DLA PARTNERS (QLD) PTY LTD
PRIVACY POLICY

DLA Partners ("DLA") is committed to treating the personal information we collect in accordance with the Australian Privacy Principles in the Privacy Act 1988 (Cth) (Privacy Act). This Privacy Policy sets out how DLA handles all personal information.

This Privacy Policy does not apply to personal information collected by DLA that is exempted under the Privacy Act, for example employee records.

DLA will modify this Privacy Policy if required to reflect its current privacy practices.

PERSONAL INFORMATION – WHAT WE COLLECT

The types of personal information we collect includes:

- names, job titles, contact and address details;
- information in identification documents (for example, passport, driver's license);
- tax file numbers and other government-issued identification numbers;
- date of birth and gender;
- bank account details, shareholdings and details of investments;
- details of superannuation and insurance arrangements;
- educational qualifications, employment history and salary;
- visa or work permit status; and
- personal information about your spouse and dependents.

It may be necessary in some circumstances for DLA to collect sensitive information about you in order to provide specific services or for recruiting purposes. Examples of the types of sensitive information that may be collected in such circumstances include professional memberships, ethnic origin, criminal record and health information.

It is generally not practical to remain anonymous or to use a pseudonym when dealing with DLA as usually we need to use your personal information to provide specific services to you, or which relate to or involve you.

PERSONAL INFORMATION –HOW WE COLLECT IT

We collect your personal information from you directly (for example, when we deal with you in person or over the phone, when you send us correspondence (including via email), when you complete a questionnaire, form or survey, or when you subscribe to our newsletter). Sometimes it may be necessary for us to collect your personal information from a third party. For example, we may collect your personal information from your employer where they are our client, from your personal representative or a publicly available record. We may also collect personal information about you from your client log in on our website.

PERSONAL INFORMATION – OTHER PEOPLES

If you provide us with someone else's personal information, you should only do so if you have their authority or consent to do so. You should also take reasonable steps to inform them of the matters set out in this Privacy Policy.

PERSONAL INFORMATION – STORAGE

DLA holds personal information in hard copy and electronic formats. We take security measures to protect the personal information we hold including physical (for example, our offices are protected with a security system and storage of files in lockable cabinets) and technology (for example, restriction of access, firewalls, the use of encryption, passwords and digital certificates) security measures. We also have document retention policies and processes.

PERSONAL INFORMATION –PURPOSE FOR COLLECTING, HOLDING, USING AND DISCLOSING

DLA collects, holds and uses personal information for a number of purposes including:

- to provide professional services;
- to provide technology services and solutions;
- to respond to requests or queries;
- to maintain contact with our clients and other contacts;
- to keep our clients and other contacts informed of our services;
- to notify of seminars and other events;
- for administrative purposes;
- for recruitment purposes;
- for purposes relating to the employment of our personnel, providing internal services or benefits to our partners and staff and for matters relating to the partnership;
- when engaging service providers, contractors or suppliers relating to the operation of our business;
- to manage any conflict of interest or independence (including auditor independence) obligations or situations;
- to conduct surveys;
- for seeking your feedback;
- to meet any regulatory obligations;
- as part of an actual (or proposed) acquisition, disposition, merger or de-merger of a business or entering into an alliance, joint venture or referral arrangement; or
- for any other business related purposes.

If you do not provide us with the personal information we have requested, we may not be able to complete or fulfil the purpose for which such information was collected, including providing you or our clients with the services we were engaged to perform.

The types of third parties to whom we may disclose your personal information include:

- experts or other third parties contracted as part of an engagement;
- our service providers;
- our professional advisers;
- as part of an engagement, if you are a customer, an employee, a contractor or supplier of services to one of our clients, then we may disclose your personal information as part of providing services to that client;
- as part of an actual (or proposed) acquisition, disposition, merger or de-merger of a business or to enter into an alliance, joint venture or referral arrangement; or
- government or regulatory bodies or agencies, as part of an engagement or otherwise, (for example, the Australian Taxation Office).

