COMPLIANCE WEEK WEST

NOV 14-15 2013 ROSEWOOD SAND HILL MENLO PARK CA

THE INTERSECTION OF ETHICS, COMPLIANCE, PRIVACY & BIG DATA

#CWWEST13

Building a Strong Privacy Function

Mark Diamond, President & CEO, Contoural

Harvey Jang, Director, Privacy & Information Management, Hewlett-Packard

Laura Hamady, Chief Privacy Officer, Groupon

Moderated by **Matt Kelly**, Editor & Publisher, Compliance Week

COMPLIANCE WEEK WEST

NOV 14-15 2013 ROSEWOOD SAND HILL MENLO PARK CA

Mark Diamond

President & CEO

Contoural

COMPLIANCE WEEK WEST

NOV 14-15 2013 ROSEWOOD SAND HILL MENLO PARK CA

Reactive vs. Proactive Privacy

Reactive

- Breach Response
- Containment
- Notification
- Investigation

HR Records

Residence and Geographical Data

PCI

Personally Identifiable Information

Employee Data

Protected Healthcare Information

Proactive

- Data Security Classification Policy
- Data Mapping
- Repository Management
- Remediation
- Defensible Disposition
- EU 2015 Preparation

Data Security Classification Policy

Potential attributes

- Privacy: customer data, employee data, health data, geographical
- Sensitivity: financial data, NDA data, IP, trade secrets, internal, public, etc.
- Access Controls: Who can see information

Current frameworks and standards

- HIPAA
- Data Protection Initiative
- FIPS 199 – confidentiality (preserve, authorize, access, disclosure), integrity (change or destruction) and availability
- ISO 27001, 27002 – information security controls, other forms of risk treatment

Best Practices

- Incorporate privacy, confidential, IP into a single standard
- Keep it simple (four categories)
- Adjust classification "buckets" to fit current needs
- Incorporate authentication, custodians
- Considering integrating with records classifications (do it once approach)

Data Mapping

A data map is an inventory of the data sources that inform prevention activities. It tells you **what you have**, **where it is**, and **who is responsible** for managing it. A Data Map may be a document, a diagram, a database, or an application.

Common types of data maps:

- Application & Infrastructure
- e-Discovery
- Records & Content Management
- Compliance
- Privacy & Sensitive Information
- Super Map (hybrid of above)

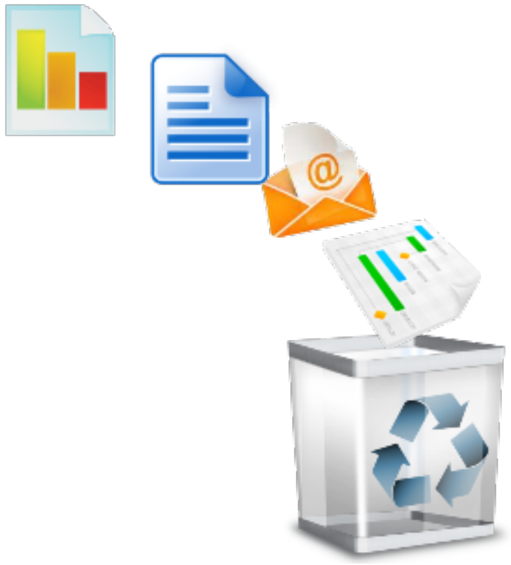
Data Privacy Maps Typically Contain:

- Privacy: PII, PHI, PCI
- Sensitivity: Financial Data, IP, Trade Secret
- Data Classifications: Public, Internal, Restricted
- Data Flows / External Data Transfers

