcontrol.com.au
Phone 1300 361 070

1. Introduction

From 12 March 2014, the Australian Privacy Principles (APP's) replaced the National Privacy Principles and Information Privacy Principles and were inserted into the Privacy Act 1988 ("the Act") at schedule 1. These principles apply to private sector organisations who deal with information relating to individuals. This legislation is designed to protect personal information about individuals and sets in place a framework and guidelines about how to deal with this information. APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP privacy policy describing how it manages personal information. Further in February 2018, the Notifiable Data Breaches ("NDB") Scheme was introduced under Part IIIC of the Act. The NDB establishes requirements and compliance mechanisms for entities in responding to data breaches.

As at 25 May 2018, the EU General Data Protection Regulation ("GDPR") was introduced providing increased transparency for data protection for all businesses transferring data to the Europe Union. While the GDPR and the APP share some similarities, Fortifire is providing robust privacy policies and procedures for its staff and clients. This includes ensuring that it conforms to all required APP's including the provision of a clearly expressed and readily available Privacy Policy. This is completed by the provision of this Privacy Policy Manual.

An APP privacy policy is a key tool for meeting APP 1's requirements.

To assist with this compliance, Fortifire ensures that all of its staff members adhere to these policies and procedures. Any breaches of these policies and procedures must be reported to the relevant staff member's manager or supervisor immediately so that any appropriate measures can be taken to mitigate any issues surrounding an identified breach.

Every staff member of Fortifire who handles personal information is required to have an understanding of the Australian Privacy Principles (APP's), the Act and the GDPR, where necessary. Where a more detailed knowledge of Fortifire's rights and responsibilities is required, the Privacy Officer will be able to provide assistance.

All staff are encouraged to discuss privacy issues with the nominated Privacy Officer.

 © Copyright – EC Credit Control 1999-2020 #**40979**

Review

Formal review of this privacy policy shall be undertaken on a 6 monthly basis with the details of this review recorded by the Privacy Officer.

2. Australian Privacy Principles (APP's)

The Privacy Act 1988 and the Credit Reporting Privacy Code 2014 places obligations and responsibilities on employers and employees to ensure that information collected from individuals is collected, retained and used in line with the APP's. Fortifire shall abide by the following APP's at all times:

APP No.

Part 1 – Consideration of personal information privacy

APP 1 Open and transparent management of personal information

APP 2 Anonymity and pseudonymity

Part 2 – Collection of personal information

APP 3 Collection of solicited personal information

APP 4 Dealing with unsolicited personal information

APP 5 Notification of the collection of personal information

Part 3 – Dealing with personal information

APP 6 Use or disclosure of personal information

APP 7 Direct marketing

APP 8 Cross-border disclosure of personal information

APP 9 Adoption, use or disclosure of government related identifiers

Part 4 – Integrity of personal information

APP 10 Quality of personal information

APP 11 Security of personal information

Part 5 – Access to, and correction of, personal information

APP 12 Access to personal information

APP 13 Correction of personal information

 © Copyright – EC Credit Control 1999-2020 #**40979**

Further information regarding the APP's can be obtained from the office of the Australian Information Commissioner at www.oaic.gov.au.

A copy of the APP's as produced by the Office of the Australian Information Commissioner is attached as Appendix A. The NDB forms part of the Act as a new implemented scheme for companies to advise its clients, in the event of a potential data breach that is likely to result in serious harm to any individuals whose personal information is involved in the breach. Fortifire's Privacy Policy Manual provides a data breach preparation and response to any potential breaches to ensure compliance under the NDB and the Act.

3. General Data Protection Regulation ("GDPR")

Upon the implementation of the GDPR on 25 May 2018, Fortifire has updated the way they use and collect personal data from residents in the EU. This involves, identifying Fortifire's data protection officer ("Privacy Officer"), how clients can contact the Privacy Officer and identifying the process of transferring client's personal information. Further, the implementation of cookies notices on Fortifire's website has been activated to ensure Fortifire's clients have adequate protection in providing consent to Fortifire in withholding their personal data.

4. Types of Personal Information That is Collected, Used, Processed & Held

Fortifire collects personal information for a variety of reasons. This personal information will be collected in the normal course of business and will relate to Goods and/or Services that are provided by Fortifire to clients. This information collected will be done so in the course of business where the client is a customer of Fortifire or when the client acts as a guarantor for another person or company that is a client of Fortifire. Fortifire will not collect information that is not relevant or sensitive in nature unless it is required in the normal course of business.

