The Latest Developments in Cross-border Data Transfer

IAPP ASIA PRIVACY FORUM 2015

Ken Chia, CIPT, Principal, Baker & McKenzie. Wong & Leow LLC
Hilary Wandall, CIPM, CIPP/E, CIPP/US, AVP, Compliance and Chief Privacy Officer, Merck & Co., Inc.

Michael Rose, Office of Digital Services Industries, US Department of Commerce

Baker & McKenzie.Wong & Leow is incorporated with limited liability and is a member firm of Baker & McKenzie International, a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

Agenda

Binding Corporate Rules, Model Contracts, APEC's CBPRs—methods for moving data from one jurisdiction to another are varied, complex and changing on a yearly basis. Get up to speed on the latest developments and receive a framework for examining which data-transfer mechanism is right for your organisation.
Why?
Explosion of Privacy Law Reforms

EU: The New Draft General Data Protection Regulation

Hong Kong: Personal Data (Privacy) Amendment Ordinance 2011

China: Provisions regulating Internet Information Services

South Korea: Personal Data Protection Act came into force in September 2011

Taiwan: Personal Data Protection Act 2010 came into effect 1 Oct 2012

Philippines: Data Privacy Act (August 2012)
Cybercrime Prevention Act (September 2012)

Malaysia: PDPA in force from 15 November 2013

Australia: Amended Privacy Act came into force 12 March 2014

Singapore: PDPA in force from 2 July 2014

India: The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Thailand: Draft privacy law being considered by Parliament

Vietnam: New Consumer Protection Law relevant

Singapore: PDPA in force from 2 July 2014

## Penalties

<table>
<thead>
<tr>
<th>Country</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Australia</strong></td>
<td>Civil and criminal penalties range from AU$340,000 for individuals or AU$1.7 million for corporations</td>
</tr>
<tr>
<td><strong>China</strong></td>
<td>Damages under Tortious Liability Law and amended Consumer Protection Law. Administrative penalties (e.g. a fine) may also be imposed. Business licence revoked in serious cases</td>
</tr>
<tr>
<td><strong>HK</strong></td>
<td>Civil and criminal penalties up to HK1 million + 5 years imprisonment for violations of direct marketing requirements</td>
</tr>
<tr>
<td><strong>Indonesia</strong></td>
<td>Administrative sanctions in the form of warning letters, fines, suspension and deregistration, and criminal sanctions of imprisonment of up to 10 years and/or fine of up to IDR5 billion may potentially be imposed</td>
</tr>
<tr>
<td><strong>India</strong></td>
<td>Damages upto INR 5 crores or more for breach of section 43A of the IT Act. Fine of INR 5 lakhs or imprisonment up to 3 years for any disclosure of personal information with intent to cause harm</td>
</tr>
<tr>
<td><strong>Japan</strong></td>
<td>Statutory penalty – imprisonment with labour up to 3 years and/or fine up to JPY300,000</td>
</tr>
<tr>
<td><strong>Malaysia</strong></td>
<td>Up to RM500,000 fine and/or imprisonment of up to 3 years</td>
</tr>
<tr>
<td><strong>Philippines</strong></td>
<td>Up to Pphp1,000,000 + imprisonment of up to 5 years</td>
</tr>
<tr>
<td><strong>Singapore</strong></td>
<td>Civil fines up to S$1 million; Criminal fines of up to S$100,000 and/or imprisonment of up 12 months for offences such as obstruction, making of false statements.</td>
</tr>
<tr>
<td><strong>Korea</strong></td>
<td>Fine up to KRW 50 million / imprisonment for up to 5 years</td>
</tr>
<tr>
<td><strong>Taiwan</strong></td>
<td>Up to NT500,000 / imprisonment for up to 5 years / civil damages from NT500 to NT20,000 per person per incident</td>
</tr>
<tr>
<td><strong>Thailand</strong></td>
<td>Up to THB 400,000 fine or 2 years imprisonment or both under the Telecommunications Business Act; Up to THB 500,000 fine or 10 years imprisonment or both under the Credit Bureau Act; Up to THB 10,000 fine or 6 months imprisonment or both under the National Health Act; Up to THB 60,000 fine or 6 months imprisonment or both under the Child Protection Act; Civil, criminal, and administrative penalties under the draft Data Protection Bill.</td>
</tr>
<tr>
<td><strong>Vietnam</strong></td>
<td>Fine up to VNP20,000,000</td>
</tr>
</tbody>
</table>
Origins of data transfer requirements and standards
Origins and Core Concepts