Most Secure: Deleted Privacy Information

Develop a Defensible, Ethical Process

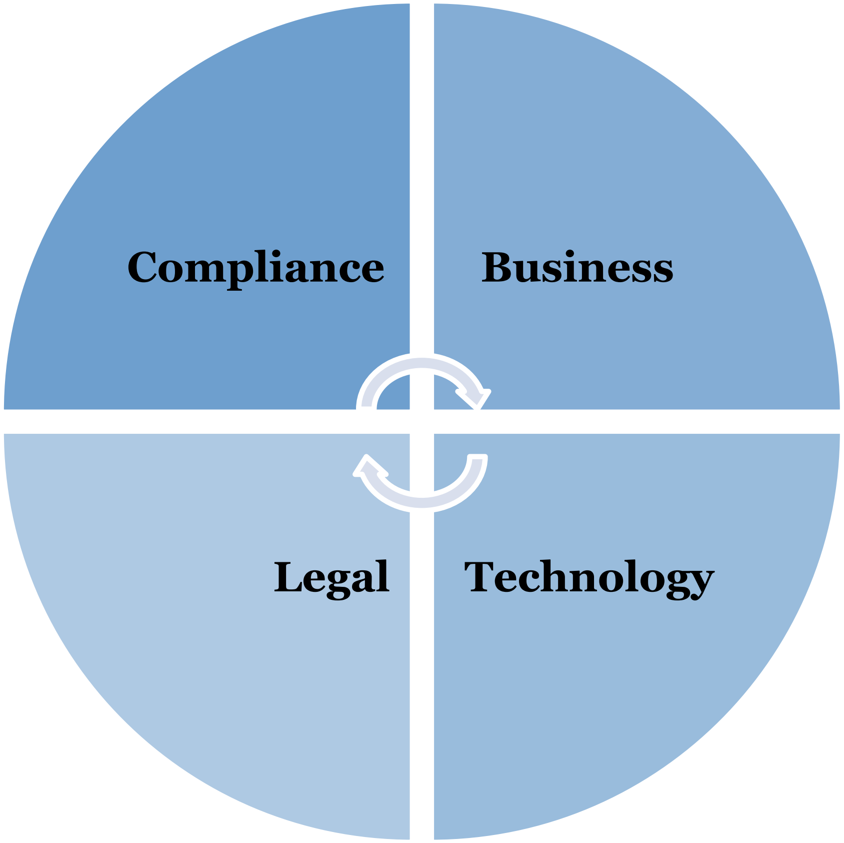
1. Good faith, routine process FRCP Rule 37(e)
2. "…designed, programmed, and implemented to meet the party's technical and business needs" (should be programmed and automatic in recycling, overwriting, updating, or expiring) FRCP Rule 37(f)
3. Deletion supported in policy
   Keithley v. The Home Store.com
4. Identify records to be saved in compliance with regulatory requirements
5. Defensible legal hold processes
6. Monitor and audit the effectiveness of the compliance program (U.S. Sentencing Guidelines)



Approach it Together

- Privacy
- Audit
- Compliance
- Records Management

- Finance
- Business Units
- HR
- End-users
- M&A



- Litigation/ eDiscovery
- Employment
- IP
- Corporate

- Infrastructure
- Applications
- Information Security

www.Contoural.com

White Papers

- How to Prevent Employees from Hoarding Documents
- Is It Time for Autoclassification Part 1 & 2
- Metrics for Information Governance
- Impact of International Regulations

Recorded Webinars

- Developing Effective In-house Discovery Response Programs
- Can We Get Employees to Change
- E-mail Archiving School for Legal
- E-mail Archiving School for IT

Articles

- Four Keys for Getting Employees to Change Their Document Retention Habits *Inside Counsel Magazine*
- Who Should Own Records Information Management, Legal or IT*? Inside Counsel Magazine*

Onsite Seminar

- Complimentary Onsite Two-hour Information Governance Seminar (2 hrs CLE)

