DOUBLE J RELOCATIONS

PRIVACY PROCEDURES

BACKGROUND AND OBJECTIVES

The *Privacy Act 1988* (Cth) and the *Australian Privacy Principles* protect personal information which belongs to individuals by placing restrictions on how that information can be collected, handled, used and disclosed. Most businesses that collect and use personal information are bound by the main requirements of the privacy laws.

The credit reporting requirements of the *Privacy Act 1988* (Cth) and the *Credit Reporting Privacy Code* apply to all businesses who allow their customers credit terms of greater than 7 days (**Credit Providers)**.

You must follow our Privacy Policy and these Procedures when collecting and using personal **and** credit information.

PRIVACY OFFICER

Our Privacy Officer is Hayley Quigley. He is responsible for ensuring that we comply with our Privacy Policy and these Privacy Procedures. Consult the Privacy Officer if you have any privacy related concerns or questions.

WHAT IS PERSONAL INFORMATION?

Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable. It does not matter whether it is true or whether it is oral or in writing.

In effect, it is information or an opinion that can identify a person, for example, their name, physical description, address, employer / place of work, salary and employment details, business activities, investments and assets and liabilities – or any combination of these.

Sensitive personal information is information or an opinion about a person's racial or ethnic origin, political opinions, membership of a political, trade or professional association or a trade union, religious or philosophical beliefs or affiliations, sexual preferences, criminal record or health information (including biometric and genetic information).

Credit information is essentially all information that relates to a person's consumer credit liabilities, credit history, capacity to pay and eligibility to be provided with consumer credit. It includes information about credit applications, defaults (of >$150 and 60 days), applications for credit information and personal insolvency.

OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

Personal information must be managed in an open and transparent way. This requires us to:

- Implement practices, procedures and systems to ensure compliance with privacy laws and appropriately handle enquires or complaints about privacy;
- Have a clear and up to date Privacy Policy that documents the way we manage personal information, including:
    - The kinds of information we collect;
    - How we collect it and for what purpose;
    - How people can access and correct their information;
    - How people can make a privacy related complaint;
    - Whether we are likely to disclose information to overseas recipients and if so, where they will be located.

Our Privacy Policy must also cover how we manage credit information that we either hold or have obtained from a credit reporting body such as VEDA.

Our Privacy Policy outlines how we manage our privacy obligations. Our Privacy Policy is available free of charge on our website and in paper or electronic form to anyone who asks for it. Provide a copy of the Privacy Policy to anyone who asks for it by giving them a copy directing them to our website or sending it to them by post or email.

COLLECTION AND USE OF PERSONAL INFORMATION

Personal information must only be collected if it is necessary for the functions and services we provide and must be collected by lawful and fair means and not in an unreasonably obtrusive way. It should only be collected from the person to whom it relates unless it is unreasonable or impracticable to do so.

When you collect personal (and credit) information, you must tell the person from whom you collect it the following things:

- Who we are and how they can contact us;
- Why we are collecting the information and to whom we usually provide it;
- If we are likely to disclose the personal information to a credit reporting body, the name and contact details of that body;
- Any law that requires the information to be collected;
- What will happen if they do not provide the information to us;
- The fact that they can gain access to the information, correct it or complain about a breach of privacy law and that the details of how to do this and how we will deal with the complaint are in our Privacy Policy; and
- Whether the information is likely to be disclosed to someone overseas and if so, the countries in which they are likely to be located.

You can do this by telling the person this information or providing them with a copy of our Privacy Collection Statement. This has been incorporated into documents and correspondence that we use to communicate with customers and potential customers for the first time (e.g. website, terms and conditions of contract, quotation, and proposal.

Showing your concern for the confidentiality of the client's information is a good way to create trust. Reassure customers that they can obtain access to their information at any time if they want to check or update it.

Collection from Third Parties

If you need to collect information from someone other than the person to whom it relates, ensure that the person that the information is about is aware of the above matters and the fact that their information has been collected, when and how this was done, and who provided it to us. Do this by contacting the person to whom the information relates and provide a copy of the privacy collection statement.

