MFAA Privacy Act Module

Last updated January 2014. Applies from 12 March 2014.

Contents

PART 1. Introduction

The *Privacy Act* (Cth) 1988 (**Privacy Act**) regulates the collection, use, and disclosure of *personal information* and *credit information.*

This document provides a brief summary of how the Privacy Act impacts finance brokers, servicers, managers, and lenders. It does not deal with provisions in detail or in a technical way. Specific advice should be obtained on specific issues.

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* commenced on 12 March 2014. The amendments significantly increased the obligations on organisations that collect *personal information* in Australia.

Broadly, the changes to the Privacy Act:

- introduced positive credit reporting;
- introduced the requirement for all *credit providers* including commercial *credit providers* to be members of an external dispute resolution scheme approved by the Office of the Privacy Commission (**OAIC**) before they obtain or disclose *credit information* from a *credit reporting body* (**CRB**);
- imposed obligations for businesses to maintain a compliance plan as well as privacy policies;
- amended the rules about disclosure of personal information to overseas entities; and
- increased fines and gives the OAIC the ability to initiate investigations.

Precedent Privacy Consents, Policies, and Compliance Plans are provided as annexures to this document. Documents in use prior to 12 March 2014 require revision.

What do brokers need to do?

1. Read the AAPs in full. They can be found here.

2. Institute systems to ensure compliance with the law, in particular the APPs.

3. Have a **Privacy Consent** – an example consent is at **Annexure 5**.

4. Have a **Privacy Policy**. The MFAA recommends that all members display their privacy policy on their website, (if they have a website). The Privacy Policy must be provided to customers on request. An example Privacy Policy for brokers can be accessed at **Annexure 8**.

5. If a broker's business is a material size, say more than five people, have a written **Compliance Plan** which specifies how the business will implement procedures and systems to comply with the APPs. An example Compliance Plan is at **Annexure 10**.

What do lenders, servicers, and managers need to do?

1. Read the Australian Privacy Principles (**AAPs**) in full. They can be found at here.

2. Institute systems to ensure compliance with the law, in particular the APPs.

3. Have a **Privacy Consent** – an example consent for lenders is at **Annexure 7**, and for servicers and managers at **Annexure 6**.

4. Have a **Privacy Policy**. The MFAA recommends that all members display their privacy policy on their website, (if they have a website). Privacy Policies must be provided to customers on request.

5. Have a written **Compliance Plan** which specifies how the business will implement procedures and systems to comply with the APPs.

6. Both consumer and commercial credit reports from *CRBs* can only be obtained by '*credit providers'* and their agents who are members of an EDR scheme accredited by the OAIC.

7. Decide whether to participate in positive credit reporting. Only lenders who provide repayment history information will be entitled to receive repayment history information from *CRBs*.

PART 2. Scheme of legislation

2.1 What does the Privacy Act regulate?

The Privacy Act was introduced in 1988 to prevent unwarranted collection, retention, and use of information about *individuals.* There are no restrictions in the Privacy Act on collecting, using, or disclosing information about companies. However, financial institutions and brokers are subject to the common law duty of confidentiality, and generally no information should be disclosed without consent.

The Privacy Act regulates the collection, use, and disclosure of *personal information* and *credit information* about individuals.

The key requirements about *personal information* are set out in the APPs The APPs are summarised at **Annexure 1**, and shown diagrammatically at **Annexure 2**. These summaries do not replace reading the AAPs in full, as they set out important rules, and there are significant penalties for breach.

The Privacy Act also regulates the use of *credit information* and the activities of *CRBs.* Entities that deal with *CRBs* are called '*credit providers'* – a term which has a wider meaning than when used in the National Credit Code. The credit reporting information flow is shown in **Annexure 3** and key provisions of the Privacy Act relating to credit information are summarised in **Annexure 4**. Brokers are not entitled to access *credit information* from *CRBs* on their own account, but they can obtain a credit report acting as agent for the individual that the report is about.

Readers who are new to the topic of privacy law are encouraged to read **Annexures 1 to 4** inclusive before reading the rest of this Module.

2.2 Credit Reporting Code

The Privacy Act operates in tandem with the Credit Reporting Code which regulates the exchange of information between *credit providers* and *CRBs.*

2.3 Some definitions

In this document, terms in *italics* have a specific meaning under the Privacy Act. Some terms are defined below and others in the text where they are first used.

AAP Entity means an entity subject to the Privacy Act.

