बैंक ऑफ़ बड़ौदा Bank of Baroda

NOTIFIABLE DATA BREACHES SCHEME

PREAMBLE

The NDB scheme applies from 22 February 2018 to all agencies and organisations with existing personal information security obligations under the Privacy Act. It was established by the passage of the Privacy Amendment (Notifiable Data Breaches) Act 2017.

The scheme includes an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. The notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches.

Agencies and organisations must be prepared to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm, and as a result require notification.

DATA BREACH

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost. A data breach may be caused by malicious action both by external and internal party, human mistakes or failure of the IT handling or security systems of the organisation.

These include:-

a. Unauthorised access to personal information by an employee

b. Inadvertent disclosure of personal information due to “human error”, for example an email sent to the wrong person

c. Disclosure of an individual’s personal information to a scammer, as a result of inadequate identity verification procedures

d. Loss or theft of physical devices (store devices, mobile phones, laptops) or paper records that contain personal information.

CONSEQUENCES OF DATA BREACH

Data breach may cause severe harm to individuals and organisation in many ways and these include:-

i. Financial fraud including unauthorised credit card transactions or credit fraud

ii. Identity theft causing financial loss or emotional and psychological harm

iii. Family violence and

iv. Physical harm or intimidation

This can also result in reputational loss to the organisation for the privacy protection and can harm entity’s commercial interests as privacy protection

contributes an individual's trust in an organisation. A lax systems and process in this area may result in loss of customer confidence which will be detrimental to interest of the Bank.

RISK MITIGATION

An entity can reduce the reputational impact of a data breach by effectively minimising the risk of harm to affected individuals, and by demonstrating accountability in their data breach response. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals occurs.

The Privacy Act contains 13 Australian Privacy Principles (APPs) that set out banks obligations for the management of personal information. Compliance with these principles will reduce the risk of Data breach. Compliance with APP 11 is key to minimising the risk of a data breach. APP 11 requires entities to take reasonable steps to protect the personal information the bank holds from misuse, interference and loss and from unauthorised access, modification and disclosure.

NOTIFIABLE DATA BREACHES (NDB) SCHEME

The NDB scheme in Part IIIC of the Privacy Act requires entities to notify affected individuals and the Commissioner of certain data breaches. The NDB scheme requires entities to notify individuals and the Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur)
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

Entities must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

The primary purpose of the NDB scheme is to ensure individuals are notified if their personal information is involved in a data breach that is likely to result in serious harm. This has a practical function: once notified about a data breach, individuals can take steps to reduce their risk of harm. For example, an individual can change password to compromised online accounts, and be alert to identity fraud or scams.

ELIGIBLE DATA BREACH

An eligible data breach is established when the following events occur:-

a. There is unauthorised access to or unauthorised disclosure of personal information, that an entity holds

b. This is likely to result in serious harm to one or more individuals

c. The entity has not been able to prevent the likely risk of serious harm with remedial action

DATA BREACH RESPONSE PLAN of BANK OF BARODA SYDNEY

BOB Sydney has prepared a Response plan. This plan enables BOB Sydney to respond quickly in case of a data breach. By responding quickly and appropriately, BOB Sydney can reduce substantially the impact of a breach on affected individuals, reduce the cost associated with those breaches and in turn reduce the potential reputational loss. The plan further will help BOB Sydney

a. To meet the obligations under The Privacy Act

b. Limit the losses and impact of the data breach

c. Help avoiding the reputational loss and maintain public confidence\

The plan envisages the roles and responsibilities in managing the data breach and specifies the action plan an entity will take in cases of data breach.

ROLES AND RESPONSIBILIES AND ESCALATION PROCESS IN BOB SYDNEY

Title	Role
Staff of Bank of Baroda Sydney	➢ Report any suspected breach to their line manager ➢ To discuss the reason for suspicion with their line manager ➢ Complete Data Breach Report and submit to line Manager
Vice President (Administration and IT)	➢ Receive the data breach report from the line manager of the department that suspect the breach ➢ Take immediate steps to contain the breach, harm and preserve any evidence. ➢ Forward the data breach report to the Risk and Compliance Officer

Risk and Compliance Officer	➢ Receive the data breach report from the Vice President (Administration and IT) ➢ Call for a meeting with the staff that reported the breach along with the line manager and VP (Administration and IT) ➢ Provide the finding to Chief Executive, Compliance Internationals and SOOA ➢ Record the findings in the incident register ➢ Determine the seriousness of the breach ➢ Evaluate the steps taken to mitigate the harm of the breach
Title	**Role**
	➢ Notify the affected individuals ➢ Notify the Office of the Australian Information Commissioner (OAIC)

REPORTING TIME FRAMES

Suspected data breach must be investigated and managed as soon as the Bank of Baroda Sydney becomes aware of such a breach. Normally it should be done immediately as soon as the issue is raised by any staff of the bank.