Harvey Jang

Director, Privacy & Information Management

Hewlett-Packard

Accountability

LIABILITY

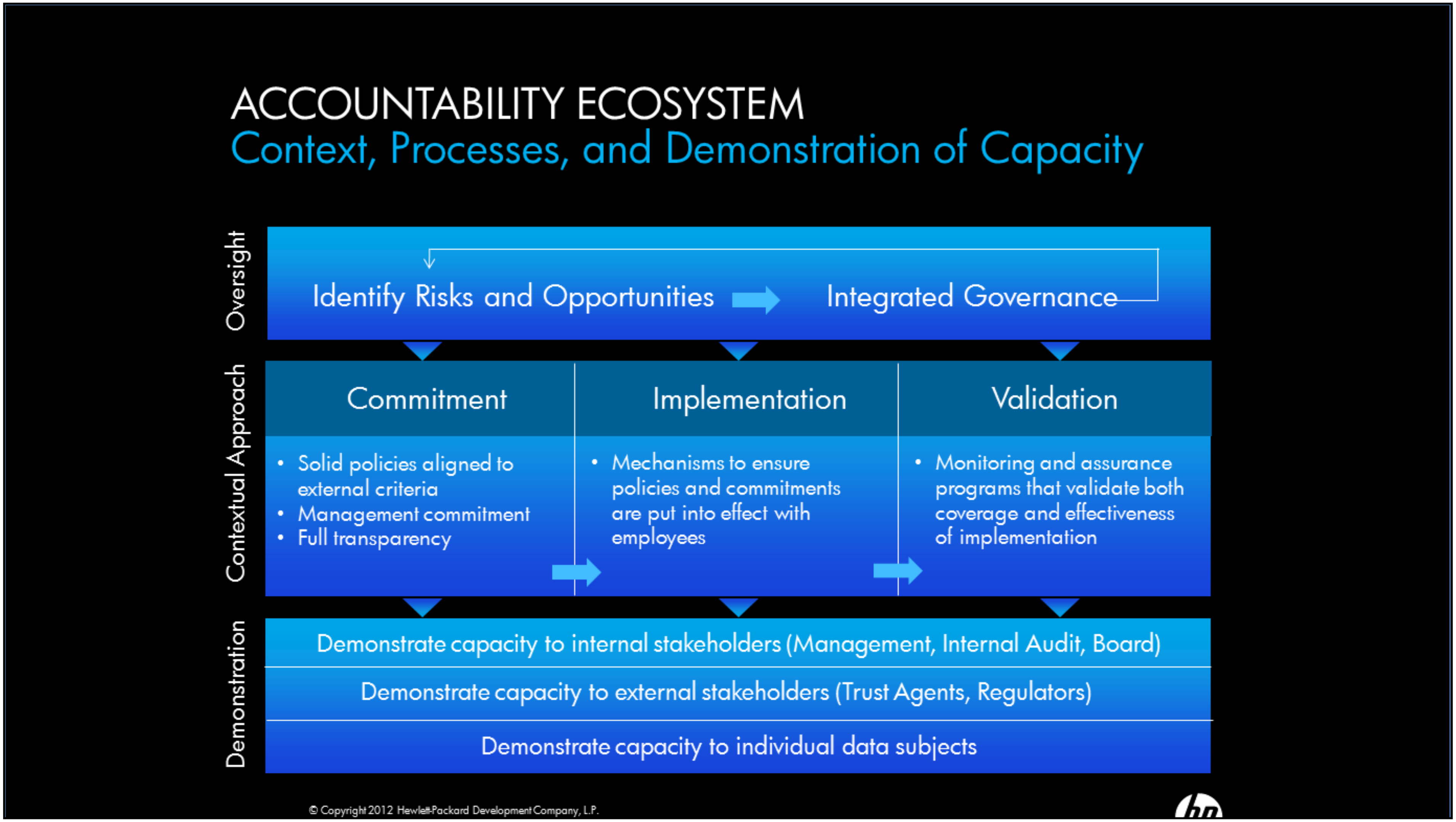
Decisions are made based on local laws and regulations

- Focuses on minimum standards
- What is legally defensible?
- What is the likelihood and impact/consequence of enforcement?

