Building YOUR Privacy Program: One Size Does Not Fit All

Justine Gottshall  
Partner, InfoLawGroup, LLP  
Chief Privacy Officer, Signal

Jgottshall@infolawgroup.com

Adam Nelson  
Executive Consultant  
Global Data Privacy Lead  
IBM Security Services

acnelson@us.ibm.com

#PrivacyAcademy

#CSACongress
Building YOUR Privacy Program: One Size Does Not Fit All

• Privacy Program Drivers
• Data Protection is a Global Issue
• Where to Start
• Consider Your Structure And Build Your Core Team
• Everyone Needs Friends: Build Your Cross Functional Organization
• Provide Strategic Leadership
• Build a Framework
• Build a Roadmap: Steps for Consideration
• 10 Key Roadblocks to Avoid
• 10 Key Takeaways
Privacy PROGRAM Drivers

There are five key drivers behind a formal global privacy program including:

- **Increased regulation** of the collection, notice, use and storage of personal information in countries throughout the world

- **Globalization** due to growth and continued interaction between people and business units, third parties, and governmental regulation

- **Overall data governance**. The need to evaluate and manage data management procedures (e.g., global processing requirements, data flows)

- The need to manage an extended network of suppliers, contractors and consultants and other third parties that work together to provide products and services to the market

- **Increased sensitivity** of data incidents and social network profiling has made customers (e.g., employees, clients and consumers) sensitive to the risks associated with unauthorized disclosure of personal information
Data Protection is a Global Issue – but how you address depends on many factors

• It’s not just the EU anymore – although the EU remains active
  ➢ Changes coming in Europe – and more active enforcement
  ➢ Asia
  ➢ Latin America
  ➢ Canada, Mexico and enhanced regulatory environment in the United States
  ➢ Comprehensive data protection laws now exist in over 90 jurisdictions

• Uneven Enforcement

• Do these laws apply to my organization?
Data Protection is a Global Issue – but how you address depends on many factors

And it’s not just a web site, app or online service – cross border transfers occur for many reasons, including:

• E-commerce
• Cloud computing, SaaS
• Vendors processing data
• Customer and technical support
• Backup and archives
Data Protection is a Global Issue – but how you address depends on many factors

Factors to Consider:

• Where are our offices located – do we have any “boots on the ground”?
• Do we otherwise have assets located in other jurisdictions?
• Where are our servers located?
• Are we directly marketing our products or services to residents of other countries?
• What language is our web site/app/etc. presented in? Are there options for the user to choose?
• Is sensitive data involved?
• Are there easy compliance steps that we could take?
• What is the enforcement history in the jurisdiction?
Where to Start?

• This can vary depending on your organization’s reach and risk profile
• A Privacy Office need to be scalable to address corporate needs
• Suggested First Steps
  ✓ Identify your data and the regulations to which you are subject
  ✓ Identify key stakeholders
  ✓ Identify the governing functional area (e.g. Compliance, Legal, Information Technology, Chief Financial Officer)
  ✓ Identify existing privacy related activities in your organization
Consider Your Structure And Build Your Core Team

A privacy office typically involves one or more of the following personnel:

• Data Protection Officer or Chief Privacy Officer
• Privacy Director
• Privacy Program Manager
• Privacy Analyst
• Privacy Attorneys
• Regional Data Protection Leads or Data Protection Officers in each jurisdiction
• Line of business privacy representatives
Consider Your Structure And Build Your Core Team

Model I

**Core Team**
- Leads Data Privacy Activities

**Executive Steering Committee**
- Reviews Major Privacy Initiatives

**Data Protection Officers or Country Leads**
- Advisory Role

---

Model II

**Crossborder Leads**

**Data Security**

**Privacy Working Group**

**Audit**

**Information Technology**

**Business**

**Legal / Compliance**
Consider Your Structure And Build Your Core Team

- CPO
- Marketing
- IT
- Sales
Consider Your Structure And Build Your Core Team

<table>
<thead>
<tr>
<th>Core Team Model</th>
<th>Privacy Council Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agile</td>
<td>Longer decision making process</td>
</tr>
<tr>
<td>Stronger ability to make policy</td>
<td>Business Unit Decisions may need to be a coordinated effort</td>
</tr>
<tr>
<td>Focused forum to discuss and evaluate corporate privacy needs</td>
<td>No Forum to discuss all privacy issues that affect organization</td>
</tr>
<tr>
<td>Full time privacy team</td>
<td>Generally not full time privacy professionals</td>
</tr>
<tr>
<td>Central decision making authority</td>
<td>Corporation may not perceive privacy council as a central decision making authority</td>
</tr>
</tbody>
</table>

Key is YOUR organization’s culture, structure, size, risks, resources (internal and external), and needs.
Provide Strategic Leadership

What works for YOUR organization?
Provide strategic leadership

Corporate Guidance and Day to Day Privacy
- Provide business-focused solutions that protect personal data while enabling business development and growth
- Implement privacy by design
- Provide awareness, tools and compliance across the business

Policy
- Establish and maintain (global) privacy policy, privacy statements, and data governance practices that address data privacy regulations

Framework
- Develop and maintain the appropriate framework upon which you process and transfer personal data. Have a governance structure that can influence strategic architecture decisions.
Provide strategic leadership

Thought Leadership

• Have a mechanism whereby the privacy governance team can provide thought leadership to senior executives.