- Recognized that OECD Countries have a common interest in protecting privacy and individual liberties; and
- That the spread of national privacy laws should not unduly restrict transborder data flows and the economic and social benefits they bring (concerned that barriers to data flow would impede economic growth)
- Recognized the need for participating countries to establish data transfer restrictions where no equivalent protections for the data exist in another country

Council of Europe Convention 108 (1981)

- Set forth similar requirements for transborder flows of personal data
- Also recognized the concept of “equivalent protection”


- Data transfer restricted outside of EU except to countries with “adequate protection,” if specifically authorised, or pursuant to a derogation


- Intended to enable privacy-respecting regional data transfers and avoid barriers to information flow, and ensure continued trade and economic growth in the region
Country by country transfer restrictions
Australia

– If an organization discloses Personal Data to a recipient outside of Australia, it must take reasonable steps to ensure that the recipient does not breach the APPs. Unless an exception applies, if the recipient handles the Personal Data in a manner that would breach the APPs if that recipient were subject to the APPs, the organization that disclosed the information will be taken to have breached the APPs.

– A key exception is if the recipient to which Personal Data is disclosed is subject to a law or binding scheme which provides the same protection as under the Privacy Act, and there are mechanisms that the Data Subject can access to enforce that law or binding scheme.

– A further exception is if the organization expressly informs Data Subjects that if information is disclosed outside of Australia, the organization will not be responsible for any failure of the recipient to protect the Personal Data in a manner consistent with the APPs, and having been so informed the Data Subject consents to the disclosure.

– Safe Harbor registration may assist in establishing that reasonable steps have been taken if the organization applied Safe Harbor principles to Personal Data from Australia.
China

– Transfers of personal data out of China are permitted so long as the consent of the data subject has been obtained and the effect of such transfer does not harm the interests of the State, cause social instability or infringe another person’s rights.

– Selected regulations suggest that local government authorities in charge of archives should be consulted before the implementation of international data transfers.

– The financial sector, however, is subject to specific restrictions. According to rules issued by the People’s Bank of China, personal financial information collected within China must be stored, processed and analyzed in China unless otherwise exempted.
Hong Kong

- Under Section 33 of the Ordinance, the data user cannot transfer Personal Data, except in certain circumstances, including the following:
  - the data user has reasonable grounds for believing that the destination jurisdiction has substantially similar provisions to the Ordinance;
  - the data subject consents in writing to the transfer; or
  - the data user has exercised due diligence to ensure that the Personal Data will not be treated in a manner which will contravene the Ordinance.

- The above requirements are not yet effective and do not currently form part of the law in Hong Kong. However, there have been indications that section 33 may come into force in the near future.
India

- Organizations in India may transfer Personal Data outside of the jurisdiction provided that
  - the receiving jurisdiction provides a similar level of protection for Personal Data;
  - impacted Data Subjects have been informed or have been provided consent; and
  - that reasonable steps have been taken to safeguard the Personal Data to be transferred.
Indonesia

- Organizations may transfer Personal Data outside of Indonesia provided that impacted Data Subjects have been informed or have provided consent; and that reasonable steps have been taken to safeguard the Personal Data to be transferred.
Japan

- There is no specific requirements for international data transfers, but the organizations in Japan may be required to take reasonable steps to safeguard the Personal Data to be transferred as part of the obligation for necessary and appropriate Security Control Measures to protect Personal Data, and to have appropriate data transfer agreements and/or other prescribed measures put in place for transfer to their data processing service providers.

- Organizations are also allowed to enter into binding corporate rules to secure international data transfers as long as such rules would not have conflicts with the purpose of use for the transferred Personal Data.
Malaysia

- The PDPA prohibits Data Users (and by extension, their Data Processors) from transferring any Personal Data of a Data Subject to a place outside Malaysia, unless:
  - it is a place specified by the Minister and published in the Gazette;
  - the Data Subject has given his or her consent; or
  - any other general exemptions apply.

