ACCOUNTABILITY METRICS: A PRAGMATIC, SCALABLE SOLUTION

Michael E. Katz, Data Privacy Manager, BP America
Ellis Parry, Global Lead - Data Privacy, BP International Ltd.
Lauren Reid, Director, Compliance Solutions, Nymity Inc.

#privacysummit
AGENDA

• Discussion on:
  – Background on BP’s drivers for measuring the status of our privacy program
  – Challenges facing a global organization
  – Our solution and lessons learned
  – Using the Data Privacy Accountability Scorecard to develop meaningful metrics

• What you’ll take away:
  – Understanding of how to develop meaningful privacy accountability metrics
  – Framework and templates for developing and monitoring privacy accountability metrics
BP AT A GLANCE

- BP is one of the world's leading international oil and gas companies.

We find Oil and Gas

We extract Oil and Gas

We move Oil and Gas

We make fuels and products

We sell to people like you.

- Countries of operation - Over 80
- Number of employees - 85,900
- Retail sites - 20,700

- as at, or for the year ended, 31 December 2012, updated for IFRS 11 and IAS19 where relevant

#privacysummit
BACKGROUND

• BP processes personal data in 80 countries around the globe, creating a complex challenge for maintaining compliance
  – One key challenge was overcoming the restrictions in EU law around transferring personal data outside the European Economic Area

• BP adopted Binding Corporate Rules (BCR) in 2010:
  – To legally comply with EU laws on intragroup transfers of personal data outside the EU Economic Area
  – To create a robust compliance framework for the processing of personal data within the BP group

• BP developed 16 Privacy Rules which are embedded in the Code of Conduct
  – BCRs are agreed with EU regulators who retain the power to inspect and enforce BP’s compliance with the legally binding rules
  – There is a requirement to conduct ongoing audits to ensure they are being followed throughout the organization

#privacysummit
OUR CHALLENGE

How do we demonstrate Privacy Compliance across 80 countries?

• BP had no standardised way of monitoring, assessing and reporting on compliance

• EU’s data privacy laws are currently subject to renegotiation
  – New proposal is the introduction of a prospective obligation to prove to external stakeholders that controllers have an effective data privacy compliance program in place
  – This ‘accountability principle’ would entail a more objective assessment of BP’s data privacy compliance program than BP was positioned to provide

#privacysummit
# PRIVACY PROGRAM AT BP

## Central Data Privacy Team – BP Legal

- **Middle/Eastern Europe and Caspian Sea**
- **Americas**
- **Western Europe, Africa and Middle East**
- **Asia Pacific**

### Local Privacy Coordinators (LPC)

- **Central Data Privacy Team** is made up of Regional Privacy Advisors
- **Mission**: To promote best practices for managing personal information in compliance with the Code of Conduct, BP Privacy Rules, and any local legal obligations.

- **LPC** is a role which is assumed on top of normal job responsibilities
- **Implement and monitor BCR in their jurisdiction and provide advice to local stakeholders**
OUR GOAL

• Answer two fundamental questions:

  1. How do we know our privacy program is embedded throughout the organization?

  2. How can we monitor the status of the program on an ongoing basis?
CRITICAL SUCCESS FACTORS

1. **Pragmatic** Ability to demonstrate compliance to BP’s 16 Data Privacy Rules in a sustainable, ongoing way
   - Simple and straightforward for LPCs - without placing undue burden or requiring them to become privacy “experts”
   - Working with existing program resources

2. **Scalable** Global view of the program, with the ability to drill down to country level
   - Understand risks at the country level and how they impact the overall enterprise-wide risk

3. **Evidence based** Enable compliance with privacy laws and regulations globally

#privacysummit
BP’S SOLUTION

- Implement the Data Privacy Accountability Scorecard via Attestor
  - Information about the privacy program, and associated evidence is collected at the country level, and measured and reported regionally and globally
  - Accountability Score is automatically generated based on answers to simple, yes/no questions
  - Demonstrate the status of the program and improvement over time
- To answer those questions BP implemented a pragmatic, scalable framework to measure and provide evidence of the implementation of our BCRs
- We’ll share our experience and lessons learned, and provide you with the framework and templates to help you implement data privacy accountability metrics at your organization.