Tip
Make sure you know how you obtained a person's information and from whom – if they ask you must be able to tell them.

Sensitive Information

Always obtain consent when you collect or disclose sensitive information. In most cases, this will occur in the usual course of dealings. Consents can be incorporated into quotation request forms and other documents used to collect this information.

You must not collect sensitive information without consent unless:

- The collection is required by law; or
- It is reasonably necessary for one of more of our activities.

Always consult the Privacy Officer if you are unsure.

Unsolicited Information

If you inadvertently receive personal information (i.e. you didn't solicit or directly collect it), we can only retain it and use it if it is information that we would have been permitted to collect in the first place – i.e. because we need it for the functions and services we provide.

You must make an assessment of unsolicited information as soon as possible after you receive it. If you would not have collected it or it is not relevant to the services or functions we provide, destroy it or de-identify it.

If in doubt, consult the Privacy Officer who will provide instructions on what to do with the unsolicited information.

USE AND DISCLOSURE OF PERSONAL INFORMATION

Personal information should only be used or disclosed for the primary purpose for which it was collected.

It can be used or disclosed for secondary purposes, i.e. different purposes than the main purpose for which we collected the information, where:

- The secondary purpose is related to the primary purpose and the individual would reasonably expect us to use or disclose it for the secondary purpose. An indirect relationship is sufficient unless the information is sensitive information in which case the secondary purpose must be directly related to the primary purpose; or
- The individual has consented to the use or disclosure; or
- The use or disclosure is required by law or by order of a court or tribunal; or
- You have reason to suspect that unlawful activity has, is or may be engaged in and use of the information is a necessary part of your investigation of the matter or in reporting your concerns to the relevant persons or authorities; or
- It is necessary for the establishment, exercise or defence of a legal or equitable claim or the purposes of a confidential alternative dispute resolution process.

We do not trade, rent or sell personal information.

You must not provide personal information to anyone other than the organisations to whom the client has expressly or impliedly authorised us to provide it to.

It may be permissible to use or disclose information in some other unusual circumstances. If you want to use or disclose personal information for any reason other than those described above, or are in any doubt about your obligations, consult the Privacy Officer who will provide advice and/or obtain legal advice where necessary.

Direct Marketing

An individual's personal information (e.g. their name and contact details) can be used for direct marketing if:

- They would reasonably expect us to do so;
- We collected their personal information from them; and
- We provide a simple means for them to request not to receive any more direct marketing communications.

If a person would not reasonably expect us to send direct marketing communications to them, or we collected their personal information from someone other than them, it must not be used for direct marketing unless:

- They consent to receiving direct marketing communications (or it is impracticable to obtain their consent);

- We provide a simple means for them to request not to receive any more direct marketing communications; and
- Each direct marketing communication:
  - If in writing - contains a prominent statement; or
  - If by telephone – makes them aware that,

  they can request not to receive such communications in the future.

We can't assume that customers expect us to send direct marketing communications to them. The test is whether a reasonable person would expect this.

If conducting a direct marketing campaign, consider whether:

- Customers have consented; or
- Our Privacy Policy explains that we will do this; or
- We notified customers in our Privacy Collection Statement that one of the purposes of collection of their information was for direct marketing.

Opting Out – If conducting a direct marketing campaign, include a simple means for customers to 'opt out' of receiving further marketing material, i.e.:

- A clear instruction on what to do; and
- A quick and simple opt out process that uses the same communication channel that is used to deliver direct marketing material (e.g. by email for email marketing).

Use words to the following effect on all promotional material: **"***Acrobat Removals Pty Ltd is delighted to provide this flyers, email, newsletters and SMS as a service to you. Please let us know if you would rather not receive it and we will remove your name from our distribution list."*

We do not charge customers to 'opt out' and if they have done so, we must ensure that their details are not used for direct marketing again.