- The factors that the Minister will take into consideration include: whether or not that place has in force any law which is substantially similar to the PDPA or serves the same purposes as the PDPA; or if that place ensures an adequate level of protection in relation to the processing of Personal Data which is at least equivalent to the level of protection afforded by the PDPA. No places have been so specified by the Minister yet.
Philippines

- The Data Privacy Act does not appear to specifically require that personal information collected from Philippine citizens or residents should be stored or processed in the Philippines. It also does not appear that the Act prohibits the off-shore storage or the transfer of such personal information to foreign jurisdictions. The Act, however, considers the “personal information controller” to continue to be responsible for personal information that may have been “transferred to a third party for processing, whether domestically or internationally.”

- There is an old law, Presidential Decree 1718, that prohibits the transfer of documents or information relating in any manner to any business carried on in the Philippines, unless such taking, sending or removal is:
  - consistent with and forms part of a regular practice of furnishing to a head office or parent company or organization outside of the Philippines;
  - in connection with a proposed business transactions requiring the furnishing of the document or information;
  - required or necessary for negotiations or conclusions of business transactions, or is in compliance with an international agreement to which the Philippines is a party; or
  - made pursuant to the authority granted by the designated representative(s) of the President.

- The Office of the President has yet to issue rules and regulations implementing the law since its passage on August 21, 1980. Hence, the law is not strictly enforced.
Singapore

- The PDPA provides that an organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA.
- Under the Personal Data Protection Regulations ("Regulations"), a transferring organisation is required to take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act.
- “Legally enforceable obligations" include obligations imposed on the recipient under
  - any law;
  - any contract that:
    - requires the recipient to provide a standard of protection that is at least comparable to the protection under the PDPA; and
    - specifies the countries and territories to which the personal data may be transferred under the contract;
Singapore

- any **binding corporate rules** (for related companies) that:
  - require every recipient to provide a standard of protection that is at least comparable to the protection under the PDPA; and
  - specify the recipients of the transferred personal data to which the binding corporate rules apply; the countries and territories to which the personal data may be transferred; the rights and obligations provided by the binding corporate rules; or
- any other legally binding instrument.

- There are no model agreements yet but the Personal Data Protection Commission ("PDPC") has indicated that these should set out protections relating to (i) purpose of collection, use and disclosure by recipient (ii) accuracy (iii) protection (iv) retention limitation (v) policies on personal data protection (vi) access and (vii) correction where personal data is transferred to another data controller. Where personal data is transferred to a data processor, only the “protection” and “retention limitation” obligation are required to be set out in a data transfer agreement.
Alternatively, the transferring organisation can satisfy the obligations if, among others:

- the individual whose personal data is to be transferred gives consent to the transfer after being given a reasonable summary in writing of the extent to which the personal data to be transferred to that country or territory will be protected to a standard comparable to the protection under the Act;
- the transfer is necessary for the performance of a contract between the organisation and the individual; or
- the transfer is necessary for the conclusion or performance of a contract between the organisation and a third party which is entered into at the individual’s request

Given that it is currently not clear what would constitute "a reasonable summary", we would not currently recommend that the organisation solely rely on the consent route unless the organisation has already binding corporate rules in place or enters into a binding legal agreement with the recipients
South Korea

– Organizations may transfer personal data outside of South Korea provided that reasonable steps have been taken to safeguard the personal data to be transferred.

– The PDPA sets out procedures required to be followed by a personal data processor in order to transfer personal data to third parties in other jurisdictions. The Information and Communications Network Act also provides for the procedures for transfers of personal data to other jurisdictions and related protective measures.
Taiwan

Under the PDPA, the central competent authority may restrict international transmission of Personal Data by non-public institutions in any of the following circumstances:

- such transmission involves major national interest;
- such transmission is subject to special provisions of an international treaty or agreement;
- the receiving country lacks proper laws and regulations that adequately protect Personal Data, and the rights and interests of a Data Subject are likely to be injured/damaged; or
- Personal Data is indirectly transmitted to a third country (area) to evade the application of the PDPA.
Thailand