***affected information recipient (*AIR)** means mortgage insurers, trade insurers, related body corporates of *credit providers*, professional and legal advisers, and contractors that process applications for credit and manage credit.

consumer credit means credit that is intended to be used wholly or primarily:

- for personal, family or household purposes;
- to acquire, maintain, renovate or improve residential property for investment purposes; or
- to refinance credit that has been provided for the above purposes.

consumer credit liability information means, in relation to a *consumer credit* contract:

- the name of the *credit provider*;
- whether the *credit provider* holds an ACL;
- the type of *consumer credit*;

- the day on which the *consumer credit* contract is entered into;
- the terms and conditions of the *consumer credit*;
- the maximum amount of credit available; and
- the day on which the *consumer credit* is terminated.

commercial credit means a loan other than *consumer credit*. The use and disclosure of credit reports is regulated in relation to both *consumer credit* and *commercial credit*. There are different rules for *consumer credit* and *commercial credit*.

credit information is a sub-set of *personal information* because the individual's identity is provided with the credit information. There are specific types of financial information that fall within this definition.

credit provider includes banks, building societies, credit unions, and companies where a substantial part of their business is the provision of loans. Businesses will also be treated as *credit provider*s if they are agents or servicers of *credit provider*s, or suppliers of goods or services that defer payment for more than seven days, such as electricity and telecommunications providers.

credit reporting body (CRB) includes what used to be called credit reporting agencies.

credit reporting information is *credit information* that is obtained from a *CRB.*

personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

sensitive information is personal information about such things as race, religion, membership of *a* trade association or profession, sexual orientation, criminal record or health information. Health information includes recording an illness or pregnancy on an application form or information collected to support a hardship application.

2.3 Who is regulated by the Privacy Act?

The Privacy Act applies to any business that:

(a) had a turnover greater than $3,000,000 in the previous financial year; or

(b) is a subsidiary of a company that had a turnover of more than $3,000,000; or

(c) regardless of turnover, discloses personal information about an individual for a benefit, service or advantage.

Most finance industry participants do not fall within the small business operator exemption as they disclose personal information about individuals for a benefit, service, or advantage, and so must comply with the Privacy Act.

2.4 What is regulated by the Privacy Act?

The Privacy Act has a separate set of provisions dealing with the collection, use, and disclosure of:

(a) *personal information*; and

(b) *credit information.*

2.5 Where does the Privacy Act apply?

The Privacy Act extends to acts done or practices engaged in outside Australia if:

- the *personal information* relates to an Australian citizen;
- the organisation has a continued presence in Australia; and
- the *personal information* was collected or held by the organisation in Australia either before or at the time of the act or practice.

Part IIIA of the Privacy Act, which relates to credit reporting by *credit providers*, does not apply to credit and defaults occurring outside Australia.

2.6 Why is the Privacy Act important?

The OAIC is able to:

(a) make determinations about privacy issues;

(b) obtain enforceable undertakings from organisations;

(c) require organisations to offer compensation for breaches;

(d) apply to court to obtain a civil penalty order of up to $1,700,000 for corporations and $340,000 for individuals; and

(e) seek criminal penalties.

2.7 Positive credit reporting

The Privacy Act allows for positive credit reporting. Prior to 12 March 2014 Australia only had negative credit reporting.

Credit providers have the choice to operate in a negative credit reporting environment or move to a more comprehensive credit reporting environment. However, if a *credit provider* only discloses negative *credit information* to a *CRB*, they will only be able to obtain negative credit reporting information.

Positive credit reporting means the *credit provider* is able to disclose more information to *CRBs*, such as whether the borrowers make loan repayments on time, the type and amount of loans that are outstanding, and the amount of a borrower's repayment obligations.

2.8 Must all contractors inform individuals when they collect *personal information?* – APP5

APP5 states that '*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 to notify the individual… [that] the entity…has collected the personal information*.'

For example, if a servicer, valuer, or law firm receives information about an individual from a *credit provider* in relation to a loan application, management, or recovery, is that servicer, valuer, or law firm have to notify the individual that it has received the information in accordance with APP5. This additional disclosure could be very confusing for customers and adds nothing to assist privacy, so long as the recipient only uses the information for the purposes of the principal.

A key issue is whether a contractor acting on behalf of an entity, should be treated separately from that entity under the Privacy Act. Section 8 of the Privacy Act largely mirrors the general law by providing that the actions of an employee will be regarded as the actions of the employer organisation for the purposes of the Privacy Act. However, this section appears to go further than the general law by providing that the actions of a person "employed by or in the **service of**…" (emphasis added) an

organisation are the actions of the organisation. This suggests that a contractor acting *in the service of* an organisation should be treated as the organisation (ie the contractor should not be treated separately from the organisation contracting it) for the purposes of the Privacy Act.

The OAIC suggests that contractors who provide services for an organisation are not considered to fall within s 8 (ie the contractor and contracting party are separate organisations for the purposes of the Privacy Act). However, the OAIC further suggests that where there is a *close relationship* between an organisation and a contractor it may mean the actions of the contractor could be treated as the actions of the organisation contracting it.