Tip
If you undertake direct marketing, set up an internal No Contact / No Call Register to record the names of customers who have opted out and wash client data against this before commencing a campaign.

Credit Information

Use of Credit Eligibility Information[1] **-** There are limits on how we can use information about a person's eligibility for credit, creditworthiness or other information obtained from a credit reporting body. As a general rule, we can only:

- Use it to assess whether we will extend credit to the person, collect overdue payments or help them to avoid defaulting on any credit we have provided and provide it to related companies;
- Provide it to other credit providers and their agents if the person consents in writing;
- Provide it to debt collectors that we appoint to collect overdue payments or consumer and commercial credit (or potential assignees of the debt).

Disclosure of Credit Information to Credit Reporting Bodies[2] **-** Only disclose an individual's credit information to a credit reporting body, if:

- It relates to events that occurred after the person turned 18; and
- The credit was provided or applied for in Australia.

[1] S 2121NA *Privacy Act 1988* (Cth)
[2] S21D-21F *Privacy Act 1988* (Cth)

Defaults - If the credit information is about a default, we must give the individual 14 days' notice in writing of our intention to provide their information to the credit reporting body. If the amount owing is later paid, inform the credit reporting body about the payment.

Repayment history – Never provide a credit reporting body with information about an individual's repayment history. Only the holder of an Australian credit licence can do this.

Always keep a record on the client's file, of any credit information you disclose to a credit reporting body.

Overseas Disclosure

If we disclose personal information to overseas recipients and they breach Australian privacy laws, we may be deemed to have breached the law.

If you will need to disclose personal information to anyone overseas, before doing so you must take reasonable steps to ensure that they:

- Will not breach the Australian Privacy Principles (e.g. ensure that they are contractually bound to comply with them); or
- Are subject to laws which provide similar protection to Australian laws and can be enforced by the individuals whose personal information is being disclosed.

Tip
Ensure that any contracts you enter with overseas information recipients, include an obligation to comply with the Australian Privacy Principles.

Consult the Privacy Officer if you need to check whether an overseas information recipient is subject to privacy laws similar to Australian laws. If the Privacy Officer is unsure and we don't have a contractual arrangement under which we can require the proposed recipient to comply with Australian laws, you must:

- Inform anyone about whom you collect personal information, that we cannot give any assurances about how the information will be used, stored or disclosed by the overseas recipient; and
- Obtain their express written consent before it is disclosed to them.

Disclosure overseas is permitted in other limited circumstances including where it is required by Australian law or an Australian court or tribunal.

These obligations also apply if you need to disclose credit information to overseas recipients.

QUALITY AND SECURITY OF INFORMATION

We must take reasonable steps to ensure that the personal information we collect, use or disclose is:

- Accurate, up-to-date, complete and relevant; and
- Kept protected from misuse, interference and loss or from unauthorised access, modification or disclosure.

In dealings with customers, ask them to confirm that the information we hold about them is correct and up to date.

If information has become irrelevant, destroy or de-identify it.

The Privacy Officer will regularly review our security measures – including assessing whether information that is no longer used and no longer required to comply with the law, can be destroyed.

These obligations also apply to credit eligibility information.

ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

Access
In most cases, customers are entitled to access the personal information we hold about them on request. If a person requests access to their personal information, we must respond within a reasonable period and where possible allow access in the manner asked for (e.g. by sending copies of records or allowing someone to inspect them at our office).

On receipt of a request for access:

- Check what particular information the person wants to ensure that you do not provide more than is required; and
- Confirm that the person requesting the information is who they claim to be by asking them to supply a copy of their driver's licence or passport to verify their identity.

You can then provide the requested information by the most cost-effective method available. This could be:

- Letting the person attend our office to inspect the information and take notes of its contents;
- Letting the person view the information and provide an explanation of its contents;
- Providing a photocopy, fax or email of the information;
- Providing a printout of information held in electronic form; or
- Providing a summary of the information.

Timeframes - If you receive a request for access, acknowledge it within 7 days. The request must then be fulfilled within the following timeframes:

- Straightforward requests - within 7-14 days; and
- Complex requests - within 30 days.

