VICTORIAN BAR

PROTOCOL

DATA BREACH RESPONSE PLAN

Governing policy: The Victorian Bar Privacy Policy

The Victorian Bar (**the Bar**) is committed to preventing data breach occurrences and ensuringthat proper procedures and clear lines of authority are in place in the event that the Bar experiences a data breach or suspects that a data breach has occurred.

The Bar manages personal information in accordance with the *Privacy Act 1988* (Cth) (**Privacy Act**). This protocol should be read in conjunction with the Bar's Privacy Policy and Acceptable Use Policy.

Purpose

The purpose of the Data Breach Response Plan (**Response Plan**) is to provide a clear procedure for the effective co-ordination and management of data breaches to ensure minimal impact to the Bar, its members and staff, and to ensure that its regulatory obligations are met. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

This Response Plan applies to any person within the Bar who handles personal information,including the Victorian Bar Council, the Executive Director, senior management, Bar staff, contractors and third parties operating on behalf of the Bar. If any of these persons suspect or become aware of a data breach, this Response Plan is activated and must be followed. Members of the Bar, service providers or any other persons who suspect that the Bar has suffered a data breach are also encouraged to report.

This Response Plan enables the Bar to work in conjunction with its wholly owned subsidiary,Barristers' Chambers Limited (**BCL**) to contain, assess and respond to

data breaches in a timely manner and to mitigate potential harm to affected individuals.

This Response Plan will be reviewed by the Bar Council every two years.

Applicable legislation

The *Privacy Amendment (Notifiable Data Breaches) Act* 2017 (**NDB Act**) amended Part IIIC of the Privacy Act and established a Notifiable Data Breaches Scheme, which requires organisations covered by the Privacy Act to notify **eligible data breaches** to the Office of theAustralian Information Commissioner (**OAIC**) and affected individuals.

Roles and responsibilities

This Response Plan sets out the roles and responsibilities relevant to the Bar in the case of adata breach or potential data breach and documents the processes to be followed, in orderto assist the Bar's response.

Data Breach Response Officer (DBR Officer)

The Bar's DBR Officer (Corporate Services Manager) is responsible for co-ordinatingthe Bar's response efforts in the event of a data breach and plays a critical role in mitigatingdamage caused by a breach.

The DBR Officer must be prepared to execute this Response Plan when a breach occurs, including by collecting all relevant information in respect of the breach and conducting a preliminary assessment with guidance from BCL and/or other relevant stakeholders, as appropriate. The DBR Officer reports directly to the Privacy Officer (Executive Director of the Bar).

Privacy Officer

The Bar's Privacy Officer has responsibility to oversee the work of the DBR Officer as well as determining the severity of the data breach and whether individuals and the OAIC are required to be notified.

The Privacy Officer is also responsible for approval of corrective actions or preventative actions in respect of the breach, as well as periodic reporting to the Bar Council as appropriate.

Staff and senior management

It is essential that the Bar's staff members and senior management are aware of their responsibilities to alert the Bar of any breach identified. Required details about the breach or potential breach, if known, must be provided to the DBR Officer.

Process where a data breach has occurred or is suspected

1. Alert

Where a data breach has occurred or is suspected, any persons to whom this Response Planapplies must bring the breach to the attention of the DBR Officer **as soon as reasonably practicable.**

Collection of information

The DBR Officer is required to collect and record the following details in respect of thebreach:

a. when the breach occurred;

b. description of the breach;

c. description of the type of personal information involved;

d. cause of the breach (if known) and how it was discovered;

e. identification of the individuals who are affected;

f. identification of the systems affected (if any); and

g. whether corrective action has occurred.

2. Containment

The DBR Officer, with guidance from BCL, must ensure that appropriate steps are taken to contain the data breach as soon as practicable.

3. Preliminary assessment

The DBR Officer must make a preliminary assessment as to whether there has been an **eligible data breach**. If the criteria for an eligible data breach is

satisfied, the breach becomesa Notifiable Data Breach (**NDB**) and triggers the Bar's notification obligations under the Privacy Act.

An **eligible data breach** is defined under Division 2 Part IIIC of the Privacy Act and ariseswhen the following criteria is satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information on or after 22 February 2018;
2. the breach is likely to result in serious harm***** to one or more individuals; and
3. the entity has not been able to prevent the likely risk of serious harm withremedial action.

