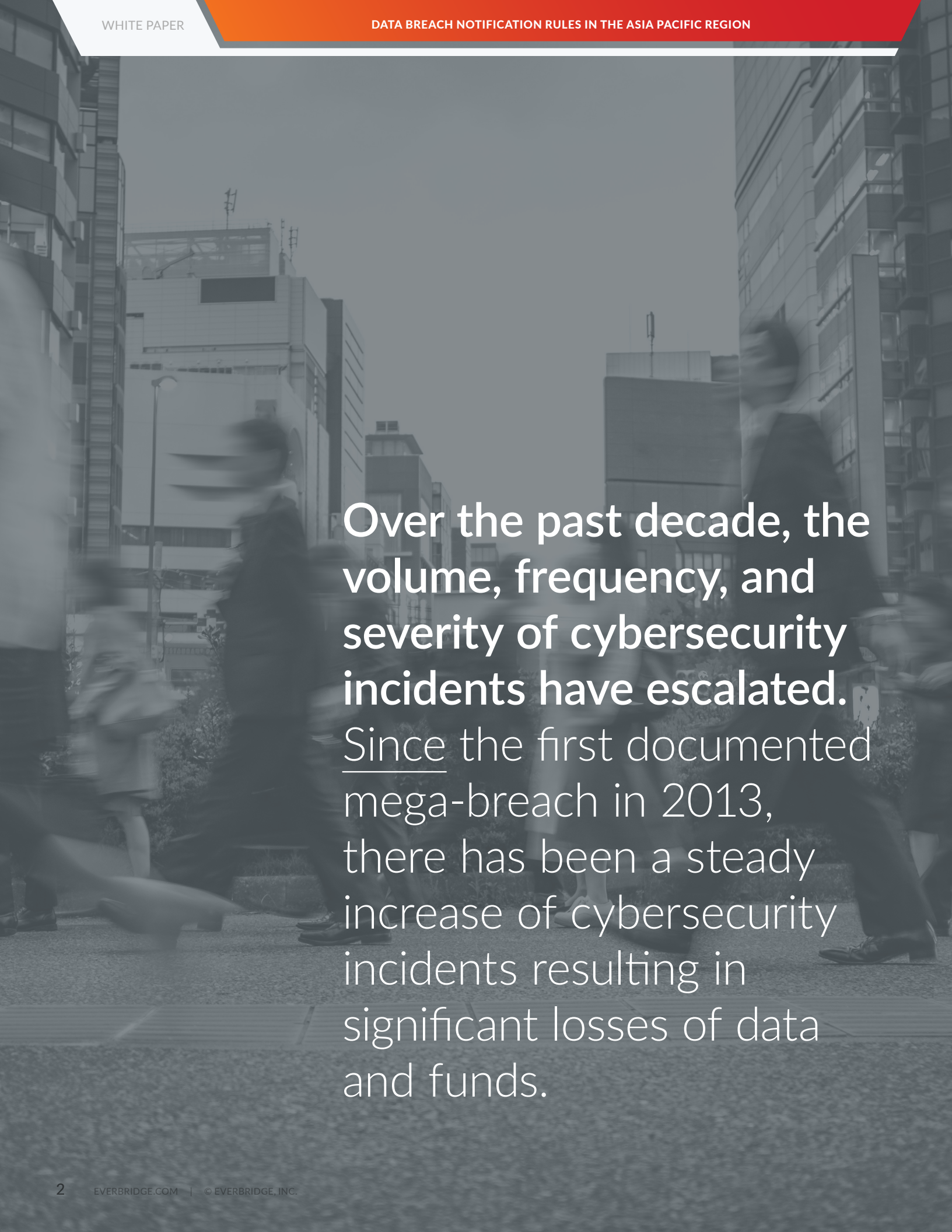
everbridge®

WHITE PAPER

Data Breach Notification Rules in the Asia Pacific Region



Over the past decade, the volume, frequency, and severity of cybersecurity incidents have escalated. Since the first documented mega-breach in 2013, there has been a steady increase of cybersecurity incidents resulting in significant losses of data and funds.

While not every account breached has had financial information compromised, the global cost of cybercrime remains staggering: conservative financial estimates tip the scale at **$1 trillion USD annually** – but studies suggest that costs could exceed **$10 trillion by 2025**.

With the frequency and severity of these attacks on the rise, many nations have experienced a noticeable impact on their gross domestic product (GDP). To combat the impact of this disruption, governments are introducing new laws and regulations addressing cybersecurity concerns. While the nuances of these laws may vary, most require organisations to notify affected users and relevant authorities should a breach occur. However, the definition of an incident requiring notification varies between countries. For example, in some jurisdictions, breaches resulting in financial losses to publicly listed companies may need to be reported to the relevant stock market, unauthorised access to user or customer information may be subject to a different reporting regime.