Even if the relationship is not a 'close relationship', no notice may be required because the recipient is only required to take 'reasonable steps' to comply with APP5.1. In some cases it could be reasonable for no steps to be taken. This may be the case where:

(a) the contractor agreement has comprehensive privacy provisions that place stringent obligations on the contractor to protect an individual's privacy;

(b) the organisation contracting out its obligations is prepared to monitor the contractor to ensure it complies with the APPs; and

(c) the organisation is prepared to be ultimately responsible for any contravention of the APPs by the contractor.

Applying this principle, an APP5 notice should not be required by entities such as valuers, document preparation houses, anybody with an interest in the credit, mailing houses, credit card producers, statement preparers, or anybody who is considering acquiring an interest in a *credit provider's* business.

2.9 Overseas Disclosure

APP8 imposes rules regarding *overseas disclosure* of *personal information.*

Overseas disclosure of *personal information* occurs when *personal information* is sent to a third party that is not located in Australia. It does not apply to disclosures by a company to a branch located outside Australia, but would apply to disclosure to a related body corporate located overseas.

The routing of *personal information* through servers located outside Australia is 'use' but not 'disclosure' for the purposes of the Privacy Act.

An entity wishing to make an *overseas disclosure* has three options to avoid being liable for any breach of the Privacy Act. However, financiers are likely to be blamed for any breach by an overseas entity despite complying with one or more of these options.

Option 1: Take reasonable steps to ensure that the recipient does not breach the APPs - APP8.1.

Option 2: Reasonably believe that:

- the overseas recipient is subject to a law that has the overall effect or is substantially similar to the ways the APPs protect the information; **and**
- there are mechanisms for the individual to seek redress under that law - APP8.2(a).

Option 3: Obtain an informed consent from the individual to the overseas disclosure - APP8.2(b). Informed consent means a consent given after the individual is made aware that they will have no protections under the APPs in relation to the *personal information* disclosed to the overseas entity.

However, in relation *credit information,* the *credit provider* must take reasonable steps to:

(a) ensure the overseas entity does not use or disclose the credit eligibility information other than in accordance with Australian legislation; and

(b) ensure the overseas entity does not breach the APPs.

The disclosure of *credit information* overseas is governed by Part IIIA of the Privacy Act. When a *credit provider* discloses *credit information* overseas, the *credit provider* will be liable for any breaches or acts that are undertaken by the overseas recipient. This is in addition to other legislation and general law principles.

PART 3. Other Legislation

3.1 Spam Act

How does all this sit with the *Spam Act 2003* (Cth)?

The *Spam Act 2003* (Cth) prohibits the sending of unsolicited commercial electronic messages linked with Australia. In summary:

(a) it is illegal to send most commercial electronic messages to or from Australia without the recipient's consent;

(b) certain commercial electronic messages are exempt from the consent requirement;

(c) those commercial electronic messages which can be lawfully sent must include accurate information about the sender and generally contain a functional unsubscribe facility;

(d) it is illegal to supply, acquire, or use address-harvesting software or a harvested address list; and

(e) civil penalties of up to $1,100,000 apply to these illegal activities.

Inferred consent can arise where the recipient has a reasonable expectation that the message will be sent. It may be reasonable to infer consent from an existing relationship with the individual.

3.2 Anti Money Laundering and Counter Terrorism Financing Act

The *Anti Money Laundering and Counter Terrorism Financing Act* 2006 (Cth) allows customer identification to occur using *credit information* held by a *CRB*. The provisions:

(a) permit *credit provider*s to disclose specified *personal information* to *CRBs* for identity verification purposes **but only with the express consent of the individual** whose identity is being verified;

(b) permit *CRBs* to conduct a matching process between *personal information* provided to it by a reporting entity and the *personal information* held on its own files and provide an assessment to the *credit provider*; and

(c) require *credit providers* to notify the individual of unsuccessful attempts to verify identity using credit reporting data.

AUSTRAC has issued guidance 11/02 which says that the express consent might require ticking a box, and that a reporting entity should not rely on a failure to opt out. The customer must also be given another option for customer identification.

PART 4. Access and correction

4.1 Introduction

The Privacy Act and the Credit Reporting Code impose requirements on those that hold *personal information* and *credit information*. Entities that do not hold *credit information* only need to comply with APP 10, 12, and 13, and not the Credit Reporting Code.

4.2 Access to *personal information*

The key provisions are:

- **APP10 – Quality of *personal information*:** An APP entity is required to take reasonable steps in the circumstances to ensure that any *personal information* that it collects is accurate, up to date and complete. Reasonable steps may include ensuring updated or new *personal information* is promptly added to relevant existing records or providing individuals with a simple means to review and update their information on an on-going basis, for example through an online portal.

- **APP12 – access to *personal information*:** An APP entity must have a mechanism for individuals to access the *personal information* that an entity holds about them. There is a list of exemptions to providing that individual with their *personal information* such as when the information relates to legal proceedings or the request is frivolous or vexatious.

