NYMITY DATA PRIVACY ACCOUNTABILITY SCORECARD™

This paper is a summary of the feedback release of the Nymity Data Privacy Accountability Scorecard™ ("Scorecard") book.

The Scorecard is an evidence based, scalable framework for the Privacy Office in responsible organisations to demonstrate accountability by monitoring, measuring, and reporting ongoing privacy management activities.

DATA PRIVACY ACCOUNTABILITY

Accountability was first established as a privacy principle over 30 years ago when the Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Data Flow ("1980 Guidelines") placed responsibility on organisations for complying with measures that give effect to all of the OECD principles. The guidelines were updated on July 11, 2013 with additions that further emphasize the importance of accountability. Part three on implementing accountability states:

A data controller should... be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines.

This update to the OECD guidelines reflects the growing focus on accountability in the global privacy community over the past five years, as well as the increasing expectations with regard to being able to demonstrate accountability.

What is data privacy accountability?

Definitions of accountability vary slightly, but are generally aligned on the importance of maintaining an effective privacy program, and being able to show that the organisation has an established privacy program in place, commonly referred to as “demonstrating accountability.”

The Article 29 Working Party describes Accountability as, “showing how responsibility is exercised and making this verifiable.” This definition reinforces the discussion regarding the fundamental elements of accountability: responsibility, ownership, and evidence.

- Responsibility - the organisation maintains an effective privacy program consisting of ongoing privacy management activities.
- Ownership - an individual is answerable for the management and monitoring of the privacy management activities.

Evidence - the Privacy Office can support, with documentation, the completion of privacy management activities.

Each of these elements builds upon the previous and all are necessary for demonstrating accountability – to remove or weaken any one of these elements would prevent the organisation from being accountable.

Responsibility
Long before there were data privacy laws, responsible organisations processed personal data responsibly as a core component of their operations. For a variety of reasons, many organisations in healthcare, financial services, or the public sector processed data responsibly even before a Privacy Office was established. Typically, organisations process an individual’s personal data responsibly as a result of corporate culture and a general adherence to societal values, they have a desire to ‘do the right thing’. The foundation for data privacy accountability is responsibility, and as such only a responsible organisation can be accountable.

“Responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed.” - Article 29 Working Party Opinion 3/2010 on the principle of accountability

Responsible organisations manage their privacy programs via privacy management activities. The activities vary between organisations as widely as do the purposes for processing personal data and the types of personal data being processed. In a privacy program, not all privacy management activities are equal. Some are more important than others. Some can be thought of as fundamental, mandatory, or core and some can be thought of as desired, ideal, surpassing compliance, optional, or elective.

To simplify the concept of responsibility, Nymity will discuss two tiers of activities: core and elective.

- Core: Core activities are defined by the Privacy Office and are fundamental to privacy management. They may be mandatory for compliance, or required by the organisation for other reasons.
- Elective: Elective activities are desired activities defined and supported by the Privacy Office that are encouraged, but not required.

Table 1 provides examples of privacy management activities that may be considered core or elective in the context of various privacy frameworks and jurisdictions.

<table>
<thead>
<tr>
<th>Examples of Core Activities</th>
<th>Examples of Elective Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain procedures to respond to access requests</td>
<td>Maintain policy/procedure for collection and use of sensitive personal data</td>
</tr>
<tr>
<td>Maintain a privacy notice that details the organisation’s personal data handling policies</td>
<td>Conduct one-off, one-time tactical training and communication dealing with specific and highly-relevant issues/topics</td>
</tr>
<tr>
<td>Maintain procedures to execute contracts or agreements with all processors</td>
<td></td>
</tr>
</tbody>
</table>
Table 1 - Examples of Core and Elective Privacy Management Activities