We do not disclose personal information to third parties for the purpose of allowing them to send marketing material to you. However, we may share non personal, de-identified or aggregated information to them for research or promotional purposes.

PERSONAL INFORMATION –DISCLOSURE OVERSEAS

Depending on the nature of the engagement or circumstances of collection, DLA may disclose your personal information to entities overseas to fulfil the purpose for which the personal information was collected, or a related or ancillary purpose or otherwise in accordance with the Privacy Act. The countries to which such disclosures are made, and types of personal information disclosed, depend on the specific circumstances of the engagement. In some circumstances, we use third party service providers. These service providers are typically located in India or the Philippines.

PERSONAL INFORMATION – DIRECT MARKETING

DLA Partners may also use your personal information for the purpose of marketing its services. If you do not want to receive marketing material from us, you can contact us as detailed below:

• for electronic communications, you can click on the unsubscribe function in the communication; or
• for hard copy communications, you can email us through our contact details below.

CHILDREN

We understand the importance of protecting children's privacy. It is our policy to never knowingly collect or maintain information about anyone under the age of 13, except as part of a specific engagement to provide professional services which necessitates such personal information be collected.

GAINING ACCESS TO PERSONAL INFORMATION WE HOLD

You can request access to your personal information, subject to some limited exceptions permitted or required by law. Such request must be made in writing. Please see our contact details below.

DLA may charge reasonable costs for providing you access to your personal information.

KEEPING PERSONAL INFORMATION CURRENT

If you believe that any personal information DLA has collected about you is inaccurate, not up-to-date, incomplete, irrelevant or misleading, you may request correction. To do so, please contact us and we will take reasonable steps to correct it in accordance with the requirements of the Privacy Act.

COMPLAINTS

If you wish to make a complaint to DLA about our handling of your personal information, please contact us. You will be asked to set out the details of your complaint in writing.

DLA will endeavor to reply to you within 30 days of receipt of the complaint and, where appropriate, will advise you of the general reasons for the outcome of the complaint. In some circumstances, we may decline to investigate the complaint, for example if the complaint relates to an act or practice that is not an interference of the privacy of the person making the complaint. If you are not satisfied with the outcome of your complaint, you can refer your complaint to the Office of the Australian Information Commissioner.

HOW TO CONTACT US

If you have a query in relation to this Privacy Policy or you would like to notify us that you no longer wish to receive marketing material from us, access or correct your personal information or to make a complaint about the handling of your personal information, please contact us as follows:

The Office Manager
DLA Partners
800 Zillmere Road
ASPLEY QLD 4034

T +61 7 3863 9444

F +61 7 3263 8008
Eclientservices@dlapartners.com.au

DLA PARTNERS (QLD) PTY LTD
DATA BREACH POLICY AND PROCEDURE

BACKGROUND AND OBJECTIVES

The *Privacy Act 1988 (Cth)* and the *Australian Privacy Principles* which can be found in Privacy fact sheet 17 (https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles) protect personal information which belongs to individuals by placing restrictions on how that information can be collected, handled, used and disclosed.

At DLA Partners (Qld) Pty Ltd (**'DLA Partners', 'DLA' 'we', 'our', 'us'**) we recognise that clients' privacy is extremely important and take our responsibilities in protecting their privacy very seriously. We are bound by, and committed to supporting our **Privacy Policy** which sets out a summary of our obligations under the Australian Privacy Principles ('**APPs**'), (https://www.dlapartners.com.au/wp-content/uploads/2016/10/DLA-Partners-Privacy-Policy.pdf).

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

- Implement practices, procedures and systems to ensure compliance with privacy laws and appropriately handle any 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 and hold it;
  - The purposes for which we collect, hold, use and disclose it;
  - How people can access and correct the information we hold about them;
  - How people can make a privacy related complaint and how we deal with such complaints; and
  - Whether we are likely to disclose information to overseas recipients and if so, where they will be located;
- Report an 'eligible data breach' to the Office of the Australian Information Commissioner ('**OAIC**') and any affected individuals pursuant to the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)*.