- **APP13 – Correction of *personal information*:** If an APP entity is satisfied that *personal information* it holds is inaccurate, out of date, incomplete, irrelevant or misleading or the individual requests that their *personal information* be corrected, then the entity must take reasonable steps to correct that *personal information*. If an entity refuses to correct the *personal information*, it must give the individual written notice setting out the reasons for the refusal and provide information about the complaint mechanisms available to the individual. .

4.2 Access to and correction of *credit information*

If an individual requests an entity that holds *credit information* to provide access or make correction to *credit information*, that entity has certain obligations to comply with the request. A person who can seek access is an *access seeker* and is either the individual or someone authorised in writing to make a request for access. An *access seeker* cannot be a *credit provider*, insurer, or real estate agent. *Access seeker*s currently include credit repair agencies.

The Credit Reporting Code imposes additional obligations on those that access the credit reporting regime in relation to access and correction to *credit information*.

*Credit provider*s must:

(a) provide means for individuals to access their *credit information* that the *credit provider* holds;

(b) respond substantively within 30 days of the individual's request for access;

(c) present the *credit information* clearly and provide reasonable explanations and summaries of the information; and

(d) advise the individual to access their *credit information* from a *CRB* for the most up to date information.

There are extensive provisions about how a *credit provider* must act if requested to correct information, including contacting other *credit providers* and *CRBs*.

PART 5. Tax File Numbers

5.1 Use of Tax File Numbers

Finance industry participants do not require tax file numbers (**TFNs**), but often receive TFNs as part of the documents used to verify income. For example, TFNs may be listed on a notice of assessment and tax returns provided by a prospective borrower for credit assessment.

Tax agents should delete TFNs before supplying tax related documents (see guidelines below).

The Privacy Act requires that a TFN recipient must not engage in practices that would breach a guideline issued by the OAIC (s13(4)).

The OAIC has issued binding guidelines pursuant to s 17 relating to the handling of TFNs, the key provisions of which are as follows.

(a) The TFN is not to be used as a general reference number, nor as an identifier for non-tax related purposes.

(b) The quotation of the TFN is not mandatory and is voluntary. The decision to quote must always rest with the individual.

(c) The use of the TFN by investment bodies to build up a database or to cross-match personal information is not permitted.

(d) The method of collection of the TFN is to be in a manner approved by the Commissioner of Taxation.

(e) The TFN must be protected to prevent loss, unauthorised access, use, modification, disclosure, or misuse.

5.2 Do TFNs need to be deleted from documents received by brokers, credit providers etc?

Some mortgage industry participants delete TFNs from electronic records, refuse to accept electronic documents containing TFNs, or cut or black out TFNs from paper documents.

In the past, TFNs were often required to be deleted from a document that an individual provided to, for example, a mortgage broker.

The current position is that TFNs need not be deleted but must be securely stored. The guidelines apply to any entity that receives a solicited or unsolicited TFN. The guidelines indicate the following:

- **Storage, security and disposal of TFN information:** TFN recipients must have in place reasonable security safeguards to prevent loss, unauthorised access, modification or disclosure of an individual's TFN. This includes restricted access to any records that contain TFNs.

- **Incidental provision of TFNs:** If an individual provides a TFN when they are not required to do so (such as on a PAYE slip), the individual may not be prevented from removing the TFN and if the individual chooses not to remove the TFN, the recipient must not record, use, or disclose the TFN.

- **Staff training:** TFN recipients must take such steps that are reasonable in the circumstances to make all staff aware of the need to protect the privacy of individuals in relation to their TFNs and make staff aware of the prohibitions on the use and disclosure of TFNs.

Annexure 1 - Australian Privacy Principles summary

Personal information is governed by the Australian Privacy Principles (**APP**s). The following is a brief summary of the APPs. This summary does not replace reading the APPs in full, which can be accessed here.

APP1: Have a privacy policy which is available free of charge, and which should be displayed on my website. The over-riding obligation is to manage *personal information* in an open and transparent way, so that individuals know how their *personal information* will be used.

APP2: If practical, deal with customers on an anonymous basis.

APP3: Only collect *personal information* that is reasonably necessary.

APP4: *Personal information* that is received without a request must be destroyed unless it could have been collected under APP3.

APP5: As soon as practical before or after collecting *personal information* provide prescribed information about how the information will be used. This is what the Privacy Consent and your Privacy Policy does.

APP6: Use *personal information* only for the particular purpose for which it was collected unless the individual consents or would reasonably expect the use for another purpose.

APP7: Only direct market if the individual would reasonably expect it, has consented, or it is impracticable to obtain that consent. Messages must provide a way to opt out.

APP8: Only disclose *personal information* overseas if you have verified that the overseas entity will not breach the APPs, is subject to similar laws as the APPs, or the individual consents.

APP9: Do not use government identifiers, such as tax file numbers.