<table>
<thead>
<tr>
<th>Examples of Core Activities</th>
<th>Examples of Elective Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Maintain policy/procedure for secondary uses of personal data</td>
<td>▪ Maintain a Code of Conduct</td>
</tr>
<tr>
<td>▪ Maintain a physical security policy (protection of</td>
<td>▪ Maintain formal communication between individuals</td>
</tr>
<tr>
<td>physical premises and hard assets)</td>
<td>accountable and responsible for data privacy</td>
</tr>
<tr>
<td>▪ Maintain job descriptions for individuals responsible</td>
<td>▪ Maintain data privacy incident/breach metrics</td>
</tr>
<tr>
<td>for data privacy (e.g. data protection officers)</td>
<td>▪ Maintain job descriptions for individuals responsible</td>
</tr>
<tr>
<td></td>
<td>for data privacy (e.g. data protection officers)</td>
</tr>
</tbody>
</table>

Ownership
Ownership is the second component of accountability and builds upon responsibility. When an individual is designated responsible for the management and monitoring of the privacy management activity, he or she is the “owner.” The owner does not necessarily complete the privacy management activity, but is ultimately responsible or answerable for it.

Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organisation to be answerable or its actions. - Data Protection Accountability: The Essential Elements, Centre for Information Policy Leadership

Data privacy accountability requires ownership at the organisational level, as the organisation must be accountable or answerable to data subjects/individuals, regulators, and business partners. In order to achieve organisational accountability, the concepts of responsibility and ownership must be embedded throughout the privacy program.

▪ Ownership in the Privacy Office - The Privacy Office is accountable for many elements of the privacy program, but the Privacy Office itself processes very little, if any, personal data. In other words, they are accountable for data privacy, but do not have direct control of the privacy management activities.

▪ Ownership in operational units - The effectiveness of the privacy program relies on the appropriate privacy management activities being performed at all points of the data life cycle, from the point of collection to the point of destruction. Ownership of many privacy management activities will reside with operational units (e.g. marketing, human resources, customer service), as that is where the data is being collected and processed.

Evidence
The third element of data privacy accountability is evidence. In responsible organisations, the owner of a privacy management activity provides supporting evidence that the activity was completed. The primary evidence will be some form of documentation which can be provided in two forms: formal and informal.

▪ Formal evidence is typically published, maintained, and communicated to designated groups (e.g., policies, procedures, reports)
Information evidence may show an example of an activity having occurred, such as an e-mail conversation between two key individuals or record of participation in a webinar.

Documentation may be produced by the Privacy Office (e.g. Data Privacy Policy, Privacy Notice), but may also be produced by other parts of the organisation and influenced or simply collected by the privacy office (e.g. Privacy Impact Assessments, IT Security Assessments).

**DATA PRIVACY ACCOUNTABILITY SCORECARD FRAMEWORK**

The Nymity Data Privacy Accountability Scorecard (“Scorecard”) is a scalable, evidence-based framework that allows organisations to:

- Monitor and measure privacy management activities
- Assign appropriate ownership
- Produce supporting evidence

In other words, the Scorecard enables organisations to demonstrate accountability for data privacy.

**Implementing the Scorecard**

The power of the Scorecard framework is derived from its simplicity of use. The following steps outline the process to implement it. Nymity has created templates which are publicly available at no charge at www.scorecard.nymity.com. Visit the portal and register to download the free templates along with an instruction book, training videos, example Scorecards, and other resources.

1. **Setup Scorecard: identify activities, ownership, and frequency**

   To start, the Privacy Office needs to identify all the privacy management activities that are currently being completed and those that would be desired or ideal to be maintained. For each activity, the organisation defines the owner and the frequency at which the owner should provide evidence.

   Nymity’s Evidencing Accountability Study™ identifies over 140 privacy management activities that are common to organisations across industries and jurisdictions, structured in 13 Privacy Management Processes™ (see appendix). The study is also available on the Scorecard portal.

