# **ANZGOG DATA BREACH RESPONSE PLAN**

The purpose of the ANZGOG Data Breach Response Plan (the **Plan**) is to outline the procedures ANZGOG staff are required to follow to identify and respond effectively in the event a data breach occurs (or a data breach is suspected to have occurred). It includes:

* Roles and responsibilities of staff/contractors and expert partner organisations, *(e.g. legal, IT, communications)*; and
* Key steps to take when a data breach occurs.

This Plan is intended to enable ANZGOG to:

* Contain, assess and manage data breaches promptly;
* Limit the consequences of a data breach – in terms of the risk of serious harm to individuals, and financial or reputational damage to ANZGOG;
* Meet its obligations under the *Privacy Act 1988 (Cth)* (**Privacy Act**) and relevant State and Territory laws, including the *Health Records and Information Privacy Act 2002 (NSW)* and the *Health Records Act 2001 (Vic)*; and
* Preserve public trust in ANZGOG.

# **Type of data ANZGOG collects**

ANZGOG engages with a broad range of people through the course of its day to day operations.

*Examples include:*

* *Employees;*
* *Health professionals and researchers;*
* *Research study participants;*
* *Donors / fundraisers;*
* *Suppliers;*
* *Volunteers – fundraisers, advocacy, events; and*
* *Online users.*

ANZGOG has a responsibility to protect the security and privacy of individuals’ personal information from misuse, interference and loss, and from unauthorised access.

*Examples include:*

* *identifying research data – including personal information of research participants including contact details, health data; and*
* *Financial information – including credit card details of donors.*

# **What type of information is protected by privacy laws?**

The Privacy Act and relevant State and Territory privacy laws protect “personal information”.

Personal information is defined as “information or an opinion about an identified individual, or an individual who is reasonably identifiable:

1. whether the information or opinion is true or not; and
2. whether the information or opinion is recorded in a material form or not.

Currently the Privacy Act does not protect ‘employee records’, these are dealt with separately under confidentiality laws. Employee records means a record of personal information relating to the employment of the employee for example, in relation to engagement, training and discipline.

Therefore:

1. mandatory data breach notification **does apply** to identifying information of natural persons such as donors, researchers and research participants.
2. Mandatory data breach notification **does not** apply to information such as de-identified information, information about companies and not natural persons and employee records.

# **What is a data breach?**

A data breach is defined as: ‘*unauthorised access to, or unauthorised disclosure of personal information, or loss of personal information where unauthorised access to, or unauthorised disclosure of, the information is likely to occur’.* For the purposes of this Plan, a data breach occurs when information held by ANZGOG is subjected to unauthorised access, lost, disclosed or modified.

*Examples include:*

* *Malicious breach – e.g. someone hacking into ANZGOG’s computer system or unauthorised access to databases &/or credit card details in the workplace, such as an employee browsing sensitive customer records without a legitimate purpose;*
* *Accidental loss - e.g. IT equipment/hard copy documents left on public transport by an employee; and*
* *Negligent disclosure – e.g. an organisation, whether intentionally or unintentionally, makes personal information accessible; or visible to others outside the organisation and releases the information from its effective control in a way not permitted by the Privacy Act, such as an employee accidentally publishing a confidential data file with personal information of one or more individuals on the internet.*

# **ANZGOG’s responsibility to secure personal information**

ANZGOG must collect, use and disclose personal information ***held*** by ANZGOG in accordance with the 13 Australian Privacy Principles contained in the Privacy Act that set out entities’ obligations for the management of personal information.

ANZGOG holds personal information if it has ***possession or control*** of a record that contacts personal information.

This includes taking such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss and from unauthorised access, modification and disclosure.

All employees are required to take reasonable steps to protect personal information held by them on behalf of ANZGOG, including securing passwords and safekeeping information whilst not in the office, including on personal devices such as mobile phones or iPads.

If you keep personal information of ANZGOG on your personal devices and there is a data breach of those devices, then this policy applies.