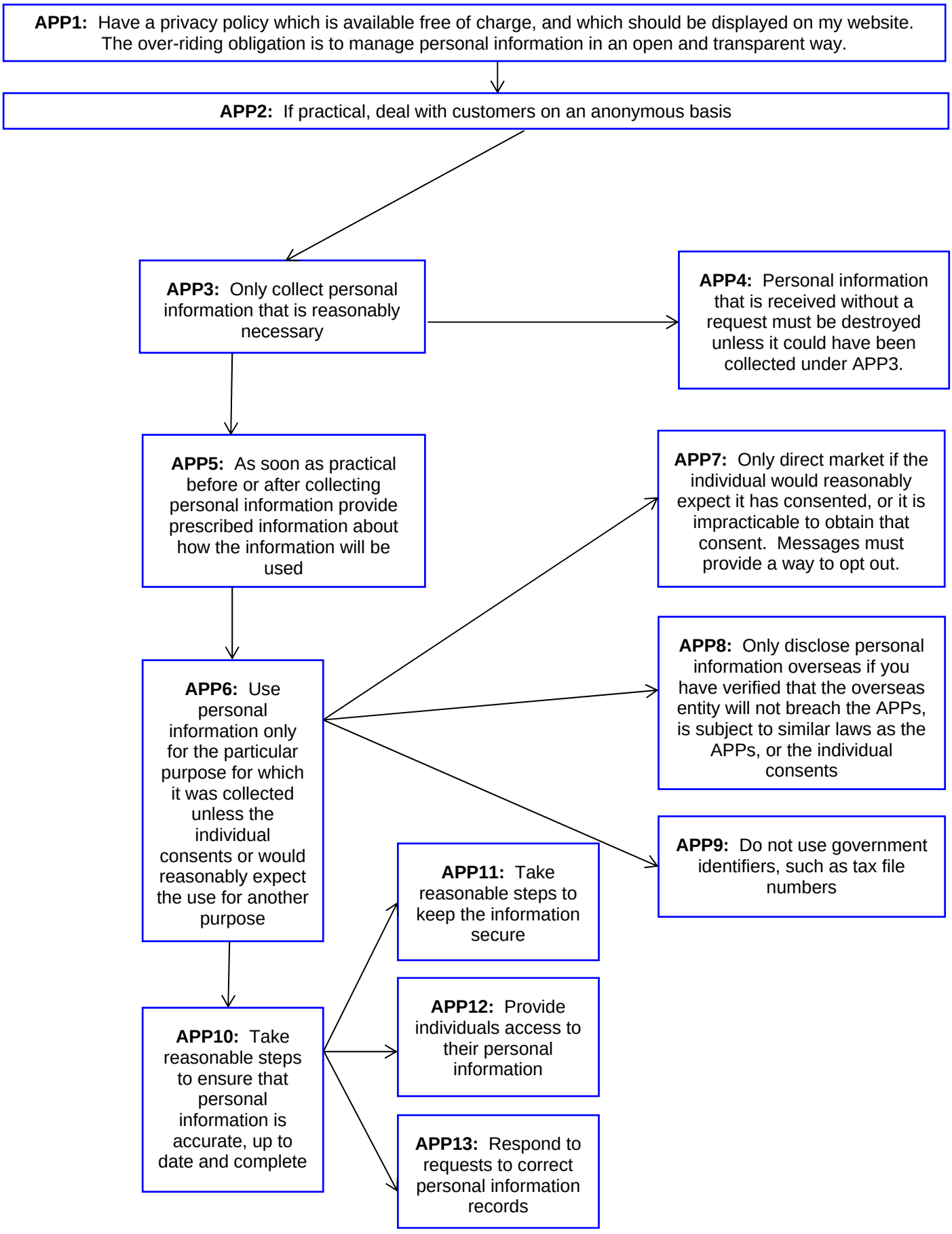
APP10: Take reasonable steps to ensure that *personal information* is accurate, up to date and complete.

APP11: Take reasonable steps to keep the information secure.

