GPEN Sweep 2018

'Privacy Accountability'

October 2018

Office of the Privacy Commissioner, New Zealand

Information Commissioner's Office, UK

Background

The 2018 GPEN Sweep aimed to consider how well organisations have implemented the concept of privacy accountability into their own internal privacy programs and policies.

Accountability has become a core element of data protection and industry guidance. At the core of existing guidance are several key elements which focus on the importance of internal policies and procedures for data governance, training and awareness, transparency about data practices, the assessment and mitigation of risk, and incident management.

Participating agencies were asked to reach out to organisations with a set of pre-determined questions which focused on these key elements of responsible data governance. Various methodologies were adopted during this year's Sweep, including, but not limited to:

- Writing out to organisations with a list of set questions via email or post;
- Directing organisations to complete online polls;
- Conducting interviews over the telephone.

To narrow the focus of the Sweep, many participating agencies focused on a particular sector(s) which was of relevance to them, including, (but not limited to;

- Education;
- Electronic commerce;
- Finance and insurance;
- Health;
- Industry;
- Legal;
- Marketing;
- Public sector (including central and local government);
- Retail;
- Telecommunications;
- Tourism;
- Transport and Leisure.

Note that some participants looked at more than once sector. Participants also looked at other sectors, but for the purpose of this report, only the most reviewed sectors are listed.

Summary Observations

Of the 667 organisations contacted as part of this year's Sweep exercise, only 53% provided substantive responses.

It was positive to note that a large percentage of organisations across all sectors and jurisdictions had appointed an individual or team who would assume responsibility for ensuring that their organisation complied with relevant data protection rules and regulations.

Based on the responses received, organisations were generally found to be quite good at giving data protection training to staff, but often failed to provide refresher training.

Participating authorities noted a large majority of organisations actively maintain privacy policies which explain how they handle personal data, and that these were often easily accessible to the public, with less than 10% of organisations having no policies at all.

When it comes to monitoring internal performance in relation to data protection standards, organisations were found to fall short in this area, with more than 20% of organisations having no programmes in place to conduct self-assessments and/or internal audits. The organisations that indicated that they did have monitoring programmes in place generally gave examples of good practice, noting that they conducted annual audits or reviews and/or regular self-assessments.

Over half of the organisations surveyed indicated that they have documented incident response procedures, and that they maintain up to date records of all data security incidents and breaches. However, it is concerning that a number of organisations indicated that they have no processes in place to respond appropriately in the event of a data security incident (just under 15% of organisations surveyed).

Tombstone Data

Data Protection Authorities who submitted results: 18

Organisations contacted: 667

Responses received from organisations: 356

Methodology Note: *Not all Data Protection Authorities ("DPAs") reported on every reporting field. The statistics for this Sweep were developed based on the actual data received for a reporting field as a percentage of those organisations swept by those DPAs that reported on that field.*

Note that various methodologies were used when collecting data for the purpose of this Sweep. For instance, some participating agencies reviewed the responses provided by organisations and gave them a rating based on the information provided, while others required organisations to rate themselves and provide evidence where possible. In the case of the latter methodology, the responses were taken at face value. It is then up to the participating agency to decide whether they want to follow up on these responses with further investigation once the Sweep is complete.

Policies, Procedures and Governance (Indicator 1)

Participating agencies indicated that around 50% of organisations that provided a response maintain an internal data privacy policy (consistent with legal requirements) and would be able to demonstrate that this has been embedded into everyday practices if required. Another 33% indicated that they were either in the process of implementing a data privacy framework or had partially implemented internal policies. Of the 358 organisations who responded to this question, 14% were deemed to have poor internal privacy practices.

Organisations were asked whether there was anyone at a sufficiently senior level who was responsible for privacy governance. Whilst this is not a legal requirement in all participating jurisdictions, it was interesting to note that of the 335 organisations who responded to this question, 67% indicated that a data privacy officer had been appointed and/or there was a dedicated member of staff at a sufficiently senior level responsible for overall privacy governance and management. A further 27% indicated that a data privacy officer had been appointed, but that there was nobody at senior level responsible for the overall privacy governance.

Some participants noted that although it is not a requirement in their jurisdiction for organisations to have a dedicated individual or team responsible for ensuring compliance with data protection regulations and guidance, it was positive to find that a number of these organisations had assigned someone with this responsibility. Only 6% of the organisations who responded either indicated that they do not have anyone responsible for data protection, or failed to specify.

Participants noted a few examples of good practice. For instance, some organisations were found to have a central individual at senior level who was responsible for data protection, with data protection 'champions' in each office or business unit. Other organisations noted that they had a number of data protection officers at different levels to ensure a clear communication network was in place.

Monitoring, Training and Awareness (Indicator 2)

Only 50% of organisations indicated that regular data protection training is given to staff (including training for new staff, and refresher training for existing staff). However, 38% of the 314 organisations that provided a response did note that some data protection training is given to staff, but they either fail to give regular refresher training, or only provide training to some employees. 9% indicated that no data protection training was offered to staff.

When asked whether performance was monitored in relation to data protection standards (for example, where the organisation conducts regular self-assessments and/or internal audits of privacy programmes in relation to complaints / enquiries / data security breaches), 36% of the 305 organisations who responded to this question indicated that they conduct regular self-audits and that they regularly review their performance in relation to data protection standards. However, 39% indicated that whilst they do conduct self-audits and performance reviews, these are required to be more thorough and/or held more regularly.