• Ensure there is a forum where senior data privacy, security, information technology and business leaders can prepare for new regulations.
  • Extend this thought leadership for the benefit of your clients, customers, and partners.

Strategy

• Establish and maintain objectives, goals and tactics to support your privacy governance model.

• Think long term. Where do you want to be in 12, 24, 36 months.
Provide strategic leadership

**Third Parties**

- How does the organization interact with Third Parties?
- Do you have Agreements in place?
- What is your vendor management process?
- Do you Audit?
- What happens at the end of the relationship?
Everyone Needs Friends: Build Your Cross Functional Organization

- General Counsel
- Chief Compliance Officer
- Chief Financial Officer
- Chief Operational Officer
- Chief Information Officer
- Records and Information Management
- Procurement Director
- Global Information Security
- Country Leads
- Human Resources
- Audit
- Marketing
- Business Development and Sales
- Business Unit Representation
Build a Framework

• You need a guidance document that will frame all your discussions on privacy – the “Framework”

• This document will be the basis for your privacy policy, your privacy statement(s) and all your privacy activities

• Helps Regulators understand your approach toward data protection

• Consider leveraging generally accepted international standards to develop your framework

• Can include a mission statement
Build a Framework – And you don’t have to start from scratch

Useful References

• Your organization’s individual business approach and objectives
• Defined industry guidance
• FTC Regulation, precedent and guidance.
• Guidance papers from California and other State Attorney Generals
• Department of Commerce – Privacy Green Paper
• The White House – Privacy Guidance/Model Privacy Impact Assessment
• FIPP’s (Fair Information Practice Principles)
• ISO 29100 – Privacy Data Protection Standards
• ISO 22307 – Privacy Impact Assessments
• Organization for Economic Cooperation and Development (OECD)
• AICPA/GAPP
• EU Data Protection Requirements (Existing and Proposed)
Build a Roadmap: Steps for Consideration

• This is essential piece for a privacy forward strategy
• Is a “time boxed” list of next steps, usually in order of priority
• Provides direction to the team and key stakeholders regarding their next steps
• Based upon corporate needs and compliance responsibilities
• Should tie into framework requirements
Build a Roadmap: Steps for Consideration

• Risk Management Evaluation
• Compliance Review
• Data Mapping “follow the data”
• Alignment with Data Security
• Privacy by Design
• Privacy Policy/Privacy Statement review and/or development
• Crossborder Data Transfer Evaluation
• Data Incident Process Review
• Corporate Privacy Training Evaluation
• Metrics Development
• Bring your own device (BYOD)
• Social Media Policy review and/or development
• Local Privacy Requirements
• Vendor Management Review
A bit about data mapping...

• Having a comprehensive map of your data is extremely useful for legal, compliance, security and business reasons

• Reality Check: Most organizations do not have a data map

• For privacy, it is important to at least know where your protected information is located.

• One of your first projects should be to locate your information

• Initially, all that is needed is
  – Data Type
  – Location
  – Countries transferred to (If applicable)
  – Encrypted (At rest/in transfer)
  – Individual Data Owner
  – Business Unit Owner
8 Key Roadblocks to Avoid

1. Forgetting that privacy is an essential aspect of corporate governance and risk management, not a luxury
2. Failing to fully empower the privacy function – “privacy matters” must be a top-down proposition
3. But also, failing to integrate across the business (and not just IT/IS)
4. Not prioritizing based on your specific risk
5. Not obtaining buy-in from all relevant business teams
6. Forgetting that policies are not enough -- implementation and actual compliance is key
7. Failing to train – everyone
8. Letting perfection be the enemy of great (or at least a really good start)
10 Key Takeaways

1. One size really does NOT fit all for developing a privacy program
2. Start with your risk profile. Your risk profile is unique and the essential foundation for your privacy program.
3. Consider the culture of your organization and what will work for you. You are looking for compliance not to just “check the box.”
4. There is the doing and the writing/policies. Both are important.
5. Although it seems like there are a plethora of regulations – and there are – key accepted principals exist and are a good place to start
6. Not every regulation applies to you
8. Don’t let great (or perfect) be the enemy of good. You might not get to 100% right away. But 90% is much better than 0%
9. “Everyone is doing it” is NOT the same as this is the way we should do it
10. Create a culture of privacy and compliance.
External Resources

• Regulators – Have a meet and greet
• Article 29 Working Party Guidance – Representatives from Data Protection Authority of each EU Member State
• Legal Associations (ABA, CBA, ISBA, EU/Asia Local Groups)
• Privacy Associations (IAPP, Privacy and American Business, Future of Privacy Forum)
• Outside Counsel or Consultant
• Social Media
  • LinkedIn
    ➢ Privacy Professionals
    ➢ International Association of Privacy Professionals
    ➢ Many, many other “Groups”