# **What is a notifiable data breach?**

ANZGOG is committed to managing any data breach incidents in accordance with:

* It’s obligations under the Privacy Act and any reporting requirements outside of the Privacy Act; and
* The requirements of the Notifiable Data Breaches (NDB) scheme (In Part IIIC of the Privacy Act) which requires ANZGOG to notify individuals and the Australian Information Commissioner about ‘eligible data breaches’.

The primary purpose of the NDB scheme is to notify individuals if their personal information is involved in an ‘eligible data breach’ so that they can take steps to minimise the risk of harm to themselves. From 22 February 2018 mandatory notification of serious data breaches is required.

An ‘eligible data breach’ requires each and all of the following:

1. a data breach (as described above); and
2. a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; and
3. ANZGOG is unable to implement remediation action to avoid serious harm.

# **How do you become aware of a data breach?**

ANZGOG has a number of procedures in place to identify as soon as possible when a data breach occurs.

*Examples include:*

* *Contractual notification obligations with third parties in the event of a breach, e.g. IT, database operators, clinical trial operators;*
* *Staff report a loss;*
* *Operational procedures, e.g. information handling procedures, regular reviews and spot-checks of ANZGOG’s procedures; and*
* *Audits.*

All contracts with organisations which hold or have access to personal information on behalf of ANZGOG should have a data breach notification clause and all such contractors should be required to report relevant data breaches to ANZGOG.

# **What do you do if you suspect or are aware of a data breach?**

If you suspect or are aware of a data breach or you are informed of a suspected or actual data breach, you are required to:

1. act quickly to remediate the risk; and
2. notify the Privacy Officer/CEO as soon as possible; and
3. provide reasonable details of the breach and assistance in investigating the data breach.

The Privacy Officer will then make an assessment as to whether or not the data breach should be notified.

*For example, if you accidentally send an email with personal information to the incorrect address, ring the recipient and ask them to delete the email without reading and then notify the Privacy Officer.*

Recalling emails only works on the internal email system.

# **What is serious harm?**

In assessing whether or not a data breach would likely to result in serious harm, you should consider the following:

* the kind or kinds of information;
* the sensitivity of the information;
* whether or not the information is protected by one or more security measures and if so the likelihood that those security measures will be overcome;
* the persons, or the kinds of persons, who have obtained, or who could obtain, the information;
* if security technology or methodology is used, the likelihood that those security technology or methodology could be circumvented;
* the nature of the harm; and
* other relevant maters.

*Examples include:*

* *Financial fraud - e.g. unauthorised credit card transactions or credit fraud;*
* *Identity theft – e.g. unauthorised access to an individual’s Driver’s Licence, Medicare details; and*
* *Family violence - e.g. unauthorised access to an individual’s home address.*

Whether serious harm is likely is determined from the perspective of a reasonable person (in ANZGOG rather than from the perspective of the person whose information has been breached) deciding if the data breach would be likely to result in serious harm to an individual whose personal information was part of the data breach.

The phrase ‘likely to occur’ means the risk of serious harm is more probable than not (rather than possible).

The OAIC has provided some guidance on serious harm in its publication ‘Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)’, which is available at: <https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response>

The OAIC gives the following example:

CareHeeps, a claims management service provider, regularly sends updates to its clients about the status of the workers compensation claims of their employees. Because of human error, an employee of CareHeeps accidentally sends an email with an attachment about the employees of Business A to another client, Business B. The attachment contains the personal information of 200 employees of Business A, and includes their name, address, date of birth, and health information about their claimed injury.

A CareHeeps employee realises the error, and contacts Business B to delete the email with the attachment. Business B confirms that one of its employees accessed the file without initially realising the error, but provides written confirmation that it has since deleted all copies of the email and attachment. The employee who accessed the file has also undertaken not to divulge the information. CareHeeps’ assessment of the remedial action taken concludes that, while the file included sensitive information about the individuals’ health, its contractual arrangements with Business B and the written assurance provided by Business B has prevented the likely risk of serious harm to any individuals. As a consequence, CareHeeps determines that it is not an eligible data breach that needs to be notified to individuals or the Commissioner.