***Note:** The term 'serious harm' is not defined in the Privacy Act. In the context of aneligible data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

The preliminary assessment must be reported to the Bar's Privacy Officer in an incident report (**Incident Report**) with details as to the following:

- the type of personal information involved;
- whether it is sensitive information (as defined in paragraph 2.8 of the Bar's Privacy Policy);
- the context of the affected information and the breach;
- the cause and extent of the breach;
- whether there are any protections that would prevent the personal information from being used;
- what steps have been taken to remedy the breach;
- the risk of serious harm to the affected individuals, such as
    - identity theft;
    - financial loss;
    - a threat to their physical safety;
    - a threat to their emotional wellbeing;
    - economic or financial harm;
    - humiliation, damage to reputation or relationships; or
    - workplace or social bullying or marginalisation;
- any legal, financial or reputational ramifications; and

- any media or stakeholder attention as a result of the breach.

The DBR Officer must take all reasonable steps to ensure that the preliminary assessment iscompleted **within 30 days** of becoming aware of the breach.

4. Notification obligations

If an NDB has occurred, the Bar must notify OAIC and affected individuals of the NDB as soon as practicable. The requirement for notification must be assessed on a case-by-casebasis and be approved by the Privacy Officer.

Notifiable Data Breach (two-step notification)

i. Notifying the OAIC

The DBR Officer, with the guidance of BCL where appropriate, must prepare a prescribedstatement to the OAIC that includes:

- the Bar's contact details;
- a description of the NDB;
- the kind of information concerned; and
- recommendations about the steps that individuals should take in response to theNDB.

The statement will be approved by the Privacy Officer and submitted to OAIC as soon as practicable. An online submission form named 'Notifiable Data Breach Statement' can be accessed via this link.

ii. Notifying individuals affected

After submitting the prescribed statement to the OAIC, the Bar must:

- take reasonable steps to notify the contents of the prescribed statement to eachof the individuals to whom the information relates; or
- take reasonable steps to notify the contents of the prescribed statement to eachof the individuals who are at risk from the NDB.

If it is not practical to undertake either of the above, the DBR Officer must ensure a copy ofthe prescribed statement is published on the Bar's website and

reasonable steps are takento publicise the contents of the statement in In Brief to notify members and staff.

Other notifications

Depending on the nature of the breach, it may also be appropriate to notify third partiessuch as the police, insurance companies, credit card companies, financial institutions, professional or other regulatory bodies.

Exception to notification

The Privacy Act allows for a 'remedial action exception' to notification, whereby the Bar is **not required** to fulfil its notification obligations if:

- it takes action in relation to the loss of personal information, or unauthorised accessor disclosure, before any serious harm is caused to affected individuals; and
- as a result of the action, a reasonable person would determine that the data breachwould not likely result in serious harm to the affected individuals.

If the Privacy Officer determines that the breach falls into the remedial exception categoryand can be managed by the Bar internally, the DBR Officer must:

- ensure immediate corrective action is taken (if not already);
- ensure a detailed report of the data breach is submitted to the Privacy Officer, outlining the following:
    - a description of the data breach;
    - the corrective actions or remedial steps taken – this may include retrieval or recovery of the personal information, ceasing unauthorised access,shutting down or isolating the affected system;
    - outcome of actions taken;
    - prevention processes implemented (if any); and
    - recommendation that no further investigation or action is necessary.

Declaration from OAIC

The Bar may seek a declaration from the OAIC that notification is not required or to modifythe period in which the notification needs to occur. The OAIC has indicated that such declarations will be limited to exceptional circumstances where delay is necessary, or the breach is not appropriate to notify.

5. Review and prevention

The Bar is committed to improving its data security processes. Following any data breach, the Bar will work with BCL and assess the need for implementation of measures to improvedata security processes, such as conducting an investigation, updating of policies andprocedures, and providing member or staff training.

Bar Council approval will be sought where appropriate.

Records management

Documents collected or created by the DBR Officer in respect of a data breach will belogged in the Bar's Data Breach Response folder, which will be accessible by the DBR Officer and Privacy Officer.

Record keeping procedures must be in accordance with the Bar's Records Management Policy.

References

- This Response Plan has been informed by:
    - The OAIC's *Guide to developing a data breach response plan*
    - The OAIC's *Data breach notification guide: a guide to handling personal informationsecurity breaches*
    - NDB Act
    - Privacy Act and Australian Privacy Principles