The DLA Partners **Privacy Policy** on the DLA Partners website outlines the way in which we and our authorised representatives collect, hold, use and disclose personal information.

This **Data Breach Policy and Procedure** document outlines how we manage any potential privacy breaches, and covers DLA Partners Employees and Contractors.

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, date of birth, sex, phone number, email address, driver's licence number and information about their employer / place of work, salary and employment, business activities, investments, assets and liabilities – or any combination of these. Businesses generally hold two types of personal information, that of employees and that of clients or customers.

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).

WHAT IS A PRIVACY BREACH?

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

- Our legal obligations in relation to its collection, handling, use or disclosure; **or**
- The provisions of our **Privacy Policy** (https://www.dlapartners.com.au/wp-content/uploads/2016/10/DLA-Partners-Privacy-Policy.pdf).

WHO IS IMPACTED BY THIS DATA BREACH RESPONSE PLAN?

When a DLA Partners Employee or Contractor (each referred to as **'DLA Representative', 'you', 'your', 'yourself'**) identify an actual or possible privacy breach, it must be reported to the DLA Partners Office Manager (**'Privacy Officer'**) immediately in accordance with this **Data Breach Response Plan**.

WHAT IS AN ELIGIBLE DATA BREACH?

When an 'eligible data breach' occurs, we must usually report it to the OAIC and affected individuals within strict timeframes. However, this may not be required if we act quickly to manage the breach and ensure that it will not cause any serious harm to an individual.

A privacy breach is 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 this is reasonably likely to result in 'serious harm' to an individual***.**

What is serious harm?

Serious harm can include identity theft and serious physical, psychological, emotional, financial or reputational harm. Some kinds of personal information breaches are more likely than others to cause serious harm e.g. those that involve sensitive information such as medical or health information, information or documents commonly used for identity theft (e.g. Medicare details, drivers licence or passport information) or financial information. Combinations of different types of personal information (as opposed to a single piece of information) may be more likely to result in serious harm.

* Outsourced / Offshored / 3rd Party Arrangements

Under the OAIC requirements if an 'eligible data breach' involves personal information that you and another organisation hold e.g. an outsourced service provider or joint venture partner, only one of them needs to assess and report the breach to the OAIC and affected individuals. However, if no-one undertakes the assessment or makes the report, they could both be liable for a breach of the requirements.

As a general rule, the entity that has the **most direct relationship** with the affected individual(s) should report. In the case of outsourced/offshored related arrangements this would be DLA partners.

You will need to ensure that your service and other relevant contracts with outsourced / offshored / 3rd parties include provisions:

- Requiring compliance with the data breach reporting regime;
- Requiring the other party to notify you immediately if there is a privacy breach and cooperate with any investigation and remediation you undertake; and
- Setting out who is responsible for assessing and reporting data breaches.

Action Required: DLA Partners Representative to contact DLA Partners Office Manager (**'Privacy Officer'**) immediately, if the issue of a potential eligible data breach arises with an outsourced / 3rd party service provider in Australia or overseas, with full details.

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — **Is serious harm still likely?** — **YES**