# **Why notify individuals if there is an eligible data breach?**

The NDB scheme has a practical purpose: once notified about a data breach, individuals can take steps to reduce their risk of harm.

*Example: an individual can change passwords to compromised online accounts and be alert to identity frauds or scams.*

The NDB scheme also boosts entities’ accountability for privacy protection.

# **Responding to data breaches**

When a data breach is identified or is suspected to have occurred ANZGOG will follow the notifiable data breaches response process (as set out by the Office of the Australian Information Commissioner (OAIC)) and outlined in Attachment 1 and detailed below.

Note the circumstances of each data breach incident is unique and the response needs to be dealt with on a case by case basis, with an understanding of the risks posed by a particular breach and the actions that would be most effective in reducing or removing these risks.

Generally when a data breach occurs the timely response, to mitigate potential harm to affected persons, follows these four key steps:

*Step 1:* ***Contain*** *the breach and do a preliminary assessment*

*Step 2:* ***Assess/Evaluate*** *the risks associated with the breach*

*Step 3:* ***Notify*** *affected individuals and relevant entities*

*Step 4: Prevent future breaches through* ***follow up review*** *actions*

When an ANZGOG staff member or contractor becomes aware of or suspects a data breach has occurred, they must immediately notify their manager who will assess the risk, document the incident and report to the Privacy Officer/CEO within 24 hours.

*In reporting a breach/suspected breach, include details such as:*

* *How did the breach occur?*
* *How was the breach discovered, by whom and when;*
* *When and where the breach happened;*
* *Type of information involved;*
* *Is the personal information still being shared, disclosed or lost without authorisation?*
* *Who has access to the personal information?*

The Privacy Officer/CEO will notify the Audit Risk & Compliance Committee (and other members of the Board as required) of data breaches believed &/or suspected to be eligible breaches.

Depending on the nature of the breach, the Privacy Officer/CEO may appoint a staff member or a response team with appropriate technical expertise (*e.g. legal advice, IT managers, security, media management, data forensics, clinical team)* to assist with the response process.

*Requirements under agreements with suppliers/third parties*

Third parties/suppliers are required to protect data by storing and using data in accordance with the obligations outlined in their agreement with ANZGOG, as well as in accordance with their legal obligations under the Privacy Act.

If ANZGOG or one of ANZGOG’s suppliers/third parties become aware of or suspect a breach of the data protection agreement has occurred, ANZGOG must be advised and ANZGOG will initiate its response plan process.

*Refer to:*

* Attachment 1: Data Breach Response Process

**STEP 1 - CONTAIN**

The delegated response team or staff member will take immediate action to contain the suspected/ known breach where possible and to limit any further access or distribution of the personal information.

*To help identify strategies to contain a data breach consider:*

* *What information is involved?*
* *How did the breach occur?*
* *What is the extent of the breach?*
* *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/disclosure, and reduce the risk of harm to affected individuals?*

*Examples of steps to contain a data breach include:*

* *Recover the lost information before it is accessed;*
* *Stop the unauthorised practice;*
* *Revoke or change computer access privileges;*
* *Shut down the system that was breached; and*
* *Alert site security.*

Retain any evidence that may help identify the cause of the data breach or be valuable in addressing all risks posed to the individuals or the entity.