For global organisations, this means employing a reporting system for cybersecurity incidents built to meet specific jurisdictional obligations for each region of operation. A Critical Event Management (CEM) platform with a powerful multi-channel communication system can help ensure compliance with complex rules across various regions - keeping all relevant parties easily and rapidly informed of an incident in accordance with local laws and other obligations.

This whitepaper is designed to help you improve your cybersecurity efforts through assessing a different incident notification regime applicable to several regions across the Asia-Pacific region.

Australia

Australia has a regularly reviewed and well-developed **national cybersecurity strategy** called the Notifiable Data Breaches (NDB) scheme. The NDB scheme stipulates that organisations and agencies must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach involving personal information occurs and is likely to result in serious harm.

This reporting regime applies to all organisations subject to the **Privacy Act** 1988 and includes businesses with an annual turnover of $3 million AUD or more. Once a notifiable breach is detected, the organisation has 30 days to assess whether the data breach may result in serious harm and file a report.

Not all cybersecurity incidents involve unauthorised access to personal data. For publicly listed companies, the Australian Security Exchange (ASX) **Listing Rule 3.1** specifies that when a listed company becomes aware of information that a reasonable person would expect to affect the entity's price or value, the ASX must be informed immediately.

The Australian Government is also considering introducing specific legislation regarding notification of ransomware attacks. Although no specific laws are currently in circulation, proposed legislative reforms may require **Australian companies with a turnover** over $10 million AUD to notify the Australian Government if they are the subject of a ransomware attack.

The **Security Legislation Amendment (Critical Infrastructure) Act 2021** (SLACI Act) placed heightened security obligations on critical infrastructure providers and the requirement to report incidents to the **Australian Cyber Security Centre** (ACSC). For most of the identified sectors, including utility operators, financial market infrastructure, healthcare, and broadcasters, there are obligations to report incidents significantly impacting the availability of an asset within 12 hours. If the report is made verbally, the affected organisation must make the report in writing within 84 hours.

For incidents that have a relevant impact on the availability, integrity, reliability, or confidentiality of an asset, organisations have an obligation to report the incident to the ACSC within 72 hours.

New Zealand

New Zealand's **Privacy Act 2020** requires organisations or companies with a privacy breach that has caused or is likely to cause anyone serious harm to notify the **Privacy Commissioner** and any affected persons as soon as they are practically able.

The New Zealand Privacy Commissioner expects that breach notifications should be made to their office no later than 72 hours after becoming aware of the breach.

Unlike the data breach notification laws of many countries, New Zealand's laws have an extra dimension. A notifiable breach includes incidents where an agency loses access to information, either temporarily or permanently. So there is an obligation that businesses inform the Privacy Commissioner of a ransomware attack that limits access to data.

The critical infrastructure sector in New Zealand does not have a mandatory cybersecurity incident reporting regime. However, the **National Cyber Security Centre (NCSC)** developed the Voluntary Cyber Security Standards for Control Systems Operators (VCSS-CSO). These standards adopts best practice controls from the North American Electric Reliability Corporate (NERC) and the National Institute of Standards and Technology (NIST). It provides critical infrastructure providers in New Zealand with a set of benchmark standards they should employ.

India

CERT-In has introduced one of the most stringent data breach notification regimes in the world, exceeding the European Union's General Data Protection Rule (GDPR) and other well-regarded schemes. In India, this strict regulation introduces a six-hour reporting deadline with an obligation to retain logs for more than 180 days after an incident.

The **CERT-In directions** apply to a broad swath of organisations, such as data centre operators, virtual private server providers, cloud service providers, and VPN services. These organisations are required to maintain customer contact information and other details for five years after any contracts or agreements with customers expire.

Unlike other reporting regimes, the range of security incidents that must be reported in India are very broad: listing at least **20 different attack** types such as website defacements, targeted scanning of networks, fake mobile apps, and malicious activities on systems related to blockchain, 3D printing, and the use of drones.