ACCOUNTABILITY

Decisions are made based on a set of ethics- & value-based criteria in addition to liability

- Tie to company values
- All employees accountable for good stewardship of data
- Real, effective & based on expectations



ACCOUNTABILITY ECOSYSTEM

Context, Processes, and Demonstration of Capacity

- Solid policies aligned to external criteria
- Management commitment
- Full transparency

- Mechanisms to ensure policies and commitments are put into effect with employees

- Monitoring and assurance programs that validate both coverage and effectiveness of implementation

Demonstrate capacity to internal stakeholders (Management, Internal Audit, Board)

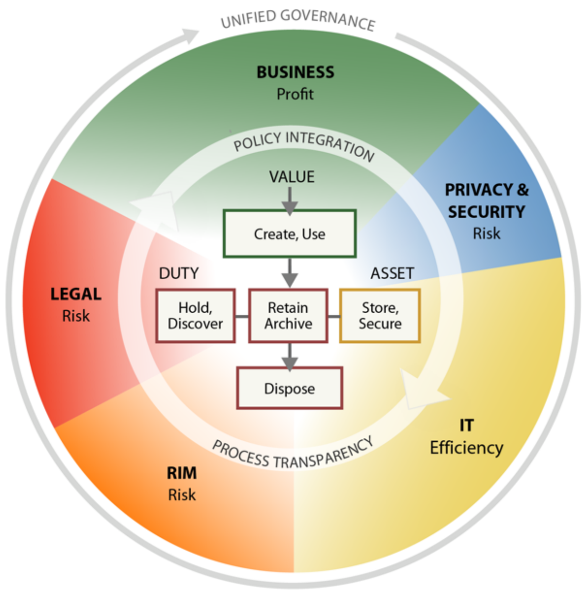
Demonstrate capacity to external stakeholders (Trust Agents, Regulators)

Demonstrate capacity to individual data subjects

Integrated Governance

Information Governance Reference Model (IGRM)

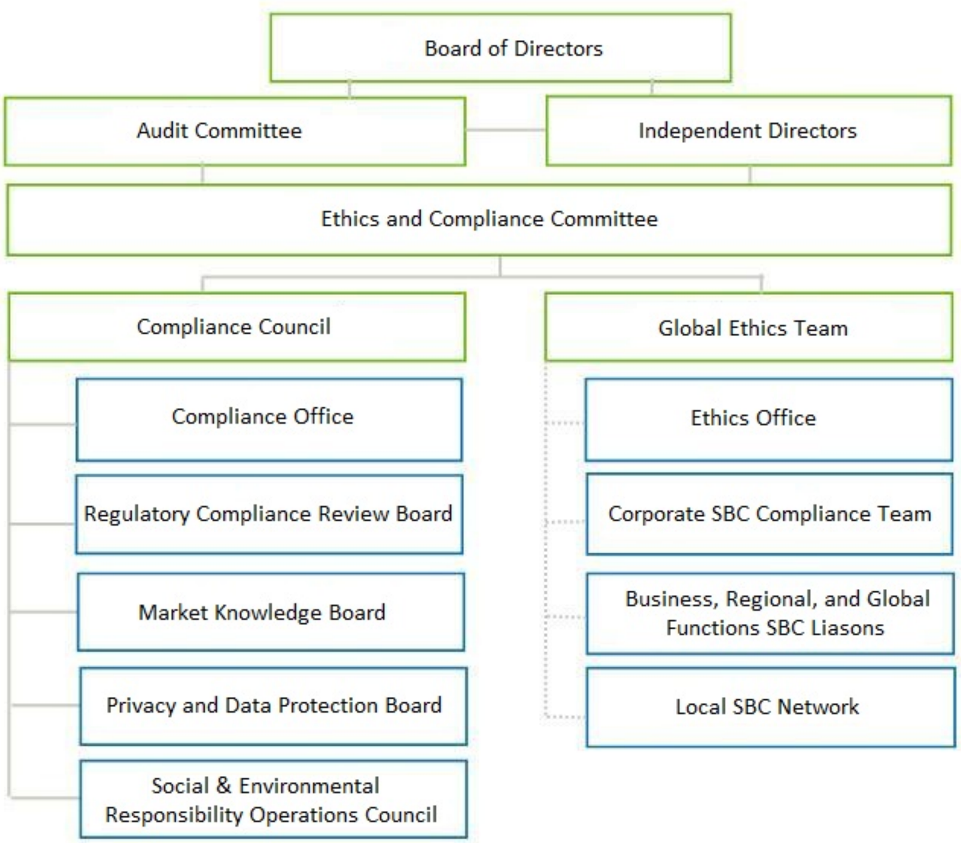
Linking duty + value to information asset = efficient, effective management