- The Privacy Notification requires that international data transfers must be in line with the rules prescribed by the National Telecommunications Commission.
- The Credit Bureau Act prohibits the transfer of data outside Thailand. Under the Credit Bureau Act, the term “data” covers anything that conveys data relating to credit information or rating, irrespective of the form.
- The draft law on Data Privacy sets out minimum requirements applicable to the disclosure of Personal Data outside Thailand.
Vietnam

- Although there is no provision that specifically addresses international data transfers, organizations or individuals may not supply the personal information of an individual without obtaining the consent of that person or unless otherwise provided by law.
<table>
<thead>
<tr>
<th>COUNTRIES</th>
<th>CROSS-BORDER DATA TRANSFER RESTRICTIONS?</th>
<th>INDUSTRY-SPECIFIC?</th>
<th>EXCEPTIONS</th>
<th>BCRs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Transfer to places specified by the authority (i.e. the &quot;whitelist&quot;)</td>
<td>Transfer to places with comparable standard of personal data protection</td>
</tr>
<tr>
<td>Australia</td>
<td>Yes, the disclosing entity remains liable for any breach by the overseas recipient unless an exception applies</td>
<td>No other than outsourcing guidelines for financial and health industry</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>China</td>
<td>Yes</td>
<td>Yes</td>
<td>×</td>
<td>x</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>Yes but not yet in force</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Indonesia</td>
<td>Yes</td>
<td>Yes</td>
<td>×</td>
<td>x</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Yes</td>
<td>No</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Singapore</td>
<td>Yes</td>
<td>No</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Thailand (Draft Bill)</td>
<td>Yes</td>
<td>Yes</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
APEC Initiatives
APEC initiatives

- APEC's 1998 **Blueprint for Action on Electronic Commerce** emphasises that the potential of electronic commerce cannot be realised without government and business cooperation.

- In 2004, the **APEC Privacy Framework** was endorsed by APEC Ministers recognising that cooperation to balance and promote effective information privacy protection and the free flow of information in the Asia-Pacific region is key to improving consumer confidence and ensuring the growth of electronic commerce.

- In 2007, a **Data Privacy Pathfinder initiative** was established to progress the implementation of the APEC Privacy Framework. The Pathfinder involves multiple projects aimed at promoting consumer trust and business confidence in cross-border data flows. It also includes general commitments regarding the development of a **Cross-Border Privacy Rules** system.
APEC Cross-Border Privacy Rules (CBPR) System

- Core documents created:
  - a detailed self-assessment questionnaire based on the nine APEC Privacy Principles for use by an applicant organization;
  - a set of baseline program requirements based on the nine APEC Privacy Principles against which an APEC-recognized Accountability Agent will assess an organization’s completed questionnaire;
  - recognition criteria to be used by APEC Economies when considering the recognition of an Accountability Agent;
  - the Cross Border Privacy Enforcement Arrangement (CPEA);
  - and
  - the Charter of the Cross Border Privacy Rules Joint Oversight Panel (JOP).
APEC Cross-Border Privacy Rules (CBPR) System

- US, Mexico, Japan and Canada in already South Korea, Philippines, Thailand, Vietnam, Singapore, Hong Kong and Australia taking steps?
  - At the time of its endorsement, all 21 APEC economies formally expressed their general intention to join the CBPR system
- Ten US companies have been certified to date by TRUSTe (Apple, Box, Hewlett-Packard, IBM, lynda.com, Merck, Rimini Street, Workday, Yodlee, Ziff Davis)
- Complementary APEC Privacy Recognition for Processors (PRP) system endorsed in February 2015
APEC CPEA

- The **APEC Cross-border Privacy Enforcement Arrangement** is an outcome of the Pathfinder initiative. It focuses on one of the four key goals of the APEC Privacy Framework, namely to facilitate both domestic and international efforts to promote and enforce information privacy protections.

- The CPEA aims to contribute to consumer confidence in electronic commerce involving cross-border data flows by establishing a framework for regional cooperation in the enforcement of Privacy Laws. The CPEA was endorsed by APEC Ministers in November 2009 and commenced on 16 July 2010.
Options
Options?

- Obtain Consent from data subjects
  - SG: need to provide reasonable summary and/or transfer only:
    - to country with comparable laws
    - under contract which provides comparable standard of protection
    - under binding corporate rules which provide comparable standard of protection
      - French CNIL initiative
    - under APEC CBPR
    - after exercising due diligence and taking reasonable steps to ensure data is protected to comparable standard?
What are the advantages of BCRs?