Charges - We must not charge anyone for lodging a request for access however, we can charge a reasonable amount to recover our expenses for providing information following a request for access. Charges must be based on the actual cost of providing access and can include staff costs of locating and collating information, photocopy charges and the cost of having someone explain information.

Refusing access - We may refuse to provide access to personal information in the following circumstances:

- The request is frivolous, vexatious (i.e. trivial), made to pursue an unrelated grievance against us or is a repeated request for the same information;
- Provision would unreasonably impact on the privacy of others;
- The information relates to existing or anticipated legal proceedings against us by the person and the information would not be discoverable in those proceedings;
- Provision would reveal our intentions in negotiations with the person in such a way as to prejudice the negotiations; or
- It is unlawful to provide access, the law permits or requires access to be denied or it would prejudice the activities of enforcement bodies.

The Privacy Officer will decide whether a request should be refused. Refer any access request to the Privacy Officer if you believe we may have grounds to do so.

If we refuse a request we must provide written reasons for this and tell the person about our procedures for making a privacy related complaint.

The Privacy Officer must approve all access refusals before they are communicated to the person who has made the request.

These obligations also apply to credit eligibility information**.**

Correction
If any personal information in our records is incorrect, incomplete, irrelevant, misleading, inaccurate or out of date or if a client requests a correction of their information, we must update the records to make them accurate, up to date, complete, relevant and not misleading and do so within a reasonable period.

On receipt of a request for correction:

- Check what particular information the person wants to correct and identify where it is stored;
- Confirm that the person requesting the information is who they claim to be by asking them to supply a copy of their driver's licence or passport to verify their identity; and
- Update the information accordingly.

Often this will occur after a person has requested access to their information.

If the person's records are no longer required we must securely destroy them or de-identify personal information contained in them.

If in doubt, consult the Privacy Officer before destroying or de-identifying information.

Timeframes – If you receive a request for the correction of information, acknowledge it within 7 days. The information must then be corrected within the following timeframes:

- Straightforward requests - within 7-14 days; and
- Complex requests - within 30 days.

If you are asked to notify the correction to others who have received the person's personal information (i.e. other companies we deal with), do so immediately unless it is impracticable or unreasonable to so do.

Charges - We cannot charge for correcting information.

Refusing correction - We may refuse to correct personal information if we do not agree that it is inaccurate, out of date, incomplete, irrelevant or misleading.

The Privacy Officer will decide whether a correction request should be refused. Refer any correction request to the Privacy Officer if you believe we may have grounds to do so.

If we do not agree that information needs to be corrected, we must provide written reasons for our refusal and tell the person who submitted the request about our procedures for making a privacy related complaint. If requested, we must also attach a statement to the information we hold (e.g. to the client file) which notes that the client believes it is out of date, incomplete, inaccurate, irrelevant or misleading.

The Privacy Officer must approve all correction refusals before they are communicated to the person who has made the request.

These obligations also apply to credit eligibility information**.**

GOVERNMENT IDENTIFIERS

We do not collect government related identifiers from customers (e.g. tax file numbers, medicare numbers or drivers licence numbers).

Do not ask customers for these identifiers. If you are given one inadvertently (e.g. because it is contained on or within another document provided by a client) ensure that this is immediately securely destroyed or otherwise permanently erased or blacked out.

PRIVACY COMPLAINTS

If you receive a complaint about the use of personal (or credit) information, hand it to the Privacy Officer immediately.

Remember that complaints need not be in writing. They may be presented by any reasonable means, e.g. by letter, telephone, in person or email.

The Privacy Officer will ensure that all privacy related complaints are handled and recorded in accordance with our Complaint Handling Procedures.

PRIVACY BREACHES

A privacy breach occurs if we hold personal information about an individual and breach:

- Our legal obligations in relation to its collection, handling, use, storage or disclosure; or
- The provisions in our Privacy Policy or these Privacy Procedures.

