MAYER·BROWN

Financial Institutions and Cloud Computing – What's on the Horizon

Rebecca Eisner
Partner - Chicago
+1 312 701 8577
reisner@mayerbrown.com

Mark Prinsley
Partner - London
+44 203 130 3900
mprinsley@mayerbrown.com

Sara S.M. Or
Partner – Hong Kong
+852 2843 2268
sara.or@mayerbrownjsm.com

Critical Issues in Sourcing

BUSINESS & TECHNOLOGY SOURCING WEBINAR SERIES

Speakers

Rebecca Eisner, a partner in the Chicago office, serves on Mayer Brown's Partnership Board. She focuses her practice on technology and business process outsourcing and sourcing, information technology transactions, privacy, and security. Her practice focuses on complex global technology, licensing and business process outsourcing transactions, including IT infrastructure and licensing, cloud computing, applications development and maintenance, back office processing, ERP implementations, finance and accounting, payroll processing, call center, HR, technology development, system integration and hosting. She regularly advises clients in Internet and e-commerce law issues. She also regularly advises on complex data protection and data transfer issues, frequently as part of transactions, as well as privacy issues and electronic contracting and signatures.

Mark Prinsley, is a partner in the London office. He heads the IP/IT, outsourcing and privacy practice in London. His practice is focused on complex IT and business process transactions which are frequently multi jurisdictional and often involve issues relating to personal data. Mark and his team have worked on cloud transactions in a variety of industries including manufacturing and financial services with a range of suppliers.

Sara Or, is a partner of Mayer Brown JSM. Sara currently heads up the Financial Services Regulatory and Enforcement practice in Hong Kong, a key focus of which is to provide a full range of legal services to financial institutions. Sara advises clients on banking, securities and insurance regulations on a regular basis. In addition to helping clients structure and set up regulated businesses, she also provides legal services needed by clients in operating the businesses. Sara's practice also includes provision of strategic advice and assistance to clients in connection with enquiries, inspections or investigations by regulators. She has established good working relationship with both financial institutions and regulators (including, Hong Kong Monetary Authority, Securities and Futures Commission and Office of the Commissioner of Insurance), and accumulated invaluable experience and knowledge on market practice as well as supervisory philosophies of regulators.

Business & Technology Sourcing Practice

"An excellent team of people for outsourcing agreements globally - pragmatic in their approach, with a wealth of experts they can call on."

~ Chambers Global 2014

"Mayer Brown is universally regarded as a leading player in the technology and outsourcing arena, with market commentators commending the ease with which its lawyers integrate with clients, delivering business-focused advice and guidance."

~ Chambers Global 2013

"Their knowledge in this area is tremendous. They know us so well they blend into our deal teams and become a natural extension to our in-house team."

~ Chambers USA 2014

Mayer Brown is universally regarded as a leading player in the technology and outsourcing arena, with market commentators commending the ease with which its lawyers integrate with clients, delivering business-focused advice and guidance."

~ Chambers USA 2013

- More than 50 lawyers around the world focused on helping clients improve their business operations by sourcing services and technology
- Advised on more than 300 significant outsourcing transactions valued at an aggregate of more than $100 billion

RECOGNIZED MARKET LEADER

CHAMBERS & PARTNERS

"Band 1" ranking in IT/Outsourcing for ten consecutive years (Chambers 2004-2014)

The LEGAL 500 UNITED STATES

Named "MTT Outsourcing Team of the Year" in 2014 and ranked in the top tier from 2010 thru 2014

IAOP INTERNATIONAL ASSOCIATION OF OUTSOURCING PROFESSIONALS

Ranked as one of the top law firms in 2009 thru 2014 on The World's Best Outsourcing Advisors list for The Global Outsourcing 100™

Agenda

- Introduction and CPD/CLE points
- The Cloud Computing Market
- Regional legal and regulatory issues in cloud contracting:
  - Asia
  - US
  - Europe
- Typical structure of Cloud Computing Contracts and three key contractual issues
  - Security
  - Warranty/Limitation of Liability
  - Data Privacy

The Market: What is Cloud Computing?

National Institute of Standards and Technology defines it as:

A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

SERVICE MODELS	DEPLOYMENT MODELS
Software as a Service (e.g. Google Gmail, Google Docs, Facebook and Twitter)	**Private Cloud**
Platform as a Service (e.g. Microsoft Azure, Force.com, Google App Engine)	**Community Cloud**
Infrastructure as a Service (Amazon, Google, Rackspace, IBM, AT&T, etc.)	**Public Cloud**
	Hybrid Cloud

What Are You Buying? Who Controls?

C = Customer, P = Provider

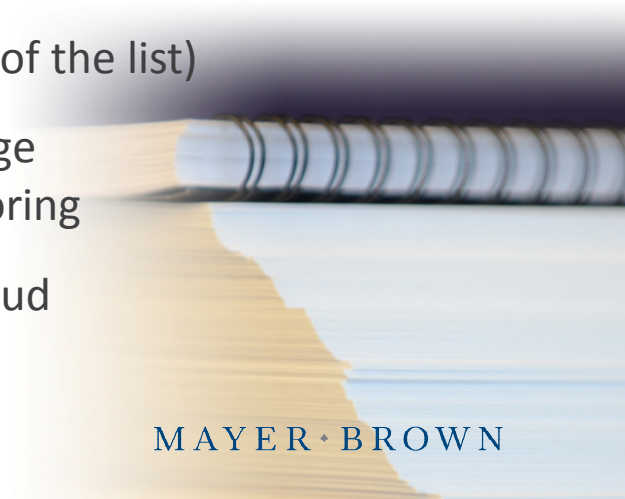
Cloud Elements (Stack)	Customer IT/ITO Provider Manages	IAAS	PAAS	SAAS
Network	C	P	P	P
Storage	C	P	P	P
Server	C	P	P	P
VM	C	C/P	C/P	P
Applications	C	C	C/P	P
Data	C	C	C	C/P