2. **Create evidence collection questions**

   The Privacy Office creates simple, concise questions to compel the evidence from activity owners. Evidence collection questions are closed questions, meaning they must be answered with “Yes” or “No” to enable quantifiable analysis (discussed below).

3. **Collect responses and evidence**

   Next, the Privacy Office consolidates the responses to the questions and supporting evidence from the activity owners, along with comments to provide additional context.
Figure 1 below shows an example of the Evidence Worksheet with steps 1-3 completed. The complete Excel workbook is available at www.scorecard.nymity.com.

### NYMITY Data Privacy Accountability Scorecard™

#### Evidence Worksheet

www.scorecard.nymity.com

<table>
<thead>
<tr>
<th>Core Activities</th>
<th>ID#</th>
<th>Question</th>
<th>Owner</th>
<th>Frequency</th>
<th>Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td></td>
<td>Is the Data Privacy Policy reviewed based on legislative and operational changes?</td>
<td>Privacy Office</td>
<td>Annual</td>
<td>No</td>
<td>The Data Privacy Policy has not been reviewed in the last two years, we plan to do so within the next two months.</td>
</tr>
<tr>
<td>C2</td>
<td></td>
<td>Do the individuals in the privacy office maintain their privacy knowledge?</td>
<td>Privacy Office</td>
<td>Annual</td>
<td>Yes</td>
<td>All members of the Privacy Office maintain privacy certifications. Email confirmation from all members of the Privacy Office that their certifications are in good standing.</td>
</tr>
<tr>
<td>C3</td>
<td></td>
<td>Does the Privacy Office track and analyze the impact of new laws, changes in laws, relevant enforcement actions and new regulator expectations?</td>
<td>Privacy Office</td>
<td>Quarterly</td>
<td>Yes</td>
<td>The Privacy Office subscribes to Nymity’s PrivaWorks to track legislative developments. No applicable changes to laws or regulations. Memo between Privacy and Legal regarding legislative developments (none noted).</td>
</tr>
<tr>
<td>C4</td>
<td></td>
<td>Do all third party contracts contain organizational standard privacy language?</td>
<td>Legal</td>
<td>Annual</td>
<td>No</td>
<td>Contracts are likely being reviewed as they have always been in the past but Legal did not provide evidence on schedule. Will follow-up.</td>
</tr>
<tr>
<td>C5</td>
<td></td>
<td>Is the online Privacy Notice updated based on changes to policy, operations, or legal developments?</td>
<td>Legal</td>
<td>Annual</td>
<td>Yes</td>
<td>The Privacy Notice was reviewed and no changes were made for 2013. Privacy Notice v3.4 (published 2/14/13) <a href="http://www.website.com/privacy">www.website.com/privacy</a></td>
</tr>
<tr>
<td>C6</td>
<td></td>
<td>Are all new employees trained on data privacy?</td>
<td>Human Resources</td>
<td>Quarterly</td>
<td>Yes</td>
<td>Employees are required to completed eLearning module for data privacy and results are tracked by HR. Report of employees who have completed data privacy training.</td>
</tr>
<tr>
<td>C7</td>
<td></td>
<td>Are procedures for responding to access requests, complaints, and inquiries reviewed and communicated?</td>
<td>Customer Service</td>
<td>Annual</td>
<td>No</td>
<td>The procedures for responding to access requests, complaints and inquiries have not been reviewed in the last two years, we plan to do so by Q2.</td>
</tr>
</tbody>
</table>

### Calculating the Data Privacy Accountability Score

The score is calculated by dividing the number of activities for which the owner has provided evidence (i.e. the response to the question is “Yes”), by the number of core or elective activities identified. The result is the percentage of activities that are completed with evidence as of that specific date: the Data Privacy Accountability Score.

\[
\% \text{ Managed} = \frac{\# \text{ of Core Activities Evidenced}}{\# \text{ of Core Activities}}
\]

When all core activities are evidenced, the privacy program is 100% Managed and has reached the target. The percentage Advanced is based on the elective activities completed and evidenced.

