Drawing a Map: Where Are You Now? Where Do You Need to Go?

Dana Simberkoff, CIPP/US, Chief Compliance and Risk Officer, AvePoint
Christina Peters, CIPP/US, CPO, IBM

Practical Privacy Series 2016
9:30 a.m. – 10:15 a.m.
Christina Peters, IBM Chief Privacy Officer
cpeters@us.ibm.com

Agenda

• Introductions (some questions to get us started)
• The IBM Perspective
• Benchmarking Global Readiness-AvePoint and CIPL Survey
• Questions
IBM at a glance

- 400,000+ employees
- 170+ countries
- Well-established privacy program

**Key Business Segments**

- Services
- Software
- Hardware
- Cloud
- Cognitive
- Research
- Financing

Diverse businesses, diverse challenges

- Analytics
- Cloud
- Cognitive
- Commerce
- Digital Business
- Education
- GBS
- GTS
- IoT
- Industry Solutions
- IT Infrastructure
- Mobile
- Security
- Social
- Watson
- Watson Health

- Controllers
- Processors
- IBM data
- Client data
Cross Company GDPR Project

... Established GDPR project to help business units take ownership of various challenges, provide and promote common approaches, and share solutions

IBM as a Controller

... using existing GPA to help internal business owners prepare for GDPR in the course of 2017
Partnership with Chief Data Office

... privacy in sync with data strategy

Successful implementation of data strategy

... depends upon a sophisticated approach to governance from beginning to end

<table>
<thead>
<tr>
<th>Governance drives value from ingestion to access</th>
<th>Data stewardship</th>
<th>Metadata management</th>
<th>Data curation</th>
<th>Data catalog</th>
<th>Rationalization of data purchases</th>
<th>Scalable &amp; secure role/access authorization</th>
<th>Privacy and security</th>
<th>Reporting</th>
<th>Auditing</th>
<th>Feedback &amp; resolution process</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXISTING DATA ASSETS</td>
<td>Spark, SQL, DataStage</td>
<td>Search Indices</td>
<td>Security, Provenance, Privacy/Policy Enforcement</td>
<td>Applications</td>
<td>Features</td>
<td>Analysis across data sets</td>
<td>Expanded access</td>
<td>Ongoing integration of new data</td>
<td>Improved data quality</td>
<td>Timely access</td>
</tr>
</tbody>
</table>
## Established framework for managing data end-to-end

<table>
<thead>
<tr>
<th>Organizational Support (BUDO, FUDO)</th>
<th>Stewardship &amp; Data Governance</th>
<th>Policies, Audits &amp; Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Acquisition</td>
<td>Data Ingestion</td>
<td>Data Integration</td>
</tr>
<tr>
<td>Data Ingestion</td>
<td>Data Integration</td>
<td>Data Access</td>
</tr>
<tr>
<td>Data Integration</td>
<td>Meta Data Management</td>
<td>Data Quality</td>
</tr>
<tr>
<td>Meta Data Management</td>
<td>Information Storage Management</td>
<td>Data Security, Privacy and Regulatory Compliance</td>
</tr>
<tr>
<td>Information Storage Management</td>
<td>Data Security, Privacy and Regulatory Compliance</td>
<td></td>
</tr>
</tbody>
</table>

- **Data Strategy**
  - Integrating DG Disciplines & Data Management Components

- **Data Management Components**
  - Providing integrated Management of DG Practices

- **Data Governance Disciplines**
  - each with detail Data Governance processes

## Key goals for GDPR implementation

... go beyond compliance...

- GDPR strategy
- policies
- education
- measurement
- technical automation

... Innovate with Confidence!
AvePoint & CIPL's first global survey to benchmark organisations’ readiness for the GDPR
Founded in 2001, AvePoint helps more than 15,000 organizations accelerate the migration, management, and protection of their data no matter where it lives – including IT systems on premises, in the cloud, and in hybrid environments.

GDPR Survey

CIPL and AvePoint launched a global GDPR readiness survey to:
- Assess current state of readiness for the GDPR
- Benchmark and evaluate readiness in relation to industry peers on an ongoing basis
- Understand key changes and compliance obligations under the GDPR
- Help determine a best implementation path forward and make appropriate resources and budgetary requests to meet their goals

The survey focuses on the key change areas in GDPR including:
- Consent and consent for children
- Legitimate interest
- Profiling
- Data portability
- Privacy impact assessments
- Data protection by design
- DPOs and resources
- Data breach reporting
- Transfers to third countries
- Accountability and privacy management programme
Survey Participants Snapshot – 232 responses

### Job Titles
- Chief Privacy Officer/Data Protection Officer
- Senior Director Global Privacy
- Legal Counsel/Attorney
- Information Security Officer
- Manager
- Consultant
- Vice President

### Company Revenues
Less than $1 Million to Greater than $100 Billion

### Survey Participants Location
- 70% Europe
- 27% Americas
- 1% Africa

- 93% operate in Europe
- More than half operate in US
- Under half in Latin America
- Under half in Asia Pacific

### Key Insights
- Consent and Legitimate Interest
- DPIA and Privacy by Design
- Security Breach Notification
- Controller-Processor Agreement
- Data Transfers outside EU – HR, Customer and Data Transfers to Vendors
- Organisational Readiness and Resources for GDPR Implementation
GDPR: Organisational Readiness

1 in 5
Have committed additional headcount, budget or external counsel spend

31%
No additional resources

1/2
Have started internal discussions

SENIOR MANAGEMENT KEY CONCERNS

1
Enhances sanctions
Data Breach reporting

2
Stricter rules on consent & reuse
Individual rights
Changes to internal privacy program

GDPR Requirements: Where do you stand?

