12 MAY 2026 9 MIN READ

OAIC Notifiable Data Breach Scheme on AWS: The Australian Playbook

Australia's NDB scheme gives you 30 days to assess and notify a suspected data breach. The clock is forgiving but the standard is not — this is the practical playbook for AWS workloads in ap-southeast-2 and ap-southeast-4.

AWS INCIDENT-RESPONSE OAIC NDB PRIVACY-ACT AUSTRALIA REGULATORY

TL;DR

Australia's Notifiable Data Breach scheme gives APP entities **up to 30 days to assess** whether a suspected breach is an "eligible data breach," then requires notification to OAIC and affected individuals "as soon as practicable" after the assessment concludes. The deadline is forgiving by APAC standards, but the post-Optus, post-Medibank regulatory environment is not. The risk on this clock is not running out of time — it is conducting a substandard assessment, under-notifying, or missing affected individuals. This guide covers the eligibility test, the assessment process on AWS, and the operational changes that distinguish a credible response from one that draws OAIC scrutiny.

What is the NDB scheme?

The Notifiable Data Breach scheme sits in **Part IIIC of the Privacy Act 1988** and has been in force since 22 February 2018. It is administered by the **Office of the Australian Information Commissioner (OAIC)**.

The scheme imposes two duties on APP entities:

1. **Assess** any suspected eligible data breach within 30 days of becoming aware of grounds to suspect one
2. **Notify** OAIC and affected individuals "as soon as practicable" after reasonable grounds to believe an eligible breach has occurred

Three details determine how the obligation actually applies:

- **The 30 days is for the assessment, not the notification.** OAIC's expectation is that you start notifying as soon as you have reasonable grounds to believe — running the full 30 days as a buffer is exactly what regulators are suspicious of after Medibank.
- **"Eligible" is a three-limb test, all of which must be satisfied.** Unauthorised access, disclosure, or loss; likely to result in serious harm; and you have not prevented the harm through remedial action. Failing any one limb means the breach is not notifiable — but you should still document the assessment.
- **The post-2022 penalty regime has teeth.** Maximum civil penalties for serious or repeated interference with privacy are now the greater of AUD $50 million, three times the benefit obtained, or 30% of adjusted turnover. OAIC has not been shy about using them.

Which incidents are likely to be eligible data breaches?

The NDB scheme does not enumerate categories the way CERT-In does. Eligibility is determined case-by-case against the serious harm test. Mapping common AWS-side scenarios to NDB exposure:

AWS-side incident	Likely eligible?	Primary detection sources
S3 bucket misconfiguration exposing customer records	Almost always	Macie, GuardDuty S3 findings, AWS Config
Compromised IAM credentials with database access	Yes if customer PII accessed or exfiltrated	GuardDuty IAM findings, CloudTrail data events, VPC flow logs
Ransomware on EC2 holding personal information	Usually yes, even if data was not exfiltrated (availability harm)	EDR on EC2, CloudWatch, GuardDuty malware findings
Phishing-driven account takeover	Yes if account had access to personal information	GuardDuty, IAM Access Analyzer, CloudTrail
Lost backup tape from on-prem to AWS migration	Yes if encrypted-with-known-key or unencrypted	Outside AWS — process gap
Third-party vendor breach affecting shared data	Yes for your share of the data	Vendor notification + CloudTrail integration logs
Public-facing API leaking PII through enumeration	Yes — and OAIC takes a dim view of these	WAF, CloudFront real-time logs, ALB access logs
Encrypted database snapshot exfiltrated with key separately secured	Usually no — remedial action prevents harm	CloudTrail S3 + KMS data events

The last row matters. The eligibility test explicitly considers whether the entity has prevented serious harm through remedial action. Strong encryption with effective key management can move a breach from notifiable to not-notifiable — but only if you can demonstrate the remedial action was effective, with evidence.

The NDB assessment timeline on AWS

Unlike CERT-In or MAS TRM, NDB does not impose an hour-by-hour clock. The relevant timeline is measured in days. A defensible assessment for an AWS-side incident usually looks like this:

Day 0 — Suspicion. Some signal triggers awareness that an eligible breach may have occurred. Examples: a GuardDuty critical finding, a customer report, an internal audit observation, a vendor notification. *Document the timestamp — this is your t=0 for the 30-day clock.*

Days 0–2 — Initial scoping. Confirm whether personal information was involved, identify affected systems and accounts, snapshot evidence. Pull CloudTrail and Macie findings for the relevant window. Decide whether to engage external IR support.

Days 2–7 — Technical investigation. Establish what was accessed or disclosed, by whom, when, and for how long. Quantify the number of individuals affected and the categories of personal information involved. This is the analytical heart of the assessment.

Days 5–10 — Serious harm analysis. Assess each category of information against the harm test. Health information, financial information, identity documents, and combinations that enable identity theft carry the highest harm risk. Demographic information alone usually does not.

Days 7–14 — Remedial action assessment. Determine whether any action taken — credential rotation, encryption-at-rest, MFA enforcement after the fact — prevents the serious harm that would otherwise arise. Document the reasoning. This is where notifiable breaches sometimes become not-notifiable.

Days 10–20 — Decision. The accountable person (usually the privacy officer, with legal counsel and the CISO) decides whether the breach is eligible. Document the decision and the supporting reasoning.

Days 14–25 — Notification preparation. If notifiable, draft the OAIC notification and the individual notifications. Map individuals to contact methods. Decide between direct individual notification and publication if direct notification is not practicable.

Days 20–30 — Notification. Submit to OAIC via the online form on oaic.gov.au. Send individual notifications. Begin public communications if required.