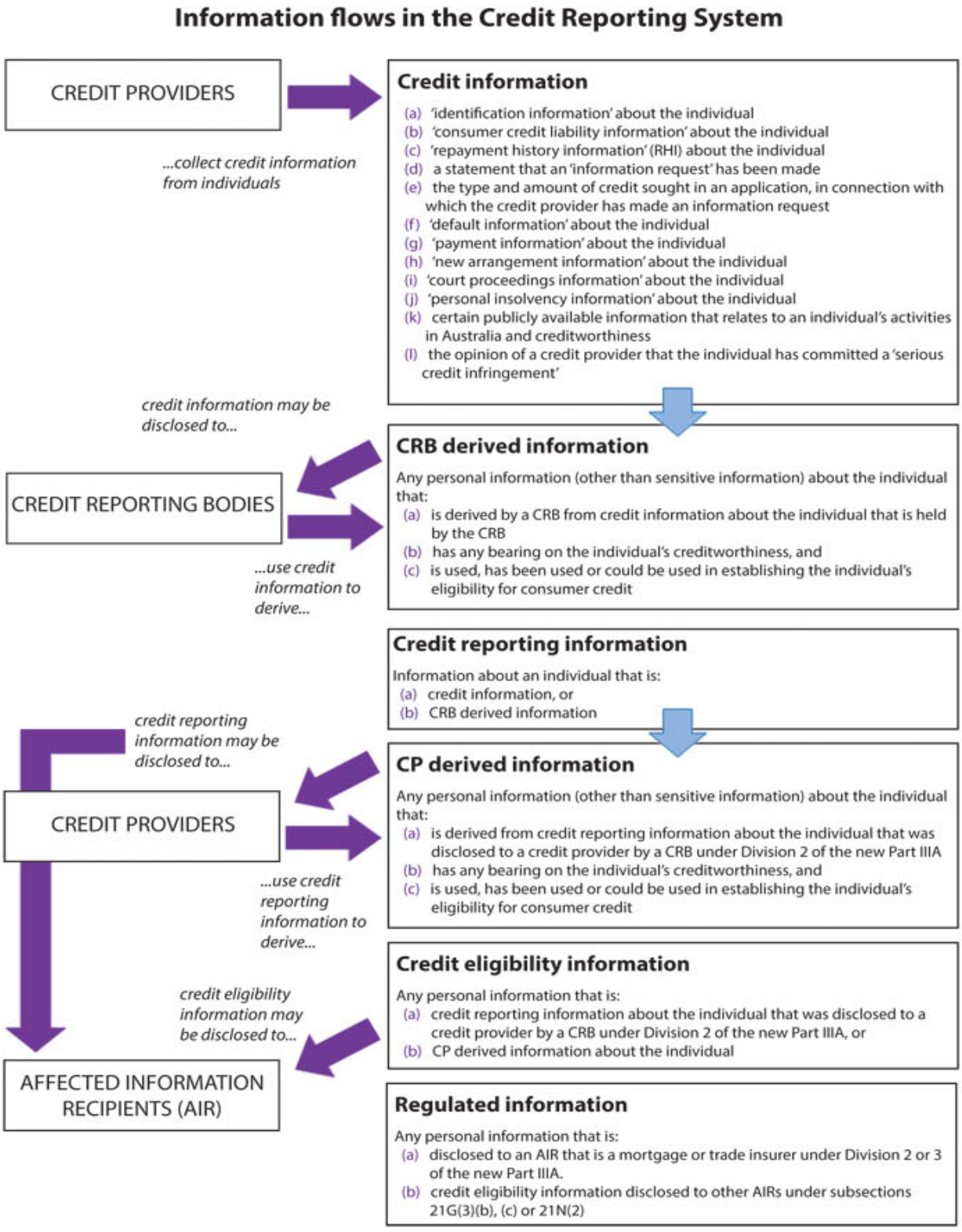
APP12: Provide individuals access to their *personal information* have a Privacy Plan (except businesses with, say, less than four five employees).

APP13: Respond to requests to correct *personal information* records.

Annexure 2 – APP Flow Chart



Annexure 3 - Information flows through the credit reporting system



Annexure 4 – Key Provisions about *credit information*

Credit eligibility information is broadly *credit information* that has been received by a *credit provider* from a *CRB*. A further explanation can be found in the 'Information flow through the credit reporting systems' diagram in **Annexure 3**. Some provisions apply to commercial credit (as indicated).

Obligations of *credit providers*

Section	Requirement
26L	*Credit reporting bodies* and *credit providers* must comply with the Credit Reporting Code.
21D(2)	A *credit provider* can only disclose *credit information* to a *credit reporting body* if the *credit provider* is a member of a recognised external dispute resolution scheme. This section applies to both *consumer* and *commercial credit*.
21D(3)	*Repayment history information* about an individual can only be disclosed by a *credit provider* if the *credit provider*: • holds an Australian Credit Licence; and • has previously disclosed *consumer credit liability information* (ie the fact the consumer has entered into the credit contract, the amount, etc).
21F	Introduces a 'ban period' when there is a hold on the disclosure of *credit information* to a *credit reporting body*. A ban period is 21 days after a consumer makes a request to a *credit reporting body* not to disclose *credit information* because that individual believes on reasonable grounds that they are a victim of fraud - see s20K(1).
21T	An individual can contact a *credit provider* to request access to and correction of *credit information* held by the *credit provider*.

Disclosure by a credit reporting body

The following instances are when a credit reporting body is permitted to disclose *credit information*.