\[
\% \text{ Advanced} = \frac{\# \text{ of Elective Activities Evidenced}}{\# \text{ of Elective Activities}}
\]

The scores can be plotted on a timeline to enable the Privacy Office to demonstrate accountability over time, as shown below in Figure 2. The Scorecard template provided by Nymity automatically generates a graph like the one below when the Evidence Worksheet (Figure 1, above) is completed.
Potential Score
Until the target of 100% Managed is reached, the % Advanced is recorded as a potential score. In other words, elective activities do not affect the overall Data Privacy Accountability Score until all core activities are completed. Even though they do not affect the overall score, the Privacy Office can still account for them and collect evidence in order to gain a more holistic view of the privacy program.

Decreased Score
Given that the privacy management activity has a frequency assigned, the owners will need to provide evidence that the activity was completed within the specified timeframe.

Scalability
A scalable framework is one that can be expanded or upgraded to meet the needs of organisations of any size, structure, or sector. The basic Scorecard approach using the templates provided by Nymity may be suitable for a small or medium organisation, whereas larger or more complex organisations may require a multi-layer approach. For example, the organisation may wish to deploy the Scorecard by department, region/jurisdiction, data type/purpose (e.g. customer, employee) or to third party processors.
ABOUT THIS PAPER

This paper is a summary of the feedback release of the Nymity Data Privacy Accountability Scorecard™ book, which is available for download (free, registration required) at www.scorecard.nymity.com.

Requesting Feedback

Nymity would appreciate feedback on the framework for demonstrating data privacy accountability:

- How this framework could be improved to help responsible organisations demonstrate accountability; and
- How this framework could be used and/or improved to allow law firms and consulting firms to better assist their clients with maintaining an effective privacy program.

In March 2014 at the IAPP Global Privacy Summit, Nymity will release Version 2 which will be updated based on feedback gathered.

Please provide feedback directly to Nymity via feedback@nymity.com or www.scorecard.nymity.com.

About the Scorecard – a Nymity Research Initiative

Over the past ten years, Nymity has had the pleasure of working with many responsible organisations that take data privacy seriously. These organisations have a culture of doing the right thing for their customers, citizens, patients, and employees by processing personal data responsibly. They have a Privacy Office and maintain an established privacy program. They strive to optimize current resources and continuously enhance privacy management.

The objective of Nymity’s Data Privacy Accountability Scorecard framework is to enable these organisations to further realise benefits from their current investments in privacy management and from their future investments in privacy management.

Data Protection Authorities (DPAs), including regulators, privacy commissioners, and others with oversight responsibility, devote a great deal of resources to educating and helping their constituents interpret and understand their expectations related to privacy management. DPAs focus on enabling organisations to comply in a way that does not hinder the organisation’s core objectives. They are also tasked with enforcing laws and regulations, including investigations of complaints or events which may indicate non-compliance with a law.

DPA investigations that take place in response to a breach or complaint reveal that some organisations do not have an established privacy program. However, in some cases, investigations reveal that incidents do occur at responsible organisations with established privacy programs as well. After all, there is an inherent risk associated with the processing of personal data and breaches may occur. DPAs can often intuitively tell the difference between a responsible organisation that experienced an error and an organisation that does not have an established privacy program. Many DPAs desire a more
objective or “empirical” method to distinguish between the organisations with and without an established privacy program.

DPAs and law makers around the world are looking for scalable and practical frameworks that enable organisations to communicate the status of their privacy programs. There has been considerable research in different parts of the world toward verification systems based on some form of external validation. The framework presented in this book is intended for use by organisations to communicate evidence directly to DPAs and other interested stakeholders, but without the need for a third-party assessment or verification. This Framework is not presented to replace third-party verification, but to augment it – refer to Chapter 5 of the book for a complete discussion.

---

2 Nymity DPA Demonstrating Accountability Workshop - 2011