If you identify an actual or possible privacy breach, report it to the Privacy Officer immediately.

Eligible Data Breaches

If a privacy breach occurs and is an 'eligible data breach' we must report it to the *Office of the Australian Information Commissioner* (OAIC) and affected individuals. We must do this within strict timeframes. However, if we act quickly to manage a breach and ensure that it will not cause any serious harm to an individual, we do not need to report the matter to the OAIC or affected individuals.

A privacy breach will be an eligible data breach if it results in:

- Unauthorised access to or disclosure of personal information; or
- Information being lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur,

and in either case, this is reasonably likely to result in serious harm to an affected individual.

Data Breach Response Plan

The Privacy Officer will investigate and deal with privacy breach reports in accordance with the following Data Breach Response Plan.

Data Breach Occurs		
Step	**Action**	**Timeframe**
1	**Contain the breach and do a preliminary assessment:** • Take immediate steps to contain breach	

	• Secure vulnerable information • Designate breach response team • Plan and coordinate investigation	Within 24 hours of breach identification
2	**Investigate cause and extent:** • How did the breach occur? • Who has it affected? • What kind(s) of information are involved? • What is the risk of harm to affected individuals? • What type of harm may occur (e.g. identity theft, financial loss, humiliation, damage to reputation, social bullying, threat to safety)?	Within 20 days of breach identification
3	**Evaluate – Is this an eligible data breach?** • Has there been unauthorised access to or disclosure of personal information? • Has information been lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur? • Is any unauthorised access to or disclosure of information likely to result in **serious harm** to an affected individual having regard to: - The kind or kinds of information the breach relates to; - The sensitivity of the information; - Whether the information is protected by one or more security measure and if so, the likelihood of them being overcome; - The persons or kinds of persons who have obtained or could obtain the information; - If security technology or methodology was used to protect the information and designed to make it unintelligible or meaningless to unauthorised persons (e.g. an encryption key), the likelihood of this being circumvented; - The nature of the harm that could be suffered by an affected individual; - Any other circumstances relevant to the breach. **Yes to these questions = eligible data breach.**	Within 30 days of breach identification
4	**Notify OAIC (if eligible data breach):** • Submit statement to OAIC setting out: - Our business' identity and contact details; - A description of the breach that has occurred; - The kind(s) of information concerned; and - Recommendations about the steps affected individuals should take in response to the breach.	Immediately if necessary to mitigate a high level of risk of serious harm. Otherwise, as soon as possible after confirmation of eligible data breach (**NB**. In limited circumstances and after obtaining legal advice the Privacy Officer may apply to

		the OAIC for an extension of time)
5	**Notify affected individuals (if eligible data breach):** • If practicable - notify the content of the OAIC statement to each individual to whom the relevant information relates; or • If practicable - notify the content of the OAIC statement to each individual who is at risk from the breach; or otherwise • Publish a copy of the OAIC statement on our website and take such other steps as are reasonable to publicise its content. Individuals may be contacted by the usual method used for communicating with them or such other way as the Privacy Officer considers appropriate to mitigate the effects of the breach.	As soon as possible after OAIC notification (**NB**. In limited circumstances and after obtaining legal advice the Privacy Officer may apply to the OAIC for an extension of time)
6	**Notify others (if appropriate) e.g.:** • Police / law enforcement agencies • Entities we are contractually bound to notify	At the same time or as soon as possible after OAIC notification
7	**Prevent future breaches** • Identify root cause of breach • Implement preventative action • Review and update privacy policy and procedures • Identify and carry out any staff training or performance management that is necessary	Within 45 days of breach identification

PRIVACY TRAINING

We ensure that our staff and representatives are aware of our Privacy obligations, Privacy Policy and these Privacy Procedures by including a Privacy component in our induction and compliance refresher training. Staff also receive on the job training as and when required.

PRIVACY REVIEW

Our Privacy Officer will review our Privacy Policy and these Privacy Procedures from time to time to ensure that they remain effective and up to date.

■