Section	Requirement
20C	A *credit reporting body* may only collect *credit information* from a *credit provider* if the *credit provider* is a member of an external dispute resolution scheme. This applies to *consumer credit* and *commercial credit*.
20E(3)	A *credit reporting body* may only disclose *credit information* to a *credit provider* if the: • *credit provider* requests the *credit information* for a *consumer credit* related purpose; • *credit provider* requests the *credit information* for a *commercial credit* related purpose, and the individual expressly consents (does not need to be in writing unless the application is in writing); • *credit provider* requests the *credit information* for a credit guarantee purpose and the individual expressly consents in writing; • *credit reporting body* is satisfied that the *credit provider* believes the

	individual has committed a serious credit infringement; or • *credit provider* holds current *consumer credit liability information* that relates to the credit extended by the *credit provider*.
	A *credit reporting body* may also make disclosures to: • a *credit provider* for securitisation related purposes; • a *mortgage insurer* for *mortgage insurance* purposes; • a trade insurer where it is for trade insurance purposes and the individual expressly consents in writing; • an external dispute resolution scheme; or • an enforcement body (such as ASIC or the ATO).
20E(4)	A *credit reporting body* may only disclose *repayment history information* to a *credit provider* that holds an Australian Credit Licence or to a *lenders mortgage insurer.*

Pre-screening assessment

Credit reporting bodies have the capability to conduct *pre-screening assessment*. A *pre-screening assessment* is the use of an individual's *credit information* that is held by a *credit reporting body* for the purposes of direct marketing by a *credit provider*. There are several conditions that need to be met:

(a) the *credit provider* must hold an Australian Credit Licence;

(b) the direct marketing must relate to *consumer credit*;

(c) the consumer credit liability information (the type of credit, date entered into, term of the credit, maximum amount of credit available, etc) and repayment history information cannot be used for other direct marketing purposes by the *credit provider*;

(d) the credit reporting body must use the *credit information* to assess whether an individual meets the criteria provided by the *credit provider*; and

(e) the individual must not have made an opt-out request.

The *credit reporting body* will disclose a list of individuals which only includes those individuals that have met the *credit provider's* pre-screening criteria. The *credit reporting body* and the *credit provider* must destroy the pre-screening information as soon as it no longer needs the information for its intended purpose.

Limits on use of credit information by *credit providers*

The following table summarises the use of *credit eligibility information* by *credit providers*.

Section	Requirement
21G(2)	If a *credit provider* holds *credit eligibility information* then it may use that *credit eligibility information*: • for *consumer credit* related purposes; or • where the *credit provider* believes the individual has committed a serious credit infringement and the *credit eligibility information* is used in connection with the infringement.

	If the *credit eligibility information* has been obtained for *consumer credit* related purposes then the *credit information* can be used for: • securitisation related purposes; or • internal management purposes related to the provision of the *consumer credit*. If the *credit eligibility information* was: • obtained for *commercial credit* purposes, then the *commercial credit eligibility information* may only be used for that particular purpose; • obtained for the purpose of assessing an application for *commercial credit* then, the *credit eligibility information* may also be used for internal management purposes directly related to the provision or management of that *commercial credit*; • obtained for guarantee purposes, then the *credit eligibility information* may also be used for internal management purposes in addition to the credit guarantee purpose; • disclosed to a *credit provider* because the *credit provider* already held *consumer credit liability information*, then the *credit eligibility information* may also be used for the purpose of assisting the individual to avoid defaulting on their obligation in relation to *consumer credit* provided by the *credit provider*; or • disclosed for securitisation related purposes, then the *credit eligibility information* may only be used for that particular purpose.
S21G(3)	A *credit provider* is able to disclose *consumer credit information* to: • the individual; • to a related body corporate; • to a person for the purposes of processing an application or a person who manages credit; • another *credit provider* with an *Australian link* and the first *credit provider* believes on reasonable grounds the individual has committed a *serious credit infringement*; or • an external dispute resolution scheme if the *credit provider* is a member of that scheme.

Limits on disclosure by *credit providers*

A *credit provider* is permitted to disclose *credit eligibility information* about an individual in the following circumstances.

Section	Requirement
21J	**To other *credit providers*** Disclosure to another *credit provider* is allowed if: • the disclosure is for a particular purpose; • the recipient has an *Australian link*; and • the individual expressly consents to the disclosure of the *credit information* to the recipient for a particular purpose.

