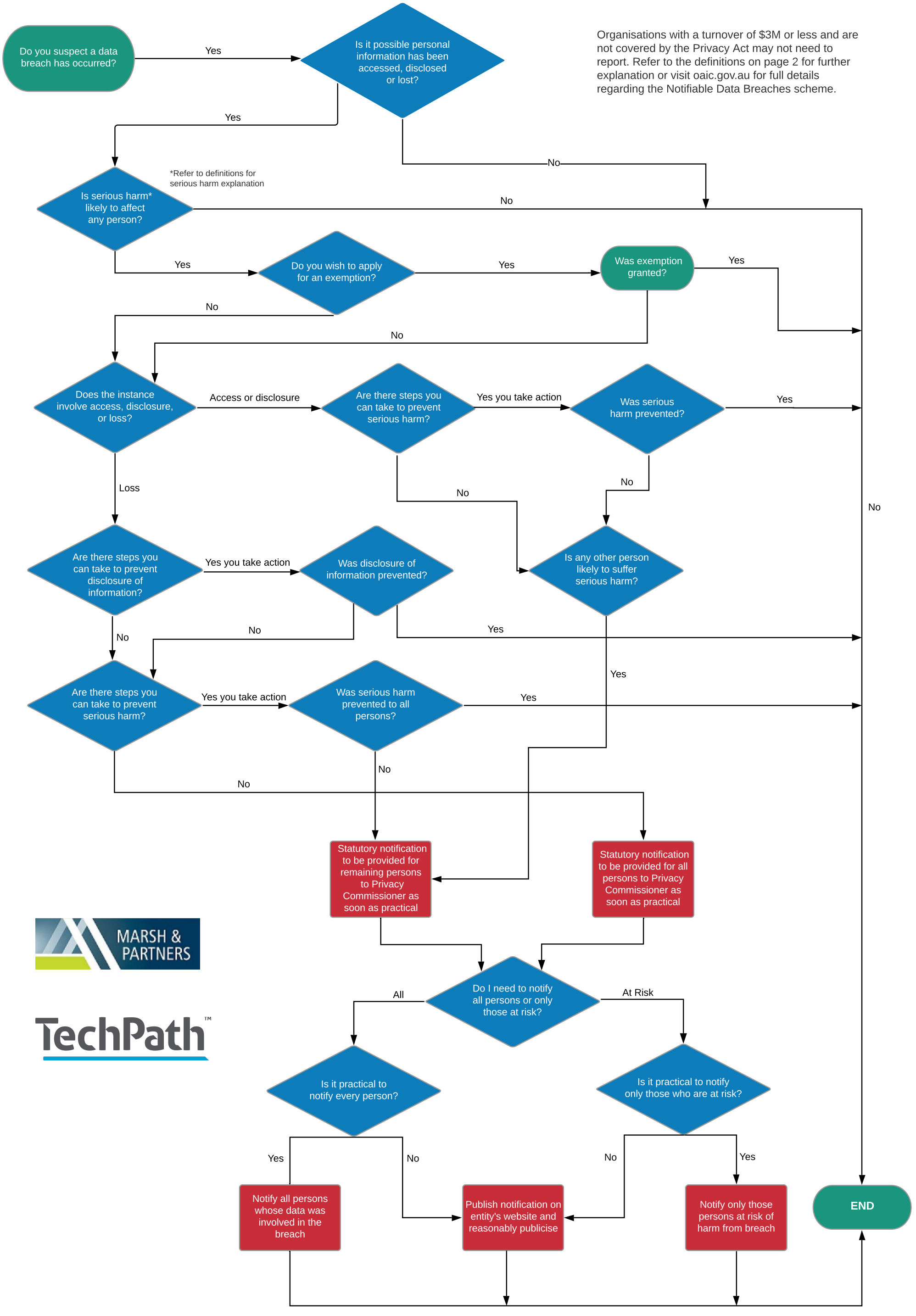
DATA BREACH NOTIFICATION FLOWCHART



Organisations with a turnover of $3M or less and are not covered by the Privacy Act may not need to report. Refer to the definitions on page 2 for further explanation or visit oaic.gov.au for full details regarding the Notifiable Data Breaches scheme.

MARSH & PARTNERS

TechPath™

DATA BREACH NOTIFICATION FLOWCHART - DEFINITIONS

Data Breach

A data breach occurs when personal information held by an organisation is **lost** or subjected to **unauthorised access** or **disclosure**.

Serious Harm

Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

Access or Disclosure

Unauthorised **access** of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking). For example, an employee browses sensitive customer records without any legitimate purpose, or a computer network is compromised by an external attacker resulting in personal information being accessed without authority.

Unauthorised **disclosure** occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity, and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity. For example, an employee of an entity accidentally publishes a confidential data file containing the personal information of one or more individuals on the internet.

Loss

Refers to the accidental or inadvertent **loss or theft** of physical devices (such as laptops and storage devices), or paper records that contain personal information, in circumstances where it is likely to result in unauthorised access or disclosure. For example, an employee of an entity leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport.

Who Needs to Report Breaches

The data breach laws apply to government agencies and private sector organisations who are currently subject to the Australian Privacy Principles under the Privacy Act. This includes private sector organisations, including not-for-profits, with an annual turnover of more than $3 million. It also includes small businesses that may be earning $3 million or less where they are a health service provider, are related to an APP entity, trade in personal information, are a credit reporting body, amongst others. There are some exceptions to the notification requirements, which relate to:

- Data breaches involving entities that hold information jointly . The entity with the most direct relationship with the individuals affected by the data breach should carry out the notification
- Enforcement related activities where the CEO has reasonable grounds to believe notifying is likely to cause prejudice
- Inconsistency with secrecy provisions. An exception may apply where the Commonwealth law prohibits or regulates the use or disclosure of information
- Declarations by the Commissioner where a NDB notification would conflict with public interest

Although a Small Business Operator (SBO) is not obligated to notify under the NDB scheme, those seeking to adopt good privacy practices and increased consumer confidence and trust are encouraged by OAIC to opt in to the Privacy Act and would therefore be obligated to report a data breach.

Please refer to oaic.gov.au for full details regarding the reporting exemptions.

How to Notify

When an agency or organisation is aware of reasonable grounds to believe an eligible data breach has occurred, they are obligated to promptly notify individuals at likely risk of serious harm. The Commissioner must also be notified as soon as practicable through a statement about the eligible data breach. This notification can be made via the 'OAIC's Notifiable Data Breach form' on the OAIC website.

For further information regarding the Notifiable Data Breaches scheme, visit oaic.gov.au

MARSH & PARTNERS

P. 07 3023 4800

www.marshpartners.com.au

TechPath™

P. 1300 033 300

www.techpath.com.au