The timeline above is illustrative — many incidents move much faster, and a clearly serious breach (large volume, sensitive data, public attention) should be notified well inside two weeks. The 30 days is an outer limit for the worst-case investigative complexity, not a default.

Pre-incident hardening — what to set up now

Four AWS-specific items consistently separate organisations that handle NDB cleanly from those that draw OAIC follow-up.

1. PII inventory in AWS

You cannot run a serious harm analysis if you do not know what personal information you hold or where. The mechanism on AWS is **Amazon Macie** for S3, plus an inventory of databases and their schemas held in a security-managed wiki or CMDB:

- Macie enabled on every account holding personal information, scanning all customer-data buckets
- A documented inventory of RDS, DynamoDB, and DocumentDB tables containing PII, with the categories of information in each
- Tagging discipline — every resource holding PII should carry a `data-classification: pii` tag, enforced via SCP or AWS Config rule

Without this, your Day 0–2 scoping turns into a two-week archaeology project.

2. CloudTrail data events on PII-bearing storage

Default CloudTrail captures management events. **Data events** (S3 object-level operations, DynamoDB item-level operations, Lambda invocations) are opt-in and cost extra. For NDB readiness, enable data events on every storage resource holding personal information. The cost is small. The difference between "we know who accessed which records" and "we know someone with these credentials made some S3 calls" is enormous in a serious-harm assessment.

3. KMS key separation

The remedial-action limb of the eligibility test is most powerful when the data was encrypted and the encryption keys were not part of the breach. On AWS this requires deliberate KMS architecture:

- Customer master keys for production data held in a separate AWS account from the workloads that use them
- Key access via IAM role assumption with short-lived sessions
- KMS key usage logged via CloudTrail data events
- Documented key rotation and access review

A compromised application IAM role that *could decrypt* data is not the same as a compromised application that *had decrypted data in memory*. The forensic distinction matters for the harm analysis.

4. Privacy impact assessment artefacts

OAIC and external parties looking at a breach response will ask what you knew about the data before the incident — what was collected, why, on what legal basis, how long retained, who had access. Privacy impact assessments are not technical, but they are what enables a credible serious-harm analysis. Maintain PIAs for every system handling personal information, refreshed annually.

AWS region selection and Australian considerations

Australia has two AWS regions: **ap-southeast-2 (Sydney)** since 2012, and **ap-southeast-4 (Melbourne)** since 2024. Three IR-relevant points:

1. **OAIC does not require data localisation, but APP 8 imposes accountability for offshore disclosures.** If personal information is transferred to a non-AU AWS region, you remain accountable for compliance with the Australian Privacy Principles by the overseas recipient. Keeping production personal data in ap-southeast-2 and ap-southeast-4 sidesteps the question. Most regulated workloads do this anyway.
2. **Cross-region replication within Australia is recommended for resilience.** Replicating S3 buckets and database snapshots between Sydney and Melbourne gives you regional failover without engaging APP 8.
3. **IRAP-assessed AWS services.** AWS Asia Pacific (Sydney) Region has been IRAP-assessed to PROTECTED level for a substantial catalogue of services. If your organisation handles Australian Government data, this matters for the security framework underpinning your NDB process — though it does not change the NDB obligation itself.

Common mistakes

Five patterns we see repeatedly when reviewing NDB readiness for AWS workloads:

- **Treating the 30 days as a target.** OAIC's published guidance and several enforcement actions make clear that the 30 days is a maximum, not a planning horizon. Notifying on Day 28 of an obviously serious breach signals stalling.
- **Conflating "eligible" with "embarrassing."** The eligibility test is about serious harm to individuals, not reputational harm to the entity. Internal pressure to find reasons not to notify is a known governance failure mode. Document the assessment, sign it off, and notify when the test is met.
- **No PII inventory before the incident.** Building the inventory inside the 30-day window costs you two weeks you do not have.
- **Notifying OAIC without notifying individuals, or vice versa.** Both notifications are required and serve different purposes. They can be issued in parallel.
- **Under-engineering KMS for the remedial-action argument.** Encryption alone is not the answer. Encryption with documented key separation and tested key access controls is.

What to do this week

If your organisation is an APP entity with AWS workloads, three actions return the most value in the first week:

1. **Build or refresh your PII inventory.** Turn on Macie if it isn't already, document every database containing personal information, and tag the resources.
2. **Enable CloudTrail data events on PII-bearing storage.** The cost is low and the forensic value is high.
3. **Run an NDB tabletop.** Use a realistic scenario — for example, a compromised IAM access key used to query a production RDS database containing customer records. Time the assessment, not just the technical response. Find out where your Day 0–7 falls over before a real incident finds out for you.

The NDB scheme is the most forgiving APAC privacy regime in terms of pure clock time. It is also the most reputationally consequential, because the post-Optus and post-Medibank regulatory environment has made data breach response a board-level concern in Australia. Organisations that treat NDB as a 30-day countdown miss the point — the standard is the quality of the assessment, not the timing of the notification.

Related guides

- AWS Incident Response in APAC — Pillar guide — the regulatory and technical overview across Australia, Singapore, India, and ASEAN.
- Meeting CERT-In's 6-hour incident reporting rule on AWS — for organisations with Indian user exposure; often runs in parallel to OAIC notification.
- MAS TRM and AWS incident response — the Singapore FSI equivalent.
- APRA CPS 234 notification obligations for AWS — the Australian FSI parallel with a 72-hour clock, frequently runs alongside NDB. *Coming soon.*
- Managed Detection and Response — Opcode's MDR service includes NDB-aligned assessment workflows.