Assessment of the data breach	All reasonable steps should be to complete the assessment within 30 days of Bank of Baroda Sydney become aware of the data breach and this is the maximum time frame. This should be done as soon as possible
Eligible Data Breach	All remedial measures should be taken as quickly as possible to contain the harmful impact and report should be made to OAIC

RESPONDING TO DATA BREACHES – ACTION PLAN

BOB Sydney has four key point step to respond to any data breaches

Step 1: Report and contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

Step 1: REPORT AND CONTAIN

Procedure for Reporting and containing data breaches

- Staff member who detects or suspects a data breach
- Complete the Data Breach Report Form and submit to their immediately line Manager and in their absence submit to the Vice President (Administration and IT)
- Line manager to assess the impact and submit the report to the Vice President (Administration and IT)
- Keep the Incident confidential as this will impact the investigation process
- Vice President (Administration should immediately take steps to contain the data breach, preserve evidence and remediate the harm
- Vice President (Administration and IT) after due assessment and submit the report with his recommendations to the Risk and Compliance Office (RCO)
- Vice President (Administration and IT) can take assistance from appropriate departments to contain the impact of the breach as timely action may contain the breach and if serious harm is not caused, it is not mandatory to notify.

Steps taken to contain the impact/harm of the breach

Data breach involves Electronic devices/records / data bases

- ❖ Isolate and quarantine the impacted data base/devises and records so that it will not impact other related records
- ❖ Shutdown the compromised systems and devices
- ❖ Ask all the staff to reset the passwords and log in credentials
- ❖ Activate the Disaster Recovery plan as envisaged in Business Continuity Management Policy and Framework

- ❖ Preserve the evidence and ensure no accidental overwriting of the evidence takes place
- ❖ Record all the messages including warning messages or pop ups which will act as an evidence

Data breach involves the loss of devices like Mobile phones / Laptops

- ❖ If possible remotedely disable the device
- ❖ Ensure the devices are protected by passwords
- ❖ Lodge a police complaint
- ❖ Call the telephone company to deactivate the SIM

Data breach due to unauthorised disclosure of personal information to third party

- Email- Recall the email from the recipient and or ask the recipient not to read and delete the email
- By Post- Call the recipient and request not to open and return the post to Bank of Baroda Sydney immediately
- Deactivate any links provided

If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security. Addressing the following questions may help you identify strategies to contain a data breach:

- ➢ How did the data breach occur?
- ➢ Is the personal information still being shared, disclosed, or lost without authorisation?
- ➢ Who has access to the personal information?
- ➢ What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

Procedure for Investigation and internal reporting into the incident

- After receiving the Data Breach Report from the VP (Administration and IT), RCO must notify to Chief Executive Officer, Head (International Banking) and Compliance International
- Assess the impact and what remediation measures have been taken by the Business head or VP (Administration and IT) and assess whether any further action required
- Investigate as to what caused the breach, collect evidences for record keeping and prepare a report to be submitted to CEO, BCC and Compliance International

- RCO must make initial assessment as to whether the incident is a data breach and if so whether it is a eligible data breach
- RCO must make a Risk assessment based on:-

  a. Number of individuals or entities affected by the breach or suspected breach

  b. Type of information compromised

  c. Likelihood of serious harm to affected persons

  d. What caused the problem – whether it is a systemic or due to individual wilful or negligence

  e. Whether remedial measures have successfully prevented serious harm to the impacted individuals or entities.

- RCO to prepare a detailed report and submit to CEO, Head (International Banking) and Compliance International

Step 2: ASSESSMENT

After determining the data breach will cause serious harm to individuals, CEO of Bank of Baroda Sydney will appoint a Data Breach Response Group (DBRG) that will consists of

1. Chief Executive Officer
2. Vice President (Administration and IT)
3. Risk and Compliance Officer

CEO may co opt if required 4. External Legal council

CEO will convene a meeting of the DBRG as soon as possible to further determine:-

a. Whether the data breach is likely to result in serious harm to the affected individual or individuals

b. Whether mandatory notification to OAIC and affected persons are required

c. To decide whether voluntary notification is advisable if it is not mandatory

In making the assessment the following factors to be taken in to account:-

1. Type of personal information involved
2. Relevance of the affected information and the breach
3. Risk of serious harm to affected individuals
4. Cause, extent and impact of the breach
5. Reputational Risk involved

Meeting of DBRG will be either in person or via a secure teleconference.

