MEDIA RELEASE

GPEN Sweep finds significant awareness of managing data breaches, concerns regarding low engagement

4 March 2020

An international privacy sweep has found that 84 percent of respondent organisations say they have systems in place for reporting data breaches, including an appointed team or group responsible for handling breaches.

Organisations that voluntarily responded to the 2019 Global Privacy Enforcement Network (GPEN) Sweep showed a significant awareness about best practices for appropriately responding to data breaches.

New Zealand Privacy Commissioner John Edwards said: “It’s encouraging to see a high-level of preparedness for data breaches from respondent agencies across the globe.”

“Privacy and data protection have gained increasing public attention in recent years. Organisations which handle personal information should get ready for New Zealand’s new Privacy Act, which will include a mandatory data breach notification requirement.”

But the results of the GPEN Sweep need to be tempered by the low response rate from organisations contacted to participate. Of the 1145 organisations approached, only 21 percent (258 organisations) provided substantive responses. Survey organisers say there are some possible reasons why the remaining organisations chose not to respond. These included potential concerns from organisations in jurisdictions with mandatory breach reporting about follow up enforcement actions if the Sweep revealed underreporting, or general concerns that responses may highlight non-compliance with data protection laws.

The results need to be read in context of the low overall response rate.

Findings

It was encouraging to note that a large percentage of organisations that responded (84 percent) across all sectors and jurisdictions had appointed a team or group responsible for managing data breaches to whom breaches should be reported.

Seventy five percent of responding organisations reported having procedures that covered key steps such as containment, assessment, evaluation of the risk associated with

breaches. Eighteen percent of responses in relation to this question indicated that their procedures were poor, suggesting that these policies could be made clearer in order to cover the key steps involved in responding to a data breach.

Sixty five percent of responding organisations rated their own procedures for preventing the recurrence of a data breach as ‘very good’ or ‘good’. However, the rest in this category had either poor procedures in place or failed to specify.

Some organisations without internal policies indicated that they relied on the guidance published by their relevant data protection authority (DPA) where needed.

One respondent described their breach assessment system, and indicated that they had implemented a red, amber, green (RAG) rating system. They stated that this takes into consideration the number of records affected, the sensitivity of the data, the distress caused, the containment or otherwise of the breach, whether the information has been recovered and whether the data was encrypted.

Data breach notification is mandatory in 12 of the 16 jurisdictions who participated in the Sweep. Almost all organisations that responded were aware of the relevant legal framework, including reporting thresholds and timeframes. Only five of those organisations demonstrated poor understanding of the legal framework.

Guidance provided by DPAs about data breach reporting was considered useful by most organisations surveyed. However, smaller organisations have struggled to absorb large amounts of guidance and lack of resourcing has prevented them from developing sophisticated data breach policies and procedures.

Falling short

Many organisations were found to fall short in terms of monitoring internal performance in relation to data protection standards, with more than 30 percent of responding organisations reporting having no programmes in place to conduct self-assessments and/or internal audits.

Only 45 percent of the organisations that responded indicated that they maintain up-to-date records of all data breaches or potential breaches.

Background

The GPEN Annual Sweep (the GPEN Sweep) this year considered how organisations in various jurisdictions handle and respond to data breaches.

Given the mass of information that is collected and held by organisations, it is inevitable that at certain times personal information will be accessed, disclosed, or otherwise acquired in a way that is not authorised. How an organisation responds to a data breach incident (including both notification as a response and steps taken to prevent future breaches) is of key importance to DPAs and the individuals whose personal information is affected.

Sixteen DPAs participated in the Sweep. Participating DPAs were asked to reach out to organisations with a set of pre-determined questions which focused on their current practices for recording and reporting data breaches.

Individual GPEN members may contact organisations in their own countries to assess what remedial action they need to take to improve their breach-related practices and procedures.

Editors' notes

1. The Global Privacy Enforcement Network (GPEN) was established in 2010 upon recommendation by the Organisation for Economic Co-operation and Development. Its aim is to foster cross-border co-operation among privacy regulators in an increasingly global market in which commerce and consumer activity relies on the seamless flow of personal information across borders. Its members seek to work together to strengthen personal privacy protections in this global context. The informal network is comprised of over 60 privacy enforcement authorities in 39 jurisdictions around the world.

2. The GPEN Sweep is currently chaired by the Office of the Privacy Commissioner, New Zealand.

3. For the exercise, participating DPAs were asked to reach out to organisations with a set of pre-determined questions which focused on their current practices for recording and reporting data breaches.

For further information, contact Charles Mabbett - 021 509 735.