#privacysummit
OUTCOME

**BP is able to Demonstrate Compliance and Accountability – on demand**

- In the event that a national privacy regulator requests or demands evidence that BP is compliant with BCRs, local laws or regulations:
  - We will be able to respond quickly and objectively
  - Our responses will be backed by evidence
  - We can document our compliance status and actions we are taking to make any improvements
THE EVOLVING PRIVACY LANDSCAPE

Privacy Program Outcomes

- Laws and Regulations
- Enforcement Actions
- Binding Corporate Rules

Privacy Program Infrastructure

- Responsibility
- Ownership
- Evidence

#privacysummit
KEY CONCEPTS
DEMONSTRATING ACCOUNTABILITY

ACCOUNTABILITY
Showing how responsibility is exercised and making this verifiable. – Article 29 Working Party

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.

#privacysummit
THE EVOLVING PRIVACY LANDSCAPE

#privacyconference
DATA PRIVACY ACCOUNTABILITY SCORECARD™

An evidence-based, scalable framework for the Privacy Office in responsible organizations to demonstrate accountability by monitoring, measuring, and reporting ongoing privacy management activities.

- Based on years of research by Nymity
- Free download of Excel Spreadsheet, with supporting resources for implementation (videos, webinars, instruction book)
- Nymity Attestor™ is an automated software solution available for more complex deployments

#privacyssummit
#privacysummit

**SCORECARD MANAGEMENT**

**SCORECARD SETUP**
- Categorize privacy management activities
- Create evidence collection questions
- Assign activity ownership
- Assign activity frequency

**COLLECT EVIDENCE**

**CALCULATE SCORE**
#privacy Summit

## SCORECARD MANAGEMENT

### SCORECARD SETUP: 1. CATEGORIZE PRIVACY MANAGEMENT ACTIVITIES

<table>
<thead>
<tr>
<th>Privacy Management Activity</th>
<th>Core/Elective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain a data privacy policy</td>
<td>Core</td>
</tr>
<tr>
<td>Maintain an internal privacy intranet, privacy blog, repository of privacy FAQs and information</td>
<td>Elective</td>
</tr>
<tr>
<td>Maintain internal guidelines for contract templates that establish data privacy obligations in all contracts and agreements</td>
<td>Core</td>
</tr>
<tr>
<td>Maintain a core training program for all employees</td>
<td>Core</td>
</tr>
<tr>
<td>Attend/participate in privacy conferences or think-tank events</td>
<td>Elective</td>
</tr>
</tbody>
</table>

### CORE ACTIVITIES

- ✔ Fundamental to privacy management
- ✔ Required for compliance
- ✔ Designated by the privacy office as mandatory

### ELECTIVE ACTIVITIES

- ✔ Desired but not mandatory
- ✔ Surpass minimum requirements for privacy management
- ✔ Supported and encouraged by the privacy office
# SCORECARD MANAGEMENT

## SCORECARD SETUP: 2. CREATE EVIDENCE COLLECTION QUESTIONS

<table>
<thead>
<tr>
<th>Privacy Management Activity</th>
<th>Core/Elective</th>
<th>Evidence Collection Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain a data privacy policy</td>
<td>Core</td>
<td>Is the Data Privacy Policy reviewed based on legislative and operational changes?</td>
</tr>
<tr>
<td>Maintain an internal privacy intranet, privacy blog, repository of privacy FAQs and information</td>
<td>Elective</td>
<td>Is the privacy intranet site maintained with resources and up to date guidance on matters related to data privacy?</td>
</tr>
<tr>
<td>Maintain internal guidelines for contract templates that establish data privacy obligations in all contracts and agreements</td>
<td>Core</td>
<td>Do all third party contracts contain organizational standard privacy language?</td>
</tr>
<tr>
<td>Maintain a core training program for all employees</td>
<td>Core</td>
<td>Are all new employees trained on data privacy?</td>
</tr>
<tr>
<td>Attend/participate in privacy conferences or think-tank events</td>
<td>Elective</td>
<td>Does the Privacy Office attend conferences and other events to learn about new developments in data privacy?</td>
</tr>
</tbody>
</table>