BCR make it possible to...

- be in compliance with the principles set out by Article 25 and 26 of the European Directive 95/46 for all flows of data within the group which are covered by the scope of the BCR,
- harmonise practices relating to the protection of personal data within a group,
- prevent the risks resulting from data transfers to third countries,
- avoid the need for a contract for each single transfer,
- communicate externally on the company's data protection policy,
- have an internal guide for employees with regard to the personal data management,
- make data protection integral to the way the company carries out its business.

Already acceptable for Singapore!

EU BCR

1. ABN AMRO Bank N.V. - Dutch DPA
2. Accenture - ICO (UK)
3. Airbus (Controller) - CNIL (FR)
4. Akzo Nobel N.V. (Controller) - Dutch DPA
5. Align Technologies B.V. (Controller and Processor) - Dutch DPA
6. American Express - ICO (UK)
7. ArcelorMittal Group - Luxemburg
8. Atmel - ICO (UK)
9. Atos (Controller and Processor) - CNIL (FR)
10. AXA - CNIL (FR)
11. Axa Private Equity - CNIL (FR)
12. BMC Software (Controller) - CNIL (FR)
13. BMW - DPA of Bavaria (Germany)
14. BP - ICO (UK)
15. Bristol Myers Squibb - CNIL (FR)
16. Cardinal Health, Inc. - IDPC (MT)
17. Care Fusion - ICO (UK)
18. Cargill, Inc. - ICO (UK)
19. Citigroup - ICO (UK)
20. CMA - CGM - CNIL (FR)
21. Continental Group - DPA of Lower Saxony (Germany)
22. D.E. Master Blenders 1753 ("DEMB")
23. ex Sara Lee International B.V. (indirect subsidiary of Sara Lee Corporation) - Dutch DPA
24. Deutsche Post DHL - BfDI, Germany
25. Deutsche Telekom - BfDI, Germany
26. DSM - Dutch DPA
27. e - Bay - Luxemburg
28. Ernst & Young - ICO (UK)
29. First Data Corporation (Controller and Processor) - ICO (UK)
30. GDF SUEZ (Controller) - CNIL (FR)
31. General Electric (GE) - CNIL (FR)
32. GlaxoSmithKline plc - ICO (UK)
33. Hermès - CNIL (FR)
34. Hewlett Packard - CNIL (FR)
35. HR Access - CNIL (FR)
36. Hyatt - ICO (UK)
37. IMS Health Incorporated - ICO (UK)
38. ING Bank N.V. - Dutch DPA
EU BCR

39. Intel Corporation - Ireland
40. International SOS - CNIL (FR)
41. Johnson Controls - Belgian DPA
42. JPMC - ICO (UK)
43. Koninklijke DSM N.V. and affiliated companies - Dutch DPA
44. Legrand (Controller) - CNIL (FR)
45. Linkbynet (Controller and Processor) - CNIL (FR)
46. Linklaters - ICO (UK)
47. LVMH - CNIL (FR)
48. Michelin - CNIL (FR)
49. Motorola Mobility LLC - ICO (UK)
50. Motorola Solutions, Inc. - ICO (UK)
51. NOVARTIS - CNIL (FR)
52. Novo Nordisk A/S - Danish DPA
53. Osram - DPA of Bavaria (Germany)
54. OVH - CNIL (FR)

55. Rabobank Nederland - Dutch DPA
56. Royal Philips Electronics - Dutch DPA
57. Safran - CNIL (FR)
58. Sanofi Aventis - CNIL (FR)
59. Schlumberger Ltd. - Dutch DPA
60. Schneider Electric - CNIL (FR)
61. Shell International B.V. - Dutch DPA
62. Siemens Group - DPA of Bavaria (Germany)
63. Simon - Kucher & Partners - DPA of North Rhine - Westphalia (Germany)
64. Société Générale - CNIL (FR)
65. Spencer Stuart - ICO (UK)
66. TMF Group B.V. (Controller and Processor) - Dutch DPA
67. Total - CNIL (FR)

Merck & Co., Inc.* Case Study

*Merck operates as Merck Sharp & Dohme (MSD) outside of the U.S. and Canada
Background