Duty: Legal obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific container of information



Board of Directors

Audit Committee

Independent Directors

Ethics and Compliance Committee

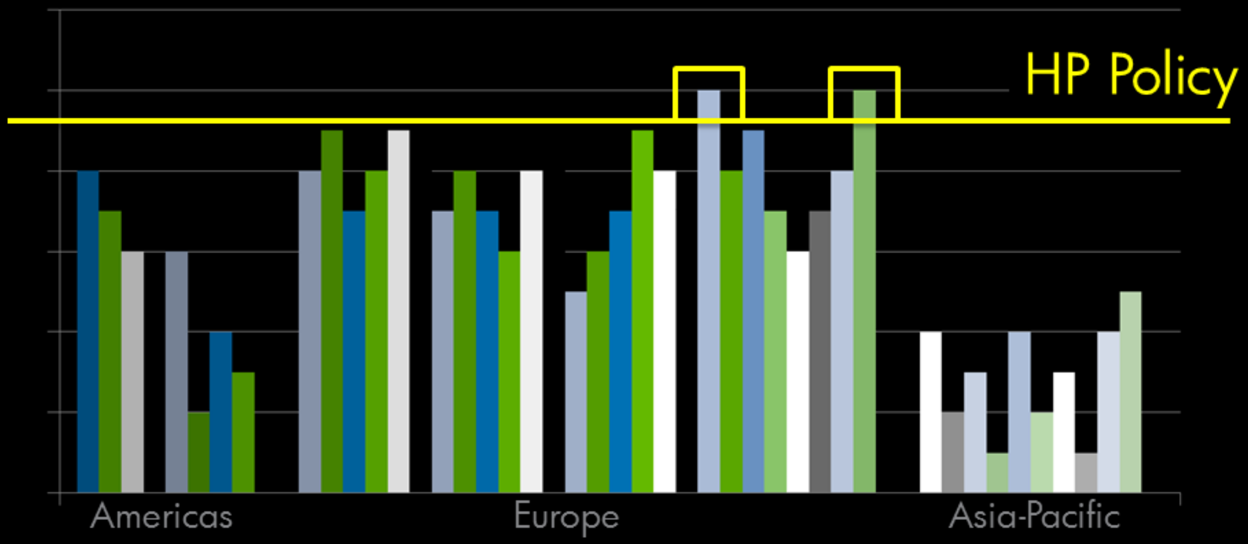
Compliance Council

- Compliance Office
- Regulatory Compliance Review Board
- Market Knowledge Board
- Privacy and Data Protection Board
- Social & Environmental Responsibility Operations Council

