Data Protection Developments: Implications for the Insurance Sector Strategies for Compliance

Chris Edwards
DLA Piper's Asia Insurance Symposium, Singapore
9 October 2013
Data Protection – Insurance Industry

- Data Protection in Asia – a snapshot
- The impact on the insurance industry
- Strategies for compliance
Data Protection in Asia – snapshot
Impact on the insurance industry
Strategies for compliance
Data Protection - Personal Data

Information

Data

Personal Data

Sensitive Personal Data
Data Protection – Asia Snapshot

"personal data"

Data Subject

collection - storage - use - transfer - disposal

Data Controller

fairly and lawfully  accurate  secure

for limited purposes  data subject rights upheld

adequate, relevant  not excessive

not kept longer than necessary  adequate protection

Data Processors
(examples)

http://blogs.dlapiper.com/insuranceflashlight/

9 October 2013
Significant developments in the last 3 years. A rapidly maturing DP landscape.

New laws
- Singapore
- Malaysia
- Philippines
- South Korea
- Taiwan

Established regimes
- New Zealand
- Japan

Significant Updates
- Australia
- Hong Kong

Changes expected
- China
- India
- Thailand
Data Protection – Asia Snapshot

Approach to DP Law
- Industry
- Omnibus

Scope of Application
- Holistic
- Public sect. exempt.
- Sect. exempt.

Regulator Powers
- Broad
- Recommend
- Overlapping

Direct Marketing
- India
- Malaysia

Breach Notification
- Yes
- No

Third Party Correction
- Obligations

DPO Requirement
- Yes
- No

Right of Private Action
- Yes
- No

http://blogs.dlapiper.com/insuranceflashlight/
Data Protection – Asia Snapshot

New EU Data Protection Regulation Proposed

- 215 page report / 350 proposed amendments
- designed to strengthen individual rights
- bring laws into the internet age
- more harmonization across the EU

Regulator enforcement

- Google Privacy Policy - EU action sees regulators combining
- Sony Playstation - UK ICO fine

Cross-border co-operation - Article 29 WG / APEC
Observations

- Increase in laws / regulations – economic rather than rights based
- Appreciable differences
- New regulators + enforcement / sanction options
- Global co-operation
Data Protection in Asia – snapshot

Impact on the insurance industry

Strategies for compliance
Impact on the Insurance Sector

Specific focus on industry by regulators – why?

- business model – large customer databases; third parties
- direct marketing activities
- rising number of complaints
A call for pro-active measures:

"I sincerely wish all corporate data users to measure up to customers’ expectations and embrace privacy and data protection as a business imperative, instead of taking a remedial approach when sanction is invoked against them,"

Allan Chiang,
Privacy Commissioner for Personal Data for Hong Kong,
Statement on “HKPA” case - 2013.
Impact on the Insurance Sector

Industry specific guidance - examples:

- Data Access Requests
- Private Investigators
- Direct Marketing
- Personal Information Collection Statements

http://blogs.dlapiper.com/insuranceflashlight/
9 October 2013
Impact on the Insurance Sector

The growth of data privacy / cyber insurance policies

http://blogs.dlapiper.com/insuranceflashlight/

9 October 2013
Data Protection in Asia – snapshot
Impact on the insurance sector
Strategies for compliance
Strategies for Compliance

Comprehensive review of:

- data protection policies, procedures and practices
- determine whether they comply with the requirements set out in relevant best practice guidance

Possible actions include revising:

- personal information collection statements
- forms used to collect personal data
- retention / security policies
- processes & training procedures
- direct marketing activities

http://blogs.dlapiper.com/insuranceflashlight/
Strategies for Compliance

Data on Employees
- Held in all locations

Data Confidential to
- Held in all locations (file / email / cached)
- For main businesses, data processing systems held in X country
- Can include highly confidential data such as medical history or criminal record data

Claims Data
- May be held in all locations (email, files)
- For main businesses, data processing systems held in X country

Commercial Data
- Held in all locations
- Higher risk as the data ‘concentrates’ and becomes material to the group

http://blogs.dlapiper.com/insuranceflashlight/
Strategies for Compliance

Overarching Data Privacy Policy

- On-line policies
- Overseas transfer notifications/consents
- Intra-group data transfer agreement
- Notices and consents at identified data capture points
- Standard third party vendor clauses
- Data retention and destruction policy
- Customer data policies
- Security policies
- HR Policies

http://blogs.dlapiper.com/insuranceflashlight/
Strategies for Compliance

Data flow diagrams

Gap analysis and risk review

Data gathering

Statement of requirements

http://blogs.dlapiper.com/insuranceflashlight/

9 October 2013
Strategies for Compliance

1. Establish Governance and planning
   - Identify stakeholders and establish cross functional teams.
   - Ensure executive level buy-in from organisation.
   - Establish the vehicle for compliance.
   - Agree initial time line for different phases.
   - Agree indicative budget for various phases.
   - Set up regular calls to monitor progress.