- Recognition by APEC and the EU that the CBPR system and the BCR system are both based on codes of conduct for international transfers that are approved by regulators (or accountability agent approved by a regulator)

- In March 2014, published a Referential
  - Aligns and compares BCRs-CBPRs
  - Case studies commenced: SOM 3 2014
  - Reports on case studies: SOM 1 2015
  - Joint action plan agreed to by APEC/EU
Merck Dual Certification Project

**Project Objective**
Support further implementation of the EU BCR – APEC CBPR Referential through a real world case study on dual certification from CBPRs to BCRs

**Merck Strategic Objectives**

Operational objective: Promote global privacy program interoperability in practice by demonstrating that a comprehensive accountable organizational privacy program can meet the requirements of multi-jurisdictional privacy systems while maintaining internal operating efficiency

Public policy objective: Identify privacy program standards aligned to the referential that might be considered by both EU and APEC regulators as appropriate for satisfying the application and approval requirements of both the BCR and CBPR systems and begin to pave the way for dual-system recognition

**Stakeholders**

Legal Advisor: Covington & Burling
APEC Accountability Agent: TRUSTe
Applicant: Merck & Co., Inc. (operating as Merck Sharp & Dohme outside of the U.S. and Canada)
Regulators: European Economic Area (EEA) DPAs (Belgium Lead), Singapore Personal Data Protection Commission, U.S. Federal Trade Commission

**Timeline**

EU BCR Application Filing and Singapore Submission: 26 November 2014
EU Lead DPA Review and Response: 9 December 2014 – 26 January 2015
EU Regulatory Review – Cooperation Procedure: 13 February 2015 – present
How our Privacy Program has Evolved …

Key Milestones 2000-2015


- **May 2006**
  - S-P first certifies to U.S.-E.U. Safe Harbor for HR Data

- **March 2003**
  - Executive Committee approves Merck Corporate Policy 50 – Global Privacy and Data Protection

- **August 2000**
  - First Merck Corporate Internet Privacy Policy approved and launched on U.S. web sites

- **November 2001**
  - Executive Committee approved Corporate Policy 43 and Merck first certifies to U.S.-E.U. Safe Harbor

**Building the new Merck Privacy Program (2010-2012)**

- **January 2011**
  - Launch global Merck Privacy Awareness Campaign

- **February – August 2010**
  - Launch and Implement new Safe Harbor Harmonization Project to integrate 4 legacy company certifications and compliance processes

- **June 2012**
  - Launch Simplification work streams

**Driving Accountability in Practice (2012-2015)**

- **January - Feb 2015**
  - First phase of EU Binding Corporate Rules (BCR) review completed. Cooperation procedures commenced

- **August 2012**
  - Launch Management Accountability Model and Implement Simplified Senior Leader Certification

- **August 2013**
  - Launch automated privacy threshold assessment and privacy impact assessment system with integrated risk assessment and control effectiveness methodology.

- **October 2013**
  - Second multinational and first health care company APEC CBPR certified (entire program certified)
The Evolving Privacy Environment is Complex ...

Our Privacy Program Elements Provide the Foundation for Compliance with Laws and Adherence to Our Values

Our Program is Built to Enable Merck to Uphold its Global Privacy Commitments and Responsibilities

Respect | Trust | Prevent Harm | Comply

100+ countries with laws addressing 4 types of privacy:
Information ● Bodily ● Communications ● Location

<table>
<thead>
<tr>
<th>Awareness</th>
<th>Policies &amp; Standards</th>
<th>Training</th>
<th>Accountability</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Culture</strong>: Promote and maintain a corporate culture that respects privacy and protects information about people</td>
<td>Implement privacy and data protection policies and standards that set forth operational principles and procedures, governance, accountability, incident handling and individual redress</td>
<td>Implement a privacy training curriculum designed to support our “Awareness” and “Policies &amp; Standards” Elements to provide functional privacy knowledge aligned to roles and responsibilities</td>
<td>Demonstrate the effectiveness of our Privacy Program by: <strong>Privacy Concept &amp; Design Review</strong>: Prospectively building and documenting privacy requirements into Merck processes and systems <strong>Periodic Assessment</strong>: Verifying privacy and data protection compliance through audits, assessments and investigations <strong>Reporting</strong>: Reporting to government authorities as required by law <strong>Governance and Annual Certification</strong>: Management acknowledgement and responsibility for assuring that requirements are addressed</td>
<td><strong>Performance Standards</strong>: Define baseline and target metrics to determine the effectiveness, maturity and risks associated with the Program <strong>Continuous Improvement</strong>: Evaluate program effectiveness, maturity and risks and areas for enhancement, improvement and risk mitigation</td>
</tr>
</tbody>
</table>