Singapore

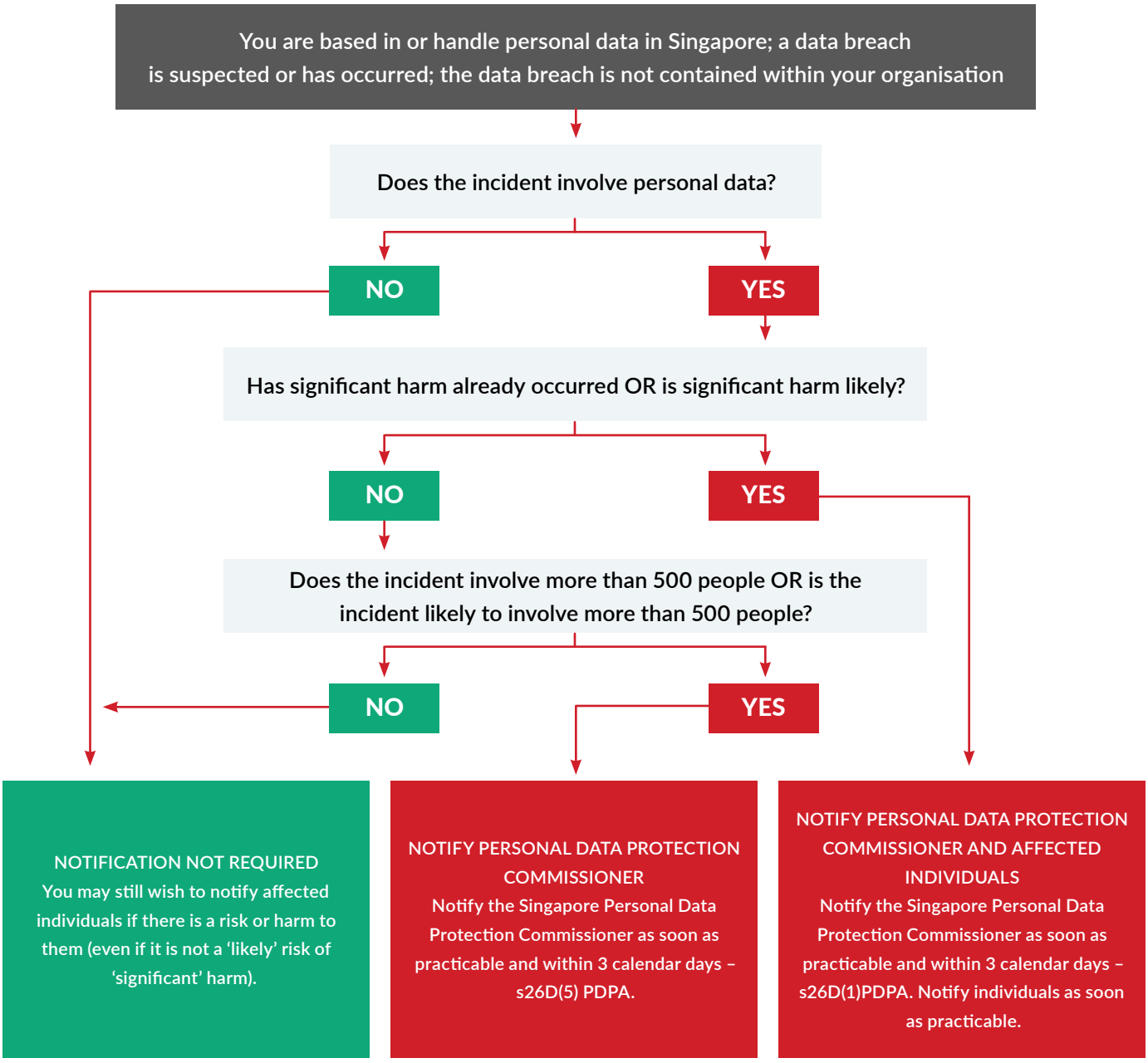
Singapore introduced mandatory data breach notification laws in **February 2021**. According to Singapore's Personal Data Protection Act 2012 (PDPA), the definition of a breach includes the unauthorized access, collection, use, disclosure, copying, modification, or disposal of personal data. In addition, the PDPA considers the loss of any storage medium or device on which personal data is stored (in circumstances where the unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data is likely to occur) a breach as well.

Like other jurisdictions, the PDPA has a reporting threshold that requires unauthorised access to data that may cause or may have caused **"significant harm."** However, if a breach does not cause or is not expected to cause significant harm but affects more than 500 people, it must also be reported.

Notifiable data breaches must be reported to the Singapore Personal Data Privacy Commissioner (PDPC) and affected individuals. Notification to the PDPC must occur within 72 hours of determining whether the data breach is notifiable: this varies from when the breach is detected.

Interestingly, even if a breach qualifies as notifiable, it may not require that a notification be sent to affected individuals. For example, if measures are taken before the breach make it unlikely that significant harm will occur, or if action is taken after the breach making it unlikely that significant harm will occur, notifications may not be required.

The Cyber Security Agency of Singapore (CSA) is currently reviewing the nation's **Cybersecurity Act (CS Act)** to enhance the cyber resilience of Critical Information Infrastructure (CII) sectors and update the Cybersecurity Code of Practice (Cup) to better deal with new and emerging threats. This review is designed to enhance the legal framework established in the CS Act established in 2018, covering physical assets such as power and water infrastructure as well as cloud and essential digital services.