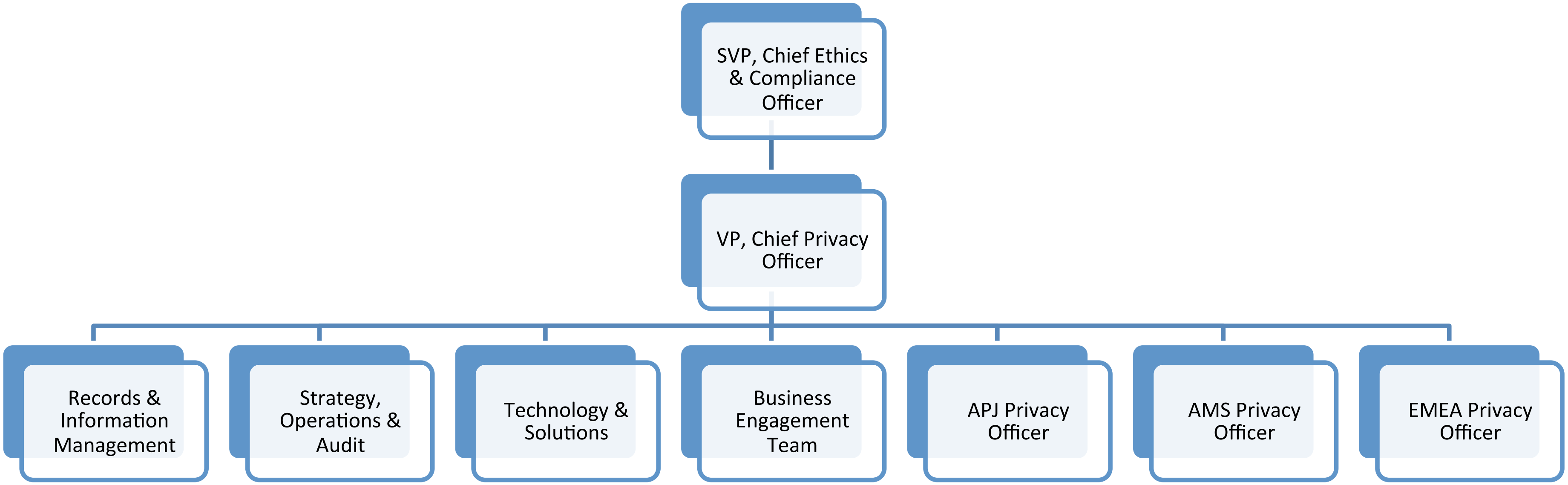
Global Ethics Team

- Ethics Office
- Corporate SBC Compliance Team
- Business, Regional, and Global Functions SBC Liasons
- Local SBC Network