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

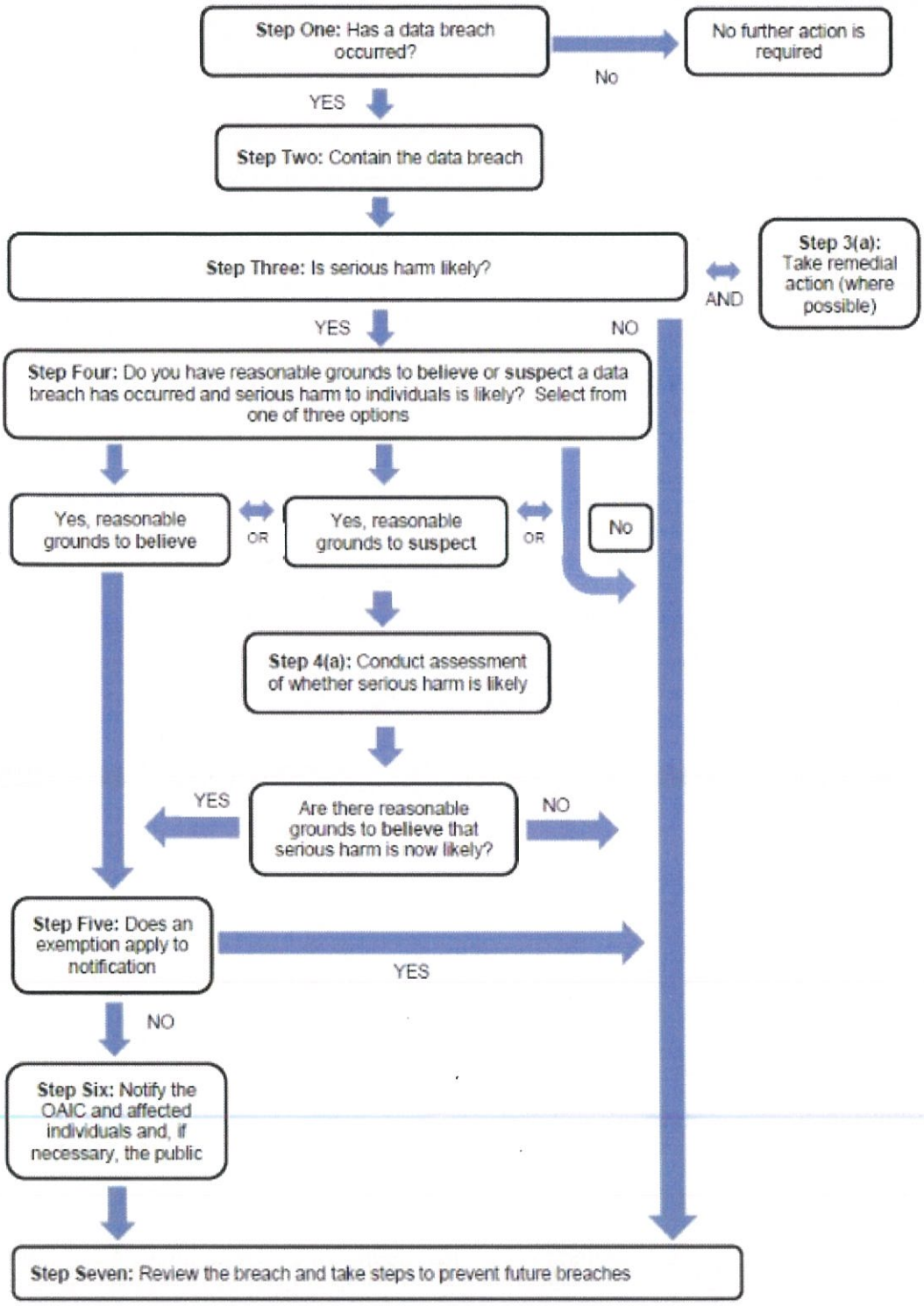
Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.


Step One: Has a data breach occurred?
No
No further action is required
YES
Step Two: Contain the data breach
Step Three: Is serious harm likely?
AND
Step 3(a): Take remedial action (where possible)
YES
NO
Step Four: Do you have reasonable grounds to believe or suspect a data breach has occurred and serious harm to individuals is likely? Select from one of three options
Yes, reasonable grounds to believe
OR
Yes, reasonable grounds to suspect
OR
No
Step 4(a): Conduct assessment of whether serious harm is likely
YES
Are there reasonable grounds to believe that serious harm is now likely?
NO
Step Five: Does an exemption apply to notification
YES
NO
Step Six: Notify the OAIC and affected individuals and, if necessary, the public
Step Seven: Review the breach and take steps to prevent future breaches