	Consent must be in writing unless the *credit eligibility information* is for the purpose of assessing an application for *consumer credit* that is not yet in writing. Disclosure by a *credit provider* of *credit eligibility information* is permitted if: • the provider is acting as an agent of another *credit provider* in the assessing of an application for credit or managing the credit; and • the provider discloses the information to another *credit provider* in the provider's capacity as an agent. Disclosure by a *credit provider* is allowed if: • the provider is carrying on a business that involves a securitisation arrangement; • the credit relates to a *credit provider* with a *Australian link*; • the original *credit provider* is not undertaking securitisation arrangements; and • the disclosure is reasonably necessary for the purchasing, funding, managing, or processing of an application for credit by means of a securitisation arrangement or undertaking credit enhancement in relation to the credit. Disclosure of *credit eligibility information* is permitted to another *credit provider* when: • both *credit provider*s have provided mortgage credit in relation to the same secured real property and have an *Australian link*; • the individual is at least 60 days overdue in making a payment; and • the *credit information* is disclosed for the purpose of either *credit provider* deciding what action to take in relation to the overdue payment.
21K	**Guarantees** A *credit provider* is able to disclose *credit eligibility information* if: • the *credit provider* has provided credit to the individual or the individual has applied for credit; • the disclosure is for the purpose of considering whether to act as a guarantor or to offer property as security for the credit; • the guarantor has an *Australian link*; and • the individual expressly consents to the disclosure of the *credit eligibility information* for that purpose. The consent needs to be in writing unless the application for credit was not in writing.
21L	***Mortgage insurer*s** A *credit provider* is able to disclose *credit eligibility information* if the disclosure is to a *mortgage insurer* with an *Australian link* for: • lenders *mortgage insurance* purposes; or • any purpose arising under a contract for lenders *mortgage insurance*.
21M	**Debt collectors**

	A *credit provider* is able to disclose *credit eligibility information* if: • the 'debt collector' carries on a business that involves the collection of debts on behalf of others; • the *credit eligibility information* is disclosed for the primary purpose of collecting payments that are overdue in relation to either *consumer credit* or *commercial credit*; and • the information that is disclosed to the debt collector is the following: - *identification information*; - *court proceedings information*; or - *personal solvency information*, which includes *default information* in relation to overdue payments of *consumer credit* where the *credit provider* does not hold any information that suggests the individual has made any payments in relation to the overdue default amount.
21N	**Other recipients** A *credit provider* is permitted to disclose *credit eligibility information* if the disclosure is to one or more of the following recipients that have an *Australian link*: • a government agency, small business of other organisation subject to the APPs; • a professional legal adviser of the entity; or • a professional financial adviser of the entity. The recipient may use the *credit eligibility information* for the purposes of either exercising the rights associated with, or considering whether to: • accept an assignment of debt; • accept a debt owed to the *credit provider* as security for credit provided to the *credit provider*; or • purchase an interest in the *credit provider* or a related body corporate.
21NA	**What if there is no *Australian link?*** If a *credit provider* wants to disclose *credit eligibility information* to an entity with no *Australian link*, the *credit provider* must take reasonable steps to: • ensure the overseas entity does not use or disclose the *credit eligibility information* other than in accordance with Australian legislation (ie above); and • ensure the overseas entity does not breach the APPs. The Australian *credit provider* will be treated as having done the act or practice of the overseas entity if it discloses *credit eligibility information* to an overseas entity with no *Australian link*.

Information to be given if an individual's application for credit is refused

Section 21P of the Privacy Act applies where an application for *consumer credit* has been refused on the basis of *credit information* held by a *credit reporting body* in relation to either the individual or a guarantor. Within a reasonable time after refusing the application for credit, the *credit provider* must:

(a) give written notice of the refusal;

(b) state that the refusal was wholly or partially based on the *credit information* held by the *credit reporting body*; and

(c) if the information is about the individual, then state the name and contact details of *the credit reporting body.*

The Credit Reporting Code extends section 21P of the Privacy Act by requiring:

(a) a *credit provider* who refuses an individual's application for credit; and

(b) has obtained *credit information* from a *credit reporting body* in the previous 90 days in relation to that individual regardless if that *credit information* forms part of the basis for the refusal

to provide written notice of the matters set out in paragraph 16.3 of the Credit Reporting Code.

Information to be given prior to listing default information with a *CRB*

Sections 6Q and 21D of the Privacy Act require an individual be given notice that a *credit provider* intends to list default information with a *CRB*. Default information is information about an overdue payment in relation to *consumer credit* if:

(a) the individual is 60 days overdue in making the payment;

(b) the *credit provider* has given the individual written notice requesting payment of the overdue amount;

(c) the *credit provider* is not prevented by the statute of limitations from recovering the overdue amount; and

(d) the amount is more than $150.

The written notice that is required by section 6Q of the Privacy Act is called the **section 6Q notice**.

After the *credit provider* has provided the required notice under section 6Q then notice under section 21D(3)(d) is required (**section 21D notice**). This notice must state that:

(a) the *credit provider* intends on disclosing the overdue payment to the *CRB*; and

(b) at least 14 days have passed since given the notice under section 21.

In addition to the Privacy Act requirements, the Credit Reporting Code states:

- the section 6Q notice must be given at least 30 days prior to the section 21D notice;
- the *credit provider* cannot disclose more than the amount specified in the section 21D notice and any payments made by the individual must be taken into account;
- all components must be overdue by at least 60 days; and
- the amount in the section 21D notice must not be disclosed to the *CRB* less than 14 days or more than 3 months after the section 21D notice.