CHANGE MANAGEMENT

FROM MERE PRIVACY COMPLIANCE TO BUSINESS STRATEGY

12 December 2013
15:00 – 16:00

www.privacyassociation.org/congress
THE MANDATE OF THE CPO

Purpose
Responsible for addressing key data protection compliance risks by providing in-depth expertise, guiding the business on how to adequately mitigate these risks and increase compliance maturity levels with regards to these risks.

Key Functions
- Provide specialist guidance
- Provide specialist risk assessments and assurance views

Key Accountabilities
- Global risk exposure assessment including new or changes to regulations
- Provide global expertise in key risks to improve compliance risk understanding and mitigation
- Support in development and maintenance of policies & training
- Support in risk assessments performed by the business in relation to key data protection compliance risks
THE CPO'S BALANCING ACT

Chief Privacy Officer

Enabling

Controlling

www.privacyassociation.org/congress
THE DILEMMA OF THE CPO

- International Projects
- Audits
- IT-Security
- Register
- Trainings
- Privacy Impact Assessment
- Filings
“COMPLIANCE IS EITHER A STATE OF BEING IN ACCORDANCE WITH ESTABLISHED GUIDELINES, SPECIFICATIONS, OR LEGISLATION OR THE PROCESS OF BECOMING SO”
CONSEQUENCE:
MORE PAPER THAN PRIVACY!
Military Strategy: “The utilization during both peace and war, of all of the nation's forces, through large scale, long-range planning and development, to ensure security and victory” (Random House Dictionary)

A strategy is a long term plan of action designed to achieve a particular goal.

Business strategy: The art and science of enabling an organization to achieve its objective.
WHAT TO DO
GLOBAL PRIVACY COMPLIANCE PROGRAM
STRATEGIC DEVELOPMENT

STAGE 1
Compliance Approach
- action-oriented
- minimum requirements
- legal focus

• Laws and Regulations

STAGE 2
Risk-based Approach
- competitive
- needs to protect
- business-oriented

• Identified Business Risks

STAGE 3
Global Approach
- best-in-class
- mutually recognized
- globally binding

• Binding Corporate Rules

Achieving a higher degree of compliance effectiveness while responding more efficiently

www.privacyassociation.org/congress
RIGHT BALANCE OF "COMPLIANCE" AND NEW TOPICS

Innovative

Complexity of the task

Necessity?

Investment focus of data privacy "newbies"

Compliance & Duties

Investment focus of data privacy "pros"

Business Enabler

Management "basis"

Importance of the task

Strategic development

Operational "hygiene"

Initiative 1

Initiative 2

Initiative 3

Initiative 4

Initiative 5

Initiative 6

Initiative 7
STRATEGIC ROADMAP FOR THE DEVELOPMENT OF A DATA PRIVACY MANAGEMENT SYSTEM

Organization & Governance

2013

- Data Privacy Strategy
- International Governance-Model
- Target Operating Model (TOM)
- Management of Complaints and Incidents
- Process Manual

2014

- KPI System / Reporting
- Introduction BCR
- Programme for Training and Awareness
- Data Privacy-Audits / PIA
- Regularly Risk Assessments
- Effective Prior Checking

2015

- Center of Excellence (CoE) & Projektbegleitung
- Privacy by Design / ReDesign
- Procedure of anonymizing data
- Concept of Deletion
- Automation / Tool Support

Processes

Technology

www.privacyassociation.org/congress
DESIGN OF A PRIVACY MANAGEMENT PROCESS

Plan
- Establishment
  - Guidelines & Policies
  - Vision & Strategy
  - Risk assessment / PIA

Implementation
- Organization & Controls
- Targeting of data privacy-risks
- Operations & Resources
- Incident management