2. Conduct Data Assessment
   - Establish main data uses and data flows.
   - Identify an overview of current level of compliance.
   - Identify key risk areas.
   - Raise awareness.
   - Identify who controls the data.
   - Identify which laws apply.

3. Develop Strategy
   - Set the high water mark for standards.
   - Decide on global or regional approach.
   - Prioritise the identified risk areas.
   - Agree approach to "controller" structure and which laws apply.
   - Finalise approach to data transfers.
   - Decide on approach risk (eg: legacy data/existing vendor agreements))
   - Identify priorities for compliance package.
   - Agree time line and budget for different phases.

4. Develop template compliance package
   - Based on high water mark standard.
   - See next slide for example of what the package might look like.
   - Training

5. Apply to each business area/country
   - Make any changes necessary to reflect national law.

6. Implement
   - Update registrations.
   - Implement notices.
   - Roll out new policies and procedures in accordance with the appropriate compliance framework.
   - Execute agreements and make any required national filings.

7. Monitoring and assessment
   - Training for employees.
   - Put in place audit/verification programme.
   - Training for sub-contractors.
   - Annual refresh programme to monitor changes in law which will impact on the compliance solution.

http://blogs.dlapiper.com/insuranceflashlight/
## Strategies for Compliance

<table>
<thead>
<tr>
<th>TASKS</th>
<th>TOOLS AND TEMPLATES:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legitimate processing</td>
<td></td>
</tr>
<tr>
<td>Carry out data usage assessment</td>
<td>Standard consent language.</td>
</tr>
<tr>
<td>Sensitive personal data strategy</td>
<td>Data flow diagrams.</td>
</tr>
<tr>
<td>Data protection gap analysis</td>
<td>Risk assessment reports</td>
</tr>
<tr>
<td>Carry out full data privacy audit</td>
<td>Privacy Impact Assessments.</td>
</tr>
<tr>
<td>Implement privacy notices and consents and</td>
<td>Data Asset Registers.</td>
</tr>
<tr>
<td>access/data sharing policies</td>
<td>Data Usage Assessments.</td>
</tr>
<tr>
<td></td>
<td>Statement of Requirements.</td>
</tr>
<tr>
<td></td>
<td>Access control procedures.</td>
</tr>
<tr>
<td></td>
<td>Privacy by design impact assessments</td>
</tr>
<tr>
<td>International transfer restrictions</td>
<td></td>
</tr>
<tr>
<td>Identify main international data transfers</td>
<td>EC Model Clauses</td>
</tr>
<tr>
<td>Develop data transfer strategy</td>
<td>Consent language</td>
</tr>
<tr>
<td>Implement data transfer strategy</td>
<td>Safe Harbor Certifications</td>
</tr>
<tr>
<td></td>
<td>Intra Group Data Transfer Agreements</td>
</tr>
<tr>
<td></td>
<td>Processor Binding corporate rules</td>
</tr>
<tr>
<td>Data security</td>
<td></td>
</tr>
<tr>
<td>Draft security policy</td>
<td>Data security policy</td>
</tr>
<tr>
<td>Implement data security policy</td>
<td>Vendor agreement processing language</td>
</tr>
</tbody>
</table>
Strategies for Compliance

Governance and accountability

Global data protection policy

Data transfer agreement

Policies and procedures

Statement of requirements

Training and awareness

Verification and audit

DPA notifications

country variations

• HR
• Client data
• Direct marketing
• Records management
• Electronic usage
• Security
• Social media
• Vendors
• Cookie
• CCTV

country variations

country variations

country variations

• Generic code of conduct
• Statement of good practice
• Local law compliance on top of this
• Sets structure for other components

http://blogs.dlapiper.com/insuranceflashlight/

9 October 2013
Data Protection – Insurance Industry
Final Thoughts / Predictions
Data Protection – Insurance Industry

Predictions:

- More active regulators – with an insurance industry focus
- Increasingly educated customers re: privacy + rights of action
- Broader types of penalties for breach
- Focus on being seen “to be doing”
- Opportunity – data privacy insurance policies
- Influence of new EU Regulation + APEC role
- Change!

http://blogs.dlapiper.com/insuranceflashlight/
http://blogs.dlapiper.com/insuranceflashlight/
Data Protection Developments: Implications for the Insurance Sector Strategies for Compliance

Chris Edwards
DLA Piper's Asia Insurance Symposium, Singapore
9 October 2013