**STEP 2 - ASSESS**

The delegated response team or staff member will promptly assess the data breach to understand the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

*For an effective assessment, gather and evaluate as much information about the data breach as possible, consider:*

* *Type of personal information involved (e.g. sensitivity of the data involved)*
* *Circumstances of the data breach including its cause & extent, for example:*

*- What was the source of the breach? (e.g. risk of harm may be lower where the source of the breach is accidental rather than intentional;*

*- Is there a systemic problem or an isolated incident?*

*- Who may have had access to the information? (e.g. is security technology used to make the data unidentifiable/inaccessible, and if so the likelihood that technology could be circumvented)*

*- The person or kind of persons who have or could obtain the information;*

* *What are the harms to affected individuals that could potentially be caused by the breach?*
* *If this harm can be removed through remedial action; and*
* *Assess the risk of other harms, including to ANZGOG such as loss of public trust, reputational damage, legal liability.*

Take remedial action to reduce any potential harm to individuals.

*For example, change access controls on compromised data before unauthorised access can occur.*

If there are reasonable grounds to *believe* *that ANZGOG has* experienced a data breach likely to result in *serious harm* to any of the individuals whose information was involved, then ANZGOG must notify *(- refer to Step 3: Notify)*.

If there are grounds to *suspect ANZGOG may* have experienced an eligible data breach, a prompt assessment of the data breach must take place.

Under the NDB scheme, ANZGOG is required to assess ‘suspected’ eligible data breaches and take reasonable steps to complete the assessment within 30 days, and endeavour to complete the assessment as quickly as possible, as the risk of serious harm to individuals often increases with time.

The time and effort invested in the assessment should be proportionate to the likelihood of the breach and its apparent severity. The assessment is the basis for deciding what actions to take.

**STEP 3 - NOTIFY**

The delegated response team or staff member will submit its assessment of the breach to the Privacy Officer/CEO who will notify the Audit Risk & Compliance Committee (and other members of the Board as required) of breaches believed &/or suspected to be eligible breaches.

If the breach meets criteria for an eligible data breach under the NDB scheme, it may be mandatory to notify the Australian Information Commissioner and individuals affected by the breach (and also other agencies, if necessary under other data protection obligations).

If ANZGOG determines the data breach is likely to result in serious harm to individuals, ANZGOG will:

1. Coordinate its notification and review response through the Privacy Officer/CEO
2. Provide a statement to the Australian Information Commissioner (using the OAIC resources available on the [OAIC website](https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify)), (and refer to Attachment 2), and containing:
   * 1. A description of the breach;
     2. The kind of information concerned; and
     3. Recommended steps for individuals.
3. Implement one of the following options to notify:
   * 1. all affected individuals;
     2. individuals at risk of serious harm;
     3. publish a statement on ANZGOG’s website and publicise it (this option only if the first two options are impractical).

The notification will include the same details ANZGOG provided in the statement to the Australian Information Commissioner, including:

* ANZGOG’s contact details;
* A description of the data breach ANZGOG has reasonable grounds to believe has occurred;
* The kind of information concerned; and
* Recommendations about the steps individuals should take in response to the eligible data breach.

1. Notify other third parties as appropriate, *e.g. the Police, ANZGOG’s insurance providers, financial institutions.*

If there has been a data breach, ANZGOG may also have to report the data breach as a contractual obligation, for example to a funder or sponsor.

*Refer to:*

* Attachment 2: What to include in an eligible data breach statement
* Also available online at: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/what-to-include-in-an-eligible-data-breach-statement> ; and
* [Notifiable Data Breach Form (online smart form)](https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB)
* Data breach preparation and response: A guide to managing data breaches in accordance with the *Privacy Act 1988* (Cth), which is available at: <https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response>

**STEP 4 - REVIEW**

The Privacy Officer/CEO will oversee any follow up actions post-breach assessment and/or notification to prevent future breaches.

The Privacy Officer/CEO in conjunction with delegated response team/staff member and ANZGOG’s Audit Risk & Compliance Committee will review and learn from the breach incident to improve ANZGOG’s personal information handling procedures, and to minimise the likelihood of a similar breach occurring again.