Optimization
- KPI System & Reporting
- Communication
- On-going improvement

Monitoring
- Regular audits
- Monitoring & Reviews
- Check of the efficiency

Act
- Check of the efficiency

Do
- On-going improvement
<table>
<thead>
<tr>
<th>Number</th>
<th>Metrics</th>
<th>Based on privacy risk impact</th>
<th>Performance Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Legal / Regulatory</td>
<td>Financial</td>
</tr>
<tr>
<td>1</td>
<td>Notice and consent - % of websites compliant with notice and consent processes (for commercial consumer information)</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td>Commercial activities only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Number of privacy audit issues open and % of privacy audit issues overdue (measured against total number of privacy issues open)</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>3</td>
<td>Increasing number of self-reported issues (measured by BU; more self-reporting is encouraged and positive)</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>4</td>
<td>Number of data privacy compliants (excluding data privacy breaches) escalated to the Privacy Office and % of complaints not resolved (measured against total number of compliants received) in a resoneable amount of time</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>5</td>
<td>Number of privacy related government or regulatory authority findings requiring intervention</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>6</td>
<td>Number of data privacy breaches by seventy (Seventy refers -&gt; L1/L2/L3 as defined by Company A policy)</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>7</td>
<td>Number of data privacy breaches by source (Source indicates -&gt; Laptop, data cards)</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>8</td>
<td>Number of data privacy breaches by reported by source (Reported by indicates -&gt; 3rd party, Company A employee)</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>9</td>
<td>% of targeted employees trained in general privacy training within set timescales</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>10</td>
<td>% of targeted employees trained in BCR training within set timescales</td>
<td>H</td>
<td>M</td>
</tr>
</tbody>
</table>
HOW TO DO IT

WRONG WAY

RIGHT WAY
Management + Change

= Change Management

YES ...
WE CAN!
ELEMENTS OF CHANGE MANAGEMENT

- Involve the top level
- Integrate all levels
- Raise a sense of responsibility
- Communicate consistently
- Dynamic trainings
- Win the individual
- Use variety of media
- Target "human aspects" (Rewards)
## CHANGE MANAGEMENT

<table>
<thead>
<tr>
<th>Make it essential</th>
<th>Make it ready</th>
<th>Make it happen</th>
<th>Make it stick</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Articulate a convincing business need for change</td>
<td>• Assure and install DP responsibility for specific processes</td>
<td>• Involvement in processes</td>
<td>• Line out positive results and further potential</td>
</tr>
<tr>
<td>• Tools &amp; techniques supporting management</td>
<td>• Create desire</td>
<td>• Assure DP culture</td>
<td>• Acknowledge every progress</td>
</tr>
<tr>
<td>• Workshops</td>
<td>• Make it individual</td>
<td>• Create involvement by knowledge</td>
<td>• Demonstrate persistency</td>
</tr>
<tr>
<td>• Sensitize employees upfront</td>
<td>• Pride</td>
<td>• Tools</td>
<td>• Reward self-reporting of issues</td>
</tr>
<tr>
<td>• Create awareness</td>
<td>• Responsibility</td>
<td>• Regular use</td>
<td>• Have audits in place to monitor</td>
</tr>
<tr>
<td>• Create a vision</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ROPI – RETURN ON PRIVACY INVESTEMENT
NUMBER BASED ARGUMENTS

Protection Perspective

Enabling Perspective

www.privacyassociation.org/congress
Dr. Peter Katko
Partner, Head of IP/IT Law

Ernst & Young Law GmbH
Arnulfstrasse 59
80636 München

Telefon +49 89 14331 25951
Telefax +49 181 3943 25951
Mobil +49 160 939 25951
Email peter.katko@de.ey.com

Dr. Stefan Weiss
Global Data Protection Officer,
Director, Legal & Compliance

Swiss Reinsurance Company Ltd
Mythenquai 50 / 60
8022 Zürich
Schweiz

Telefon +41 43 285 4448
Telefax +41 43 282 4448
Mobil +41 79 207 3142
Email Stefan_Weiss@swissre.com

www.privacyassociation.org/congress