Questions should be:
- Related to privacy management activities
- Clear and concise
- Closed ended – able to answer “yes” or “no”

#privacyssummit
Do you seek legal advice on the correct interpretation of your local data privacy law?*

Frequency: Annually

Do you communicate data privacy developments to local stakeholders (e.g. HR, HoC, your Line Management)?*

Frequency: Annually
<table>
<thead>
<tr>
<th>Privacy Management Activity</th>
<th>Core/Elective</th>
<th>Evidence Collection Question</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain a data privacy policy</td>
<td>Core</td>
<td>Is the Data Privacy Policy reviewed based on legislative and operational changes?</td>
<td>Privacy Office</td>
</tr>
<tr>
<td>Maintain an internal privacy intranet, privacy blog, repository of privacy FAQs and information</td>
<td>Elective</td>
<td>Is the privacy intranet site maintained with resources and up to date guidance on matters related to data privacy?</td>
<td>Communications</td>
</tr>
<tr>
<td>Maintain internal guidelines for contract templates that establish data privacy obligations in all contracts and agreements</td>
<td>Core</td>
<td>Do all third party contracts contain organizational standard privacy language?</td>
<td>Legal</td>
</tr>
<tr>
<td>Maintain a core training program for all employees</td>
<td>Core</td>
<td>Are all new employees trained on data privacy?</td>
<td>Human Resources</td>
</tr>
<tr>
<td>Attend/participate in privacy conferences or think-tank events</td>
<td>Elective</td>
<td>Does the Privacy Office attend conferences and other events to learn about new developments in data privacy?</td>
<td>Privacy Office</td>
</tr>
</tbody>
</table>
## SCORECARD MANAGEMENT

### SCORECARD SETUP: 4. ASSIGN ACTIVITY FREQUENCY

<table>
<thead>
<tr>
<th>Privacy Management Activity</th>
<th>Core/Elective</th>
<th>Evidence Collection Question</th>
<th>Owner</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain a data privacy policy</td>
<td>Core</td>
<td>Is the Data Privacy Policy reviewed based on legislative and operational changes?</td>
<td>Privacy Office</td>
<td>Annual</td>
</tr>
<tr>
<td>Maintain an internal privacy intranet, privacy blog, repository of privacy FAQs and information</td>
<td>Elective</td>
<td>Is the privacy intranet site maintained with resources and up to date guidance on matters related to data privacy?</td>
<td>Communications</td>
<td>Annual</td>
</tr>
<tr>
<td>Maintain internal guidelines for contract templates that establish data privacy obligations in all contracts and agreements</td>
<td>Core</td>
<td>Do all third party contracts contain organizational standard privacy language?</td>
<td>Legal</td>
<td>Annual</td>
</tr>
<tr>
<td>Maintain a core training program for all employees</td>
<td>Core</td>
<td>Are all new employees trained on data privacy?</td>
<td>Human Resources</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Attend/participate in privacy conferences or think-tank events</td>
<td>Elective</td>
<td>Does the Privacy Office attend conferences and other events to learn about new developments in data privacy?</td>
<td>Privacy Office</td>
<td>Annual</td>
</tr>
</tbody>
</table>

#privacysummit
# privacysummit

## SCORECARD MANAGEMENT

**COLLECT EVIDENCE USING THE EVIDENCE WORKSHEET**

### Nymity Data Privacy Accountability Scorecard™

**Evidence Worksheet**

[www.scorecard.nymity.com](http://www.scorecard.nymity.com)