The personal information that is collected may include, but will not be limited to the following;

1/ Full name

2/ Address

3/ Date of birth

 © Copyright – EC Credit Control 1999-2020 #**40979**

4/ Credit references if applicable
5/ Publicly available information which relate to the clients activities in Australia
6/ Any information recorded in the National Personal Insolvency Index
7/ Driver's licence details
8/ Medical insurance details (if applicable)
9/ Electronic contact details including email, Facebook and Twitter details
10/ Next of kin and other contact information where applicable

The client acknowledges that provided the correct Privacy Act disclosures have been made that Fortifire may conduct a credit report on the client for the purposes of evaluating the credit worthiness of the client.

Fortifire ensures that all personal information is held in a secure manner. Where applicable and to the best of Fortifire's knowledge all computers or servers have the required security protections in place to safeguard and protect any personal information that is held by Fortifire.

We may use cookies on our website. Cookies are small files which are stored on your computer. They are designed to hold a modest amount of data (including personal information) specific to a particular client and website, and can be accessed either by the web server or the client's computer. In so far as those cookies are not strictly necessary for the provision of Fortifire's services, we will ask you to consent to our use of cookies when you first visit our website.

In the event that you utilise our website for the purpose of purchases/orders, Fortifire agrees to display reference to cookies and /or similar tracking technologies, such as pixels and web beacons (if applicable), and requests consent for Fortifire collecting your personal information which may include:

(a) IP address, browser, email client type and other similar details;
(b) Tracking website usage and traffic; and
(c) Reports are available to Fortifire when Fortifire sends an email to the client, so Fortifire may collect and review that information

If you consent to Fortifire's use of cookies on our website and later wish to withdraw your consent, you may manage and control Fortifire's privacy controls through your browser,

 © Copyright – EC Credit Control 1999-2020 #**40979**

including removing cookies by deleting them from your browser history when you leave the site.

Fortifire also regularly conducts internal risk management reviews to ensure that its infrastructure (to the best of its knowledge) is secure and any identifiable risks have been mitigated as much as they can be in the normal course of business.

5. Procedures and responding to potential breaches of Privacy

In accordance with the NDB Fortifire is aware of its responsibilities to notify its clients in the event of a potential data breach that may cause serious harm to clients. Further, in the event the client is located in the Europe Union ("EU"), Fortifire acknowledges that any potential data breaches will be safeguarded by the provisions of the GDPR.

Fortifire will collect and process personal information in the normal course of business. This personal information may be collected and processed, but is not limited to, any of the following methods;

1/ Credit applications forms
2/ Work authorisation forms, quote forms or any other business documentation
3/ Publicly available databases that hold information
4/ Websites that detail information such as Sensis, Facebook, Google etc
5/ By verbally asking you for information as part of normal business practices

Where relevant to data processing as per the GDPR, and in particular where Fortifire uses new technologies, and takes into account the nature, scope, context and purposes of processing and considers that the data processing is likely to result in a high risk to the rights and freedoms of natural persons, the Privacy Officer shall, prior to the processing of personal information, carry out an assessment of impact of the envisaged processing operations by way of a protection impact assessment. The data protection assessment will be required in instances whereby:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

 © Copyright – EC Credit Control 1999-2020 #**40979**

(b) processing on a large scale of special categories of data referred to in Article 9(1) of the GDPR, or of personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
(c) a systematic monitoring of a publicly accessible area on a large scale.

The assessment shall be carried out in accordance with Article 35 (7) of the GDPR and carry out reviews of such data protection impact assessments when there is any change of the risk associated with the processing of personal information.

As a client of Fortifire and agreeing to Fortifire's Terms and Conditions of Trade, which includes Fortifire's privacy statement you hereby agree and consent to the provisions of this Privacy Policy Manual, including but not limited to the collection, processing, use and disclosure of your personal information. In the event that you withdraw your agreement and consent to any of the above use, processing collection and disclosure, then Fortifire warrants that any request by you to withdraw your consent or agreement shall be deemed as confirmation by you to cease any and/or all collection use, processing and disclosure of your personal information. You may make a request to withdraw your consent at anytime by telephone and/or by email to the following contact details;

The Privacy Officer
Fortifire
Unit 1/9 Keane Street
CURRAJONG QLD 4812
admin@fortifire.com.au
(07) 4773 4004

Fortifire will ensure that any Information that is to be obtained from you is done so verbally or using Fortifire's prescribed forms which;

Authorise Fortifire:

1/ To collect personal information; and
2/ Inform the individual what personal information is being collected; and
3/ Inform the individual why (the purpose) the personal information is being collected; and
4/ Inform the individual why & when personal information will be disclosed to 3rd parties.