BCR/ CBPR/ Safe Harbor | Data Protection | Breach Notification | Health Privacy | Workplace Privacy | Online/ Mobile Privacy | Telecomm | Location Privacy

Information Protection
Data Protection
Breach Notification
Health Privacy
Workplace Privacy
Online/ Mobile Privacy
Telecomm
Location Privacy
## Dual Certification Project Mapping Analysis

<table>
<thead>
<tr>
<th>Privacy Framework Category</th>
<th>Requirements</th>
<th>EU BCRs</th>
<th>APEC CBPRs</th>
<th>Singapore PDPA</th>
<th>Switzerland FADP</th>
<th>Referential Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Substantive Privacy and Data Protection Standards</strong></td>
<td>Transparency and Fairness, Purpose Limitation, Data Quality, Security, Access, Correction, Objection, Onward Transfer, Basis for Processing Personal Data, National Law Limitations, Relationship to National Law</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>14, 17</td>
</tr>
<tr>
<td><strong>Compliance Verification</strong></td>
<td>Training, Complaint Handling, Audit Program, Compliance Oversight</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>19</td>
</tr>
<tr>
<td><strong>Enforceability</strong></td>
<td>Internally Binding - Entities, Internally Binding - Employees, Third Party Beneficiary Rights, Liability of Applicant Entity, Sufficiency of Applicant Entity Assets, Burden of Proof, Access to the BCRs, Cooperation Duty</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>3, 13</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Geographic Scope, Material Scope, Entity List, Purposes of Transfer / Processing</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>1, 2, 23</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td>Definitions, Effective Date and Changes</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>9, 28, 27</td>
</tr>
</tbody>
</table>

**Legend**
- Green: Comparable Requirements
- Yellow: More Stringent or More Detailed Requirements
- Light Grey: Requirement on Partially Addressed
- Dark Grey: No Comparable Requirement
- Merck Case Study: Revisions Requested by EU Lead DPA

© 2015 Baker & McKenzie, Wong & Leow
Privacy Interoperability @ Merck

Our Program is Built to Enable Merck to Uphold its Global Privacy Commitments and Responsibilities

Respect | Trust | Prevent Harm | Comply

100+ countries with laws addressing 4 types of privacy:
Information, Bodily, Communications, Location.

Awareness | Policies & Standards | Training | Accountability | Metrics

Framework for data transfer mechanism selection to countries not recognized as “adequate/equivalent”

Is my data transfer one-time or ongoing?

- **Ongoing**
  - Does the country of origin recognize Safe Harbor, BCRs or CBPRs?
    - **YES**, implement program to obtain approval to participate in Safe Harbor, BCRs or CBPRs, as applicable
    - **NO**, enter into data transfer agreements containing essential clauses with recipient entities

- **One-time**
  - Can consent to the transfer be obtained from data subjects?
    - **YES**, obtain and retain evidence of specific consent for the transfer
    - **NO**, determine whether an exception exists or anonymise the data prior to transferring

  - **NO**, if data transfer agreements are impracticable, consider other alternatives
Data Localisation

- Russia Federal Law No. 242-FZ
  - As of Sept. 1, 2015, Russian and foreign companies will be required to record and store personal data of Russian nationals using databases located on Russian territory.
  - “Residency Requirements for Data in Clouds—What Now?” by Lothar Determann, Edward Bekeschenko And Vadim Perevalov

- Indonesia Reg 82
  - Electronic System Operator for public services shall place a Data Center and Disaster Recovery Center in the territory of Indonesia for law enforcement, protection and sovereignty of the state and its citizens.

- Vietnam Decree 72
  - ISPs have to establish at least one server inside Vietnam containing entire history of information posting activities on general information websites and sharing on social networks.