04/03/2020

GIBRALTAR REGULATORY AUTHORITY

2nd Floor, Eurotowers 4
1 Europort Road
Gibraltar

Tel: +350 20074636
Fax: +350 20072166
e-mail: info@gra.gi
url: http://www.gra.gi

PRESS RELEASE

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

The Gibraltar Regulatory Authority ("GRA"), as the Information Commissioner, took part in the annual Global Privacy Enforcement Network Sweep (the "GPEN Sweep"), which this year considered how organisations in various jurisdictions handle and respond to personal data breaches.

Sixteen data protection authorities ("DPAs"), including the GRA, participated in the GPEN Sweep. 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.

The GRA focused on the reporting and handling of data breaches by gambling operators in Gibraltar. The results obtained established the following positive trends:

- The gambling operators targeted were well acquainted with the requirements of both the reporting and handling of data breaches to the GRA.

- The operators appeared to have a robust understanding of their obligations under relevant data protection legislation in regard to data breach notification requirements. The results also showed that they had appropriate reporting mechanisms, management processes and associated policies.

- Further, the gambling operators were aware of the impact that data breaches may have on their organisation as well as to the data subjects, and considered ongoing training and internal audits to be of great importance to help remedy/mitigate the risk of further breaches.

In terms of the global results, the GPEN Sweep found that 84 percent of respondent organisations said they had systems in place for reporting data breaches, including an appointed team or group responsible for handling breaches.

Organisations that voluntarily responded to the GPEN Sweep showed significant awareness about best practices for appropriately responding to data breaches.

But the global results of the GPEN Sweep need to be tempered by the low response rate from organisations contacted to participate. Of the 1145 organisations approached globally, 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 GPEN 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.

Global 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.

75 percent of responding organisations reported having procedures that covered key steps such as containment, assessment, evaluation of the risk associated with breaches. 18 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.

65 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 DPA where necessary.

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 GPEN Sweep. Almost all organisations that responded were aware of the relevant legal framework, including reporting thresholds and timeframes. Only 5 of those organisations demonstrated poor understanding of the legal framework.

Guidance provided by local 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.

As always, the GRA is available to anyone wishing to discuss matters which affect their privacy, or feel that their data protection rights are not being correctly addressed.

For further information please contact the GRA by telephone on +350 200 74636 or by email on privacy@gra.gi.