Process for identifying Mandatory Notification of Data Breach (MNDB) scheme obligations (For initial consideration and s.48 assessments)

A data breach has occurred, does it involve personal information?

Yes → MNDB scheme obligations may apply

No → MNDB scheme obligations do not apply

Gather information and determine the likelihood of serious harm, having regard to:

- The kind of personal information
- The sensitivity of the information
- Is information protected by one or more security measures?
- The likelihood measures could be overcome
- Persons (or kinds), who have obtained, or who could obtain, the personal information
- The nature of the harm likely to result from the data breach
- Depending on the circumstances, any other relevant matters, like how long information was exposed, circumstances of affected individual, how it occurred, combinations of personal information and actions taken by agency to reduce the risk of harm.

Determine knowledge, suspicion or belief of EDB and relevant obligations

Does the information indicate and/or support an Eligible Data Breach (EDB)?	Eligibility	Scheme obligations		
		Contain and mitigate	Assess	Notify
Evidence indicates only a **possibility**, (**note**: you may need to seek more information and consider containment)	Possibility			
Some evidence supporting notion of EDB. Not enough for belief, but **more than a possibility**	Reasonable suspicion	✓	✓	
Sufficient evidence to accept the notion that the breach is eligible, as opposed to rejecting it	Reasonable belief	✓		✓
Knowledge that an EBD has occurred	Knowledge	✓		✓

For more detailed information see assessment guideline and tool. Agencies should also consider non-scheme obligations.

Office of the Information Commissioner Queensland

IPOLA