Chief Executive Officer and in consultation with VP (Administration and IT) will determine whether the breach is a Eligible Data Breach. This will be taken based on the assessment and findings of the DBRG.

If the breach is assessed to be a Non Eligible Data Breach, RCO will record this incident in the Risk Register of Bank of Baroda Sydney and close the Report. This may involve voluntary notification to OAIC and to the affected individuals.

Record Keeping and Evidence Preservation

- To preserve all records and evidence of the data breach
- Record of preliminary investigation
- Copy of the Data Breach Report lodged by the staff member
- Report of the DBRG
- Close out report and if feasible copy of the Risk Register

This should be preserved to satisfy OAIC in case of any investigation and comply with statutory and legal obligation. All the matters should be kept highly confidential.

Step 3: NOTIFY

Bank of Baroda Sydney will notify OAIC and the affected individual or individuals. DBRG will prepare a draft notification to OAIC using the OAIC Notification Template provided in the website

Procedure for Notifying OAIC – Information requirement of Part A of the OAIC notification

1. Identity and contact details of BOB Sydney
2. Description of the Data Breach
3. Type of information that has been compromised
4. BOB Sydney's suggestions and steps that should be taken by the individuals to protect the information

Information requirement of Part-B (optional)

1. Number of individual affected
2. Additional information about steps taken as a response to the breach
3. Other information to assist OAIC in determining whether appropriate process has been followed.

Website details to online access the form: https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

Notification must be sent to the OAIC by email to enquiries@oaic.gov.au

The acknowledgement of the receipt of this report form should be preserved and forwarded to CEO, DBRG, Head (International Banking) and Compliance International. Also efforts to be made in phoning OAIC and getting confirmation

Procedure for Notifying affected Individuals

DBRG must prepare a draft notification to affected individuals. The notification to affected individuals must include:-

a. How and when the data breach occurred?

b. When it was detected?

c. Type of personal information that is likely compromised

d. Steps taken by BOB Sydney to mitigate the harm and steps to prevent further damage or harm

e. Extent of information data breach and likely impact

f. Steps that individuals should take to protect themselves and what BOB Sydney will do to assist

g. Contact details of Bank of Baroda to seek assistance

h. Information regarding notification to OAIC

i. Procedure to lodge a complaint to OAIC

Chief Executive Officer is responsible to forward the notification to individuals.

Record should be kept by BOB Sydney as to the date and time and method of notification to affected individuals and any confirmation of receipt of this notification as a proof for record keeping.

ADDITIONAL NOTIFICATION

BOB Sydney may have to notify additional people as follows and this will be determined by DBRG:-

Type	**Instance**
Internal Staff	Widespread discussion between staff of BOB Sydney
Law Enforcement Agencies	If the breach involves unauthorised access, wilful act of any staff or individuals or any criminal activity

Service Providers and Cyber security providers	Extent of data breach and whether it involves any negligence due to the faulty product or service level of the provider
Regulators	APRA, ASIC and ATO if it involves financial information

Step 4: REVIEW

Once steps 1 to 3 have been completed, BOB Sydney should review and learn from the data breach incident to improve its personal information handling practices. This might involve:

- a security review including a root cause analysis of the data breach
- a prevention plan to prevent similar incidents in future
- audit to ensure the prevention plan is implemented
- a review of policies and procedures and changes to reflect the lessons learned from the review
- changes to employee selection and training practices
- Review of service delivery partners that were involved in the breach.
- Updating security measures
- Reviewing data breach response plan
- Adequacy of data protection or service level agreement with the security providers
- Reviewing strength of physical security control like video camera etc.,
- Review of privacy clause

Data breach response plan quick checklist

Information to be included Yes/No Comment	Yes / No	Comment
What a data breach is and how staff can identify one		
Clear escalation procedures and reporting lines for suspected data breaches		
Members of the data breach response team, including roles, reporting lines and responsibilities		

Details of any external expertise that should be engaged in particular circumstances		
How the plan will apply to various types of data breaches and varying risk profiles with consideration of possible remedial actions		
An approach for conducting assessments		
Processes that outline when and how individuals are notified		
Circumstances in which law enforcement, regulators (such as the OAIC), or other entities may need to be contacted		
Processes for responding to incidents that involve another entity		
A record-keeping policy to ensure that breaches are documented		
Requirements under agreements with third parties such as insurance policies or service agreements		
A strategy identifying and addressing any weaknesses in data handling that contributed to the breach		
Regular reviewing and testing of the plan		
A system for a post-breach review and assessment of the data breach response and the effectiveness of the data breach response plan		