Global Privacy Laws



Privacy Organization Structure



SVP, Chief Ethics & Compliance Officer

VP, Chief Privacy Officer

Records & Information Management

Strategy, Operations & Audit

Technology & Solutions

Business Engagement Team

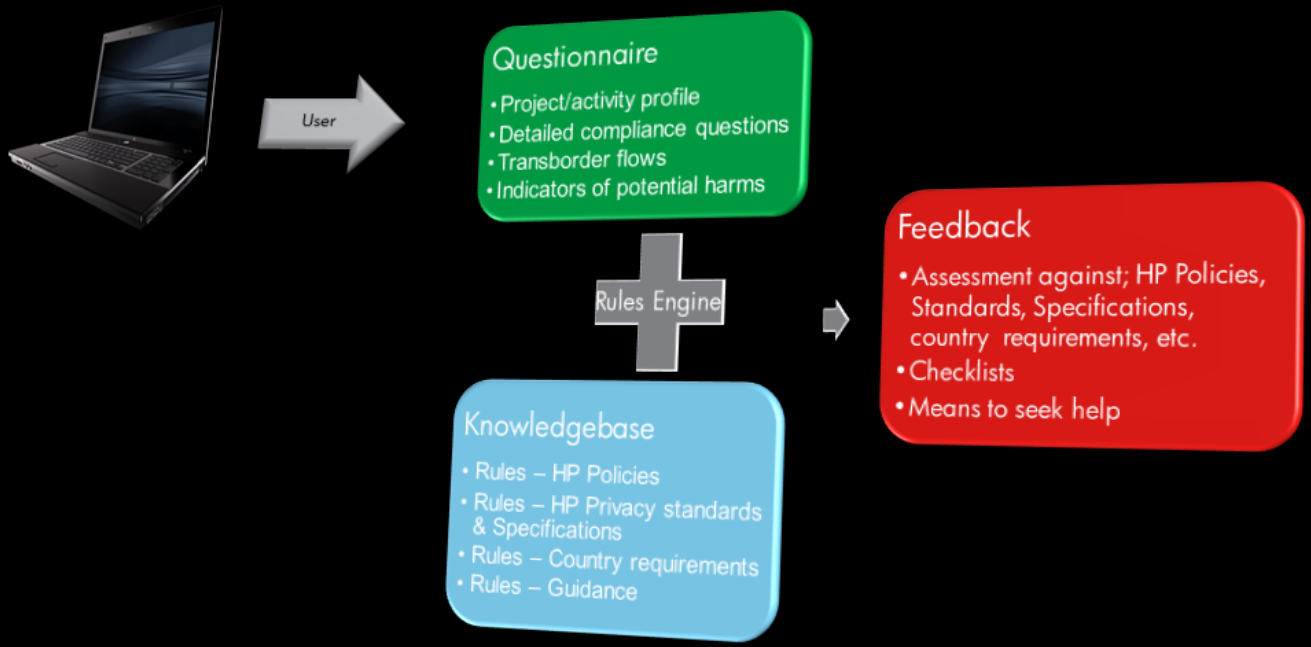
APJ Privacy Officer

AMS Privacy Officer

EMEA Privacy Officer

Effective Implementation

Ensuring our policies and standards are implemented effectively



Questionnaire

- Project/activity profile
- Detailed compliance questions
- Transborder flows
- Indicators of potential harms

Knowledgebase

- Rules – HP Policies
- Rules – HP Privacy standards & Specifications
- Rules – Country requirements
- Rules – Guidance

Feedback

- Assessment against; HP Policies, Standards, Specifications, country requirements, etc.
- Checklists
- Means to seek help

Demonstration

- Management Reporting
- Audit - internal and external
- EU/US Safe Harbor
- Model Contracts
- Binding Corporate Rules – Controller / Processor
- APEC Cross-Border Privacy Rules

Laura Hamady
Chief Privacy Officer
Groupon

Protecting Privacy at a Young Company

- Groupon is celebrating 5th birthday
- Explosive organic domestic growth, and global growth by acquisition
- First three years: start-up culture (premium on innovation, growth and autonomy)
- Business continues to evolve at speed; offering new services and products where personal data is increasingly central

Develop Allies: Lead via Innovation & Integration

In the beginning there was a guerrilla…

- Legal team of one; used many tactics
- Using products, experimenting, asking questions
- Learning the back-end; how and why to offer informed advice & alternatives
- Integrating and forging stand-alone relationships of trust and allegiance with security teams (app sec, product sec, site integrity, IT)
- Leveraging resources; allegiance and partnerships with HR and internal audit

Integrating Privacy: Relevancy & Responsibility

Be present, remain relevant

- Learn the technology
- Don’t advise without dialogue: ask questions, suggest alternative solutions, best practices
- Solutions should be understood tangibly: how does this promote the best interest of the company, and enhance the experience and rights of customers?
- How much does it cost? Why is it worth it?

Establish baseline standards

- Standards should be as holistic and international as possible
- Engage and share ownership locally
- Teach and foster internal awareness of externally-facing statements and standards
  - Safe Harbor
  - Model Contracts
  - Privacy Statements
  - Security Statements

Iterative Approach to Solving Privacy Challenges

Do more with less…

- No stand-alone privacy function; housed in U.S. legal regulatory & government affairs function
- Stay abreast
  - Cybersecurity issues
  - Cookies and tracking
  - Geolocation data
  - Mobile
  - Payment services
- Capitalize on contingencies
- Persuade privacy skeptics

Basic to better…

- Lay tripwires
- Limit and proceduralize access to data
- Deploy mandatory trainings
- Hold practical trainings
- Conduct awareness-raising exercises
- Evangelize privacy-by-design framework to encourage security and collection limitations into core design

The Future is Easier

- Increased international coordination and centralized standards
- Recognition of privacy impact on business
- Company maturation and need to compete for consumer trust