Some examples of good practice were noted. A few organisations said that online training systems had been implemented, and network access would be revoked if training was not completed before a specified deadline.

Transparency (Indicator 3)

Organisations were asked whether they actively maintain polices which explain how they handle personal data, and whether these are easily accessible to the general public. Of the 338 organisations that responded, 55% demonstrated that they maintain a clear privacy policy, which is easily accessible to customers and the general public, while 31% indicated that whilst they do have a privacy policy in place, this may not

necessarily be easily accessible to the general public, may lack key principles of data protection, or may be outdated. In addition, 9% stated that they have no privacy policy in place for customers and the general public.

Not all participants viewed the privacy notices of the organisations involved in the Sweep, but some of those who did noted that it was generally unclear in the policy as to whether the organisations has data protection officers in place, and failed to provide contact information.

One participant noted that when they tried to reach out to a couple of organisations, the email was returned as 'undeliverable', which suggests there are some issues around accountability and transparency to the extent that customers are not able to reach the designated privacy contact at the company.

Responsiveness and Incident Management (Indicator 4)

When questioned as to whether a documented incident response procedure is maintained, 52% of 355 organisations indicated that they have a documented incident response procedure, whilst 13% indicated that they do not have an incident response procedure documented.

Organisations were asked in the event of a data security breach whether they had procedures in place to deal with this appropriately (regardless of whether this was documented or not). Of 290 organisations who responded to this question, 58% indicated that they have clear measures in place to deal with incidents as they arise, and clear steps in place to notify affected individuals and the relevant regulatory authority. A further 33% noted that whilst their ability to appropriately deal with a data breach was satisfactory, they may lack some essential steps and there is room for improvement.

Participating agencies noted examples of good practice, for instance some organisations have developed risk management manuals, while others have set up dedicated teams to respond to and handle security risks.

88% of 308 organisation maintain records of data security incidents, although 45% of these stated that these records may not always be kept up to date. 11% indicated that they do not keep records of incidents.

Some organisations stated that they maintain up to date incident logs which are tested annually and sit alongside breach/incident escalation

policies and incident management procedures. Some organisations noted that they have checklists which detail every step to follow in the event of a security incident.

Organisations were also asked to indicate how prepared they are to respond to requests and complaints raised by data subjects, and other queries raised by external enquirers (such as the data protection regulator). Of 326 organisations, 49% said that they have clear measures in place to deal with privacy-related concerns and queries, and that they would be equipped to respond to queries from relevant regulators. However, 14% indicated that that they have no such measures in place.

Participants noted that some organisations stated that they have processes in place to contact data subjects via email, phone, or post if necessary, and also procedures to publicise any details of incidents via the internet.

Risk Assessment, Documentation and Data Flow (Indicator 5)

46% of 287 organisations indicated that they have documented processes in place to assess the risks associated with new products, services, technologies and business models (for instance, the organisation may conduct privacy impact assessments). However, 19% of organisations demonstrated little to no understanding of the importance of assessing risks associated with new products, services, technologies and business model.

Participants who identified poor practices noted that some organisations seemed to be aware of the need for a risk assessment process, but had not taken any steps to document this process.

Participants also noted some examples of good practice. Whilst it was not a legal requirement in their jurisdiction to conduct risk and/or privacy impact assessments, it was positive to see that many organisations still had processes in place to assess risks when planning to develop or issue new products or services.

Organisations were asked to indicate whether they maintain inventories of personal data holdings, and whether they track data flows (for example, this would include data shared with third parties). Of the 313 organisations who responded, 53% stated that they actively maintain logs of all data held by them, and 48% maintain records of any data flows. In addition, 35% indicated that they have some understanding of the sort of

data they hold but fail to maintain an adequate inventory of the personal data held by them. 9% demonstrated little to no understanding of the sort of data they hold, and fail to maintain an adequate inventory.

Some participants noted that a number of the organisations who claimed not to have any inventories in place were in the process of changing this or building a new framework to enable them to record personal data holdings.

It was concerning to note that a small minority of organisations appeared to have a limited understanding of what constitutes 'personal information'. In these cases, the focus on personal information tended to be in relation to customer information, and did not extent to the personal data of employees.

Other findings

- As noted above, only 53% of organisations contacted provided a substantial response. Some participants were particularly concerned with the low number of respondents in their jurisdiction.

- There were some examples of good practice. For instance, some participating agencies noted that some of the organisations 'swept' had set up internal privacy and data portals containing links to data protection policies, forms, templates, and materials.

- A number of organisations were able to demonstrate use of best security practice by being ISO/IEC 27001 certified.

- Some participating agencies found it more challenging to engage with smaller organisations as opposed to larger organisations.

- Some participants who looked at the private and public sectors noted that there generally appeared to be less of a focus on privacy accountability in the private sector than in the public sector.

Conclusion

In summary, whilst many organisations across all sectors were generally quite good at delivering some form of data protection training to their employees, there is significant room for improvement to ensure that the training not only covers the necessary elements of the relevant data protection legislation, but also to ensure that refresher training is given to staff at all levels.

Whilst there were many examples of good practice, it was found that a number of organisations had no processes in place to deal with the complaints and queries raised by data subjects, and were not equipped to handle data security incidents appropriately.

Based on these findings, it is clear that whilst most organisations have a good understanding of the basic concepts of accountability, in practice there is room for improvement. Organisations need to ensure that they continue to monitor their performance to ensure they are adhering to the data protection standards laid out in the relevant laws and regulations, and ensure that they have clear, documented procedures in place to deal with data security complaints.