Source: www.fticonsulting.com

China

China's Personal Information Protection Law (PIPL) came into effect in November 2021. The PIPL takes a broad view of the data it protects with provisions for data held in China and data held outside the country where it pertains to the provision of products and services to persons in China, the analysis/assessment of the behaviour of persons in China, and other circumstances provided by law.

The implementation of the PIPL is managed through regulations drafted by the Cyberspace Administration of China (CAC), which covers the PIPL and the country's Cybersecurity Law and Data Security Law.

The regulations stipulate that a breach of important data affecting more than 100,000 people should be reported to the CAC **within eight hours** of the breach. Following the report, the breached entity will need to provide an account of the incident within five business days regarding the source of the breach, any harm caused by the breach, and measures taken to protect against future breaches.

Japan

In Japan, the **Amended Act on Protection of Personal Information (APPI)** passed by the Japanese legislature in June 2020 and came into effect in April 2022. The AAPI covers regulations relating to offshore personal data transfers and personally referable data like web browser search history, purchase history with a retailer, and information stored in website cookies.

The Personal Information Protection Commission (PPC) must promptly receive a preliminary notification about the incident after the entity becomes aware of a breach. While the guidelines that support the APPI are vague, they explain that while "promptly" is determined case-by-case, three to five calendar days are generally appropriate.

The APPI defines four different types of incidents that are subject to the notification regime:

+ Breaches of data including sensitive data
+ Breaches of data including data that may result in an economic loss if used improperly
+ The number of data subjects at risk of breaches is more than 1,000
+ Breaches with unjust purposes

For the first three categories of a breach, the PPC must receive a second notification within 30 days. That deadline extends to 60 days for the fourth breach category. That notification must contain a summary of the incident, categories of personal data subject to the incident, and the number of data subjects whose personal data was breached. The report needs to describe the cause of the incident, any potential secondary damage, notification of data subjects, and any other information which helps the PPC understand the incident.

BREACH NOTIFICATION ACROSS THE ASIA PACIFIC REGION

Country	Legislation/Rules	Notification Periods	Notes
Australia	Privacy Act 1988 Security Legislation Amendment (Critical Infrastructure) Act 2021 ASX Rule 3.1	30 days 12 - 72 hours ASAP	Australia has specific rules for breaches of personal information and attacks on critical infrastructure. Incidents that may impact the value or share price of a listed company must be notified to the ASX.
New Zealand	Privacy Act 2020	ASAP - 72 hours	Rules cover unauthorised access to data and the inability to access data (e.g. ransomware).
India	CERT-In directions (2022)	ASAP - 72 hours	Covers a broad range of incident types.
Singapore	Personal Data Protection Act 2012	72 hours from determining the incident is notifiable	There are reporting thresholds for both types of incidents and the number of affected people.
China	Personal Information Protection Law	Eight hours	Covers data within and outside China affecting parties within China.
Japan	Amended Act on Protection of Personal Information	ASAP 30 or 60 days	Initial report to be made “promptly.” Subject to the type of incident.

Why Critical Event Management is Important

In the event of a data breach, companies must follow the appropriate regulatory regime: this includes having access to contact information for all affected parties (even if primary and operational systems can't be reached). Notifications must include the required information and be sent within prescribed deadlines to avoid potential legal action and fines for noncompliance.

The right CEM solution can store information independently of core systems and send required information within regulatory timeframes, making it a critical tool. Without, organisations may be left scrambling to find appropriate communication channels to inform those needed of a breach. By streamlining the event management process, a CEM solution helps maintain compliance by ensuring templates and communication channels are ready to use at a moment's notice.

Everbridge has a proven track record of supporting major governments, banks, airports, and critical infrastructure providers around the globe. Learn how Everbridge can help your organisation meet changing global regulatory requirements and compliance standards with our **best-in-class CEM**.

© EVERBRIDGE, INC. | EVERBRIDGE.COM 10

Let's Talk

Would you like to know more about our Digital Operations Solution? Get in touch or contact us at Apac_Marketing@everbridge.com to learn more.

About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise-grade software-as-a-service applications that automate and accelerate organizations' operational response to critical events to Keep People Safe and Organizations Running™. For two decades Everbridge has partnered with customers and grown software and service capabilities to meet their needs. Today, Everbridge provides a single unified platform that allows organizations to manage the full lifecycle of a critical event. Everbridge understands the range of threats faced by organizations and communities and how critical it is to adapt within this volatile global threat landscape. Fostering resilience can also be a competitive advantage. Everbridge specializes in five core resilience solutions to meet these needs: Business Operations, Digital Operations, People Resilience, Public Safety, and Smart Security. Over 6,200 global customers rely on the company's Critical Event Management (CEM) platform to quickly and reliable aggregate and assess thread data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes.

Click here to learn more about Everbridge and follow us on **LinkedIn** and **Twitter**.