*Examples include:*

* *Identify and address any weaknesses in data handling that contributed to the breach;*
* *Update policies and procedures as necessary;*
* *Revise staff training as required; and*
* *Update the ANZGOG Plan if necessary.*

# **Related legislation, policies or procedures**

The ANZGOG Data Breach Response Plan has been prepared in accordance with:

* Privacy Regulations;
* OAIC’s Data breach preparation and response – A guide to managing data breaches in accordance with the *Privacy Act 1988* (Cth), February 2018, which is available at: <https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response>;
* ANZGOG Human Resources Policy and employment contracts;
* ANZGOG Privacy Policy; and
* In consultation with ANZGOG’s CEO and staff.

# **Responsibilities**

Responsibility for privacy management is shared across ANZGOG. Everyone has a part to play.

**All staff / contractors**

* All staff and contractors have a responsibility to notify their direct line manager (copying in the CEO) of any data breaches and report/escalate as required; and
* If delegated, staff are to respond to the matter, ensure all follow up action is completed, and provide details of the action taken in writing within 14 days.

**Team leaders**

* Escalate any data breaches to the CEO as soon as possible and consult within 24 hours as to the response to contain and assess the data breach risk; and
* Responsible, by area of responsibility, to ensure all follow-up action is completed and documented and submitted to the CEO.

**Communications Manager**

* Responsible for developing a clear communications strategy in response to any data breach, including the Statement to OAIC Commissioner (using the approved Notifiable Data Breach Form online smart form) – refer to Attachment 2) for any notifiable breaches; and the strategy for notifying individuals and/or publishing a statement online and publicising it.

**CEO**

* Responsible for training staff on the Data Breach Response Plan (including any updates to the Plan) and ensuring all appropriate procedures are in place;
* Investigate and report any data breaches; and escalate to ANZGOG’s Audit Risk & Compliance Committee those breaches believed or suspected to be eligible breaches;
* Responsible for reviewing any data breaches reported by ANZGOG staff, advising staff as to the response required *(e.g. assessment as to whether it is a notifiable data breach),* and determining whether it is a notifiable data breach;
* Oversee agreed data breach response;
* Evaluate how any data breaches occurred and the success of the response, including any strategic implications to improve the effectiveness of the Plan; and
* Oversee any follow up actions post-breach assessment, *(e.g. required updates to the Plan, additional training for staff, and revised contracted obligations)*.

**ANZGOG Audit Risk and Compliance Committee**

* Responsible for reviewing any data breaches reported by ANZGOG’s Privacy Officer/CEO along with the recommended actions; and approving data breach response process, including notification strategy;
* In conjunction with the Privacy Officer/CEO, review and learn from the breach incident to improve ANZGOG’s personal information handling procedures, and to minimise the likelihood of similar incidents in the future; and
* Supervise an internal audit of the Plan to ensure the plan is implemented, including any updates.

# **Documentation**

The delegated response team or staff member will:

* Be careful not to destroy any evidence that may help identify the cause of the data breach or be valuable in addressing all risks posed to the individuals or the entity.
* Document and keep records of the data breach/suspected breach, including the steps taken throughout the response process to contain, assess, notify and review the data breach incident.

# **Timeframe and Review**

This plan is to be reviewed under the approval of the Audit Risk and Compliance Committee:

* Every two years;
* In the event of legislative changes; and
* In the event of a data breach incident, to review the effectiveness of the Plan.

# **Compliance with this Plan**

ANZGOG is committed to maintaining the highest standards of conduct. Every staff member is responsible for maintaining standards that inspire public confidence and trust in ANZGOG’s work.

If you are unsure of the appropriate course of action in a particular circumstance covered by this Plan, discuss the matter with your supervisor.

Failure to comply with this Plan may lead to disciplinary or remedial action.

If you are aware of a breach of this policy notify your supervisor.

# **Contact**

For further information, please contact the Privacy Officer at [insert].

# **Attachments**

|  |  |
| --- | --- |
| **Attachment** | **Document Name** |
| 1 | Data Breach Response Process (as set out by OAIC) |
| 2 | What to include in an eligible data breach statement (as set out by OAIC) |
| 3 | ANZGOG’s Key Contacts |