<table>
<thead>
<tr>
<th>Core Activities</th>
<th>% Managed (core activities completed and evidenced)</th>
<th>% Advanced (elective activities completed and evidenced)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Question</strong></td>
<td><strong>Owner</strong></td>
<td><strong>Frequency</strong></td>
</tr>
<tr>
<td>C1 Is the Data Privacy Policy reviewed based on legislative and operational changes?</td>
<td>Privacy Office</td>
<td>Annual</td>
</tr>
<tr>
<td>C2 Do the individuals in the privacy office maintain their privacy knowledge?</td>
<td>Privacy Office</td>
<td>Annual</td>
</tr>
<tr>
<td>C3 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>
</tr>
<tr>
<td>C4 Do all third party contracts contain organizational standard privacy language?</td>
<td>Legal</td>
<td>Annual</td>
</tr>
<tr>
<td>C5 Is the online Privacy Notice updated based on changes to policy, operations, or legal developments?</td>
<td>Legal</td>
<td>Annual</td>
</tr>
<tr>
<td>C6 Are all new employees trained on data privacy?</td>
<td>Human Resources</td>
<td>Quarterly</td>
</tr>
</tbody>
</table>
#privacysummit

## NYMITY Data Privacy Accountability Scorecard™

### Evidence Worksheet

www.scorecard.nymity.com

3/15/2013

% Managed (core activities completed and evidenced)
64% Managed - 7 out of 11 core activities

% Advanced (elective activities completed and evidenced)
29% Advanced - 2 out of 7 elective activities

### Core Activities

<table>
<thead>
<tr>
<th>ID#</th>
<th>Question</th>
<th>Owner</th>
<th>Frequency</th>
<th>Response</th>
<th>Comment</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</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>
<td>Data Privacy Policy v2.8 (published 1/18/13)</td>
</tr>
<tr>
<td>C2</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.</td>
<td>Email confirmation from all members of the Privacy Office that their certifications are in good standing.</td>
</tr>
<tr>
<td>C3</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.</td>
<td>Memo between Privacy and Legal regarding legislative developments (none noted).</td>
</tr>
<tr>
<td>C4</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>
<td></td>
</tr>
<tr>
<td>C5</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.</td>
<td>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>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.</td>
<td>Report of employees who have completed data privacy training.</td>
</tr>
</tbody>
</table>

---

**SCORECARD MANAGEMENT**

**COLLECT EVIDENCE USING THE EVIDENCE WORKSHEET**

**OWNER RESPONDS “YES” OR “NO”**

**COMMENT PROVIDES ADDITIONAL DETAIL**

**LOG EVIDENCE**
Do you seek legal advice on the correct interpretation of your local data privacy law?*  
*08/27/2013  Yes  
We engage with an external law firm to provide advice on matters related to data privacy when necessary.  
Frequency: Annually  
Evidence: Email correspondence with external law firm  
(renew in 250 days – by 08/27/2014)

Do you communicate data privacy developments to local stakeholders (e.g. HR, HoC, your Line Management)?*  
*08/27/2013  Yes  
I presented an update on US Regulatory Changes to the Legal team.  
Frequency: Annually  
Evidence: Presentation to Legal Team of State and Federal Updates  
(renew in 250 days – by 08/27/2014)
NYMITY Data Privacy Accountability Scorecard™

Potential Score = % of Elective activities completed if score is less than 100% Managed

% Advanced = # of Elective activities completed and evidenced ÷ # of Elective activities

Target = 100% of Core activities completed and evidenced

% Managed = # of Core activities completed and evidenced ÷ # of Core activities

Current Score

Potential
LESSONS LEARNED

- Senior Management and Legal team buy in is critical
- Get support from the people who will be responsible for updating the tool
- Pilot the tool in some countries with more rigorous privacy regimes
- Keep the questions simple and aligned with your current Privacy Rules/Policies etc.
- Do not make it sound like a report card.
- Include the review with quarterly conversation with Local Privacy coordinators

#privacysummit
ADDITIONAL BENEFITS

• Able to identify areas which may need improvement and then show that improvement over time
• Distributes work of monitoring compliance across the organization, doesn’t just fall to the privacy office
• Can very easily demonstrate the impact that one country has on the program overall, compare one country to another
• Encourages participation throughout the year, not just a “mad dash” to respond to a compliance audit
• Resource for LPCs - they can learn from their counterparts in other countries and they better understand what is expected of them
• When there is turnover in the role, the new LPC can see all of the relevant history of how things were done before