 © Copyright – EC Credit Control 1999-2020 #**40979**

It is the responsibility of Fortifire to ensure that any personal information obtained is as accurate and up to date as possible and information is only collected by lawful means in accordance with the Act and relevantly, in accordance with the GDPR.

6. Purposes For Which Information Is Collected, Held, Used and Disclosed

Disclosure to Third Parties

Fortifire will not pass on your personal information to third parties without first obtaining your consent.

In accordance with the Act, including the GDPR (where relevant), Personal Information can only be used by Fortifire for the following purposes:

1/ Access a credit reporter's database for the following purposes:
   a) To assess your application for a credit account; or
   b) To assess your ongoing credit facility; or
   c) To notify a credit reporter of a default by you (providing Fortifire are a member of an approved OAIC External Dispute Resolution Scheme ("EDRS") for consumer defaults); or
   d) To update your details listed on a credit reporter's database; or

2/ Check trade references noted on the prescribed form for the following purposes:
   a) To assess your application for a credit account; or
   b) To assess your ongoing credit facility; or
   c) To notify a default (subject to 1(c) above).

3/ Market Fortifire's products and services.

4/ Any other day to day business purposes such as complying with ATO requirements, managing accounting returns or legal matters.

Relationship with Credit Reporter - In the event that notification of a default has been reported to a Credit Reporter and your credit file has been updated (including any changes to the balance outstanding or contact details), then the Credit Reporter shall be notified as soon as practical of any such changes.

Fortifire will only gather information for its particular purpose (primary purpose). In accordance with the Act, including the GDPR (where relevant), Fortifire will not disclose this information for any other purpose unless this has been agreed to by both parties.

 © Copyright – EC Credit Control 1999-2020 #**40979**

7. How An Individual May Access Personal Information Held, And How They May Seek Correction of Such Information

You shall have the right to request from Fortifire a copy of all the information about you that is retained by Fortifire. You also have the right to request (by telephone and/or by email) that Fortifire correct any information that is incorrect, outdated or inaccurate.

Any requests to receive your personal information or to correct personal information should be directed to the following contact details;

The Privacy Officer
Fortifire
Unit 1/9 Keane Street
CURRAJONG QLD 4812
admin@fortifire.com.au
(07) 4773 4004

Fortifire will destroy personal information upon your request (by telephone and/or by email) or when the personal information is no longer required. The exception to this is if the personal information is required in order for Fortifire to fulfil their performance of services or is required to be maintained and/or stored in accordance with the law.

8. How An Individual May Complain About A Breach Of The APP, And How The Complaint Will Be Dealt With

You can make a complaint to Fortifire's internal dispute resolution team ('IDR') regarding an interference with and/or misuse of your personal information by contacting Fortifire via telephone or email.

Any complaints should be directed to the following contact details in the first instance;

The Privacy Officer
Fortifire
Unit 1/9 Keane Street
CURRAJONG QLD 4812
admin@fortifire.com.au
(07) 4773 4004

 © Copyright – EC Credit Control 1999-2020 #**40979**

In your communication you should detail to Fortifire the nature of your complaint and how you would like Fortifire to rectify your complaint.

We will respond to that complaint within 7 days of receipt and will take all reasonable steps to make a decision as to the complaint within 30 days of receipt of the complaint.

We will disclose information in relation to the complaint to any relevant credit provider and or Credit Reporting Body that holds the personal information the subject of the complaint.

In the event that you are not satisfied with the resolution provided, then you can make a complaint to the Information Commissioner on the OAIC website at www.oaic.gov.au

9. Will Personal Information Be Disclosed To Overseas Recipients?

Fortifire does not disclose information about the client to third party overseas recipients unless the client has provided its consent. Fortifire will notify you if circumstances change regarding overseas disclosure and will comply with the Act and the GDPR in all respects.

Unless otherwise agreed, Fortifire agrees not to disclose any personal information about the client for the purpose of direct marketing. You have the right to request (by telephone and/or by email) that Fortifire does not disclose any personal information about you for the purpose of direct marketing.

10. Availability Of This Privacy Policy Manual

This Privacy Policy manual is available to all clients of Fortifire. It will be made available (where applicable) on Fortifire's website. This manual will also be available upon request at Fortifire's business premises and is available to be sent to you if required. If you require a copy of this Privacy Policy please make a request utilising the following contact information in the first instance:

The Privacy Officer
Fortifire
Unit 1/9 Keane Street
CURRAJONG QLD 4812
admin@fortifire.com.au
(07) 4773 4004

 © Copyright – EC Credit Control 1999-2020 #**40979**

11. Privacy Officer (Responsibilities)

Fortifire has appointed an internal Privacy Officer to manage its privacy matters. The name of this officer is available by making contact with Fortifire. The privacy officers duties include (but are not limited to) the following:

The Privacy Officer needs to be familiar with the APP's. Educational material is available from the office of the Privacy Commissioner which explains what Fortifire needs to know in order to comply with the Privacy Act.