- Privacy Management Programme
- Use/Contracting with processors
  - Data breach notification
- Individual rights

Legitimate interests, Privacy By Design, DPIA and risk are the areas requiring most clarification

Equally Processors are not ready for new obligations imposed by GDPR
**Consent & Legitimate Interest**

- **90%** Use consent for majority or some data processing today
- **78%** Do not consistently obtain separate consent for different processing operations
- **83%** Currently using legitimate interest or will be post GDPR
- **33%** Will be relying more on the legitimate interest processing basis under the GDPR than they currently do

- **Heavy reliance on consent today** - over a third of organisations use it for the majority of their processing (38%) and over a half (53%) for limited processing
- **Only a third or a quarter of organisations currently comply with new GDPR consent requirements** - only 22% gather consent for separate processing operations, 34% are able to demonstrate consent in all instances, 3/4 require consent as a condition of product/service.

**Data Protection Impact Assessments (DPIAs)**

- **50% +** conduct DPIAs in circumstances required by GDPR
- **1/3** have a framework and procedures to identify & classify risk
- **40%** already incorporate Privacy by Design for all new projects
- **1/4** use in-house or commercial automated system for DPIAs
- **2/3** of current DPIAs are carried out in Word/Excel format
- **42%** already incorporate Privacy by Design in some instances
Security Design Assessments

- Conduct Security Design Assessments on **NEW** IT systems: 59%
- Only conduct Security Design Assessments on **EXISTING** IT systems: 41%

Data Classification & Lifecycle Management

- 1/3 of organisations currently tag sensitive content
- 40% do not know how data is treated or processed throughout its lifespan
Data Inventories

1/2
have internal data inventory/record of processing

60%
have inventories of international data transfers

1/2
have no data inventory or internal records of processing with information required by GDPR

Breach Notification

What measures and procedures do you currently have in place to respond to data breaches?

- Internal reporting procedures / hotlines: 75.6%
- Incident response plan: 77.6%
- Incident response team: 63.5%
- Conduct dry-run/data breach scenarios: 33.3%
- Cyber insurance coverage: 31.4%
- PR and media consultant retained: 32.7%
- Forensic experts retained: 28.2%
- None: 7.1%
- Other: 10.9%

Great majority (64-78%) have breach notification reporting, response plan and team.

But just under a third have PR, media and forensic teams in place, conduct dry-run and have cyber insurance.

77% are subject to a data breach reporting obligation, or voluntary reporting – under US, E-Privacy, national EU or other law.
Controller – Processor Relationship & Agreements

Are Controllers reviewing and negotiating current agreements?

- 1/3 Are in progress
- 40% Have not yet started

Majority of organisations’ standard processing agreements already reflect some of the new GDPR requirements (76%)

Only a half have contracts that address individual rights and require processor to provide information (1/2)

Controller Processor Agreement

Do your standard data processing terms include additional terms required by the GDPR?

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract requires processor to make information about the processing available to the controller</td>
<td>N/A 12.7%</td>
</tr>
<tr>
<td>Contract requires the processor to provide assistance in respect of regulatory queries</td>
<td>52.1%</td>
</tr>
<tr>
<td>Contract requires processor to notify data breaches</td>
<td>68.3%</td>
</tr>
<tr>
<td>Contract addresses data subject rights</td>
<td>73.2%</td>
</tr>
<tr>
<td>Contract prevents sub-processing without consent</td>
<td>56.3%</td>
</tr>
<tr>
<td>Contract imposes duty of confidentiality on relevant staff</td>
<td>70.4%</td>
</tr>
</tbody>
</table>

- A great majority of standard terms already include new requirements of the GDPR.
- Just over a half of organisations address individual rights in contracts and require processor to provide information about processing.
Questions?

Resources
Some Tools to Help Organisations

LEARN

GDPR Benchmark Report
Download full report

White Paper
The Operational Impact of the European Union General Data Protection Regulation (GDPR) on IT

GDPR Blog Series
More ways to learn

AvePoint’s GDPR Solutions
Tools for GDPR compliance

www.avepoint.com/GDPR

DO

AvePoint Privacy Impact Assessment System
Our free privacy impact assessment tool exclusively distributed by the International Association of Privacy Professionals (IAPP)

https://iapp.org/resources/apia/
Gracias | Ευχαριστώ | Danke | Grazie | Hvala | Obrigado | Kiitos | شكرا | 谢谢
---|---|---|---|---|---|---|---|---
Ahsante | Teşekkürler | متشكرم | Salamat Po | Cám ơn | شكرا | Terima Kasih | Dank u Wel | Tack
---|---|---|---|---|---|---|---|---
ধন্যে | Köszönöm | ありがとうございました | ขอบคุณ | Muğlum | شكرا | ขอบคุณ |  obrigado | Tack
---|---|---|---|---|---|---|---|---
多謝 | 多謝 | 多謝 | 多謝 | 多謝 | 多謝 | 多謝 | 多謝 | 多謝

**Questions?**