If a person complains to the Privacy Commissioner that Fortifire has breached their privacy, the Information Commissioner may contact the Privacy Officer to discuss the complaint, and to see whether there is any means of settling the matter. The Privacy Officer shall provide whatever assistance is necessary. The Privacy Officer may be asked to provide background information or identify the staff members who can do so.

Complaints

In the event that a complaint about privacy issues is received the Privacy Officer will:

1/ Take ownership of the complaint and ensure that it is dealt with in a timely manner.
2/ Acknowledge receipt of the complaint within 24 hours and advise the complainant of their rights.
3/ Fully investigate the complaint.
4/ Respond, with findings, to the complainant within 30 days of receipt.
5/ Keep a record of all complaints received for ongoing review of policies and procedures.

In the event that a complaint about privacy issues is received via a credit reporter the Privacy Officer will:

1/ Take ownership of the complaint and ensure that it is dealt with in a timely manner.
2/ Acknowledge receipt of the complaint to the credit reporter within 24 hours.
3/ Fully investigate the complaint.
4/ Respond, with findings, to the credit reporter within 7 days of receipt.
5/ Keep a record of all complaints received for ongoing review of policies and procedures.

 © Copyright – EC Credit Control 1999-2020 #**40979**

APPENDIX A - INFORMATION PRIVACY PRINCIPLES

Part 1 – Consideration of Personal Information Privacy

Australian Privacy Principle 1 – open and transparent management of personal information

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

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up to date policy (the *APP privacy policy*) about the management of personal information by the entity.

1.4 Without limiting sub-clause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

 © Copyright – EC Credit Control 1999-2020 #**40979**

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Australian Privacy Principle 2 – anonymity and pseudonymity

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

2.2 Sub-clause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/ tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Part 2 – Collection of Personal Information

Australian Privacy Principle 3 – collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) sub-clause 3.4 applies in relation to the information.

3.4 This sub-clause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

 © Copyright – EC Credit Control 1999-2020 #**40979**

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities. Note: For *permitted general situation*, see section 16A. For *permitted health situation*, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

Australian Privacy Principle 4 – dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under sub-clause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If sub-clause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

Australian Privacy Principle 5 – notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in sub-clause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of sub-clause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order— the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/ tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a

 © Copyright – EC Credit Control 1999-2020 #**40979**

registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Part 3 – Dealing with Personal Information

Australian Privacy Principle 6 – use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) sub-clause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This sub-clause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For *permitted general situation*, see section 16A. For *permitted health situation*, see section 16B.

6.3 This sub-clause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

 © Copyright – EC Credit Control 1999-2020 #**40979**

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with sub-clause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

Australian Privacy Principle 7 – direct marketing

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions – personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Exception – sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception – contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

Australian Privacy Principle 8 – cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Sub-clause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

 © Copyright – EC Credit Control 1999-2020 #**40979**

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, sub-clause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For *permitted general situation*, see section 16A.

Australian Privacy Principle 9 – adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) sub-clause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

 © Copyright – EC Credit Control 1999-2020 #**40979**

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) sub-clause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For *permitted general situation*, see section 16A.

Regulations about adoption, use or disclosure

9.3 This sub-clause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this sub-clause are prescribed, see subsections 100(2) and (3).

Part 4 – Integrity of Personal Information

Australian Privacy Principle 10 – quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up to date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

Australian Privacy Principle 11 – security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

 © Copyright – EC Credit Control 1999-2020 #**40979**

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Part 5 – Access To, And Correction Of, Personal Information

Australian Privacy Principle 12 – access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access – agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite sub-clause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access – organisation

12.3 If the APP entity is an organisation then, despite sub-clause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

 © Copyright – EC Credit Control 1999-2020 #**40979**

(g) denying access is required or authorised by or under an Australian law or a court/ tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of sub-clause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting sub-clause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of sub-clause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

Australian Privacy Principle 13 – correction of personal information

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

 © Copyright – EC Credit Control 1999-2020 #**40979**

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under sub-clause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

The information provided in this fact sheet is of a general nature. It is not a substitute for legal advice.

 © Copyright – EC Credit Control 1999-2020 #**40979**