The Market: Know What You Are Buying

- Terms you may hear:
  - Public, private, hybrid, dedicated, shared, multi-tenant, single tenant
  - You need to know what is dedicated (used solely for the particular customer), and what is shared (used by two or more customers)
- What elements of the "stack" are dedicated versus shared?
- Why does this matter?
  - Affects privacy, security and compliance risks
  - Affects control and transparency the customer may have
  - Affects commercial terms of the solution

The Market: Have a Cloud Policy

- Many companies are developing cloud computing policies that cover these and other topics:
  - Linking cloud use policy with security policies for gap analysis and risk review
  - Requirement for a business case
    (build versus buy versus keep what you have)
  - Risk review
    (risks change depending on the type of cloud service, provider, type of data and criticality to business)
  - Compliance review
    (with regulatory, data protection and security at top of the list)
  - Assignment of one or more team members to manage and oversee cloud procurement and ongoing monitoring
  - Acceptable range of contract terms outcomes for cloud



Some Banks Using Cloud Services

JPMorgan Chase & Co.	**JPMorgan Chase** Application development — *Private Cloud* Apprenda Feb 2013
SOCIETE GENERALE	**Societe General Bank & Trust** Migration of core banking systems to a cloud computing architecture — *Private Cloud* March 2013
ICBC 中国工商银行 INDUSTRIAL AND COMMERCIAL BANK OF CHINA	**ICBC Credit Suisse** Applications development/cloud based data centre — *Private Cloud*
Bank of America Merrill Lynch	**Bank of America** Testing a revamp of its data storage processes. Migration expected during 2015 — *Private Cloud*
BBVA	**BBVA** Email Google Apps — *Public Cloud*
bankinter	**Bankinter** Using Amazon Web Services for credit risk checking on customers and prospective customers — *Public Cloud*

OVERVIEW OF REGIONAL LEGAL DEVELOPMENTS

Legal and Regulatory Overview – Asia

Sources of Regulatory Requirements

- Banking or Financial Services Regulator
  - e.g. Hong Kong Monetary Authority (HKMA)
  - Supervisory Policy Manual on Outsourcing
- Privacy Commissioner
  - e.g. Privacy Commissioner of Personal Data, Hong Kong

Legal and Regulatory Overview – Asia

- Information Leaflets on
  - Cloud Computing
  - Outsourcing the Processing of Personal Data to Data Processors
- Guidance on Data Breach Handling and the Giving of Breach Notifications
- Privacy Management Programme: A Best Practice Guide
- Guidance on the Proper Handling of Customers' Personal Data for specific industries

Legal and Regulatory Overview – Asia

No Standardization Initiatives

- No standardization within banking industry
- No standardization among Asian markets

Legal and Regulatory Overview – Asia

Principal Obligations

- Notification to Bank customers or customer consent
- Regulatory approval or “blessing”
- Bank remains liable to Bank customers for data security and handling
- Bank liable for breach by cloud provider and its sub-contractors

Legal and Regulatory Overview – Asia

Breach Consequences

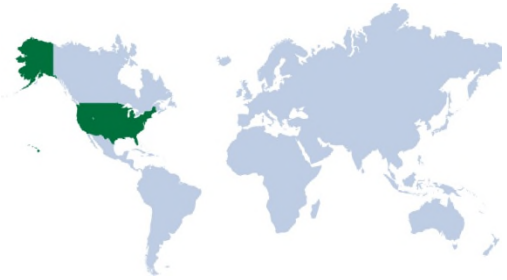
- Bank customers' right to claim compensation
- Complaints and investigations
- Offences and penalties
- Negative publicity and reputation risk

Legal and Regulatory Overview – US

No Single Privacy/Security Federal Law –
Various sources of responsibility and standards

- Laws and regulations
- Bank regulator guidance
- State laws
- Caselaw
- Industry Standards (PCI DSS)
- FTC influence

Legal and Regulatory Overview – US

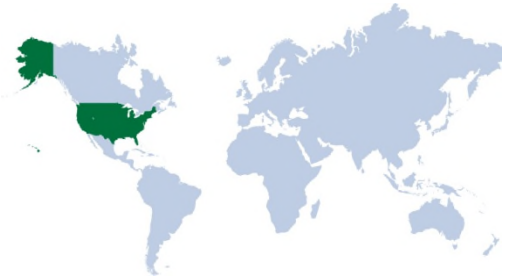


- Gramm-Leach-Bliley Act (GLBA)
- OCC Third Party Relationships – Risk Management Guidance Oct. 30, 2013
- US FRB: "Guidance on Managing Outsourcing Risk" Dec. 5, 2013
- FFIEC IT Subcommittee Outsourced Cloud Computing, July 10, 2012
- FFIEC and OTS exam books
- Consumer Financial Protection Bureau
- Fair Credit Reporting Act/FACT Act
- OFAC
- Bank Secrecy Act and Anti-Money Laundering
- ID Theft Red Flags
- State Privacy Security Laws (Breach Notification — 47 States and Encryption (MA and NV), use of SSN's, etc.)
- Industry Standards (PCI)
- Litigation and enforcement cases
- Federal Trade Commission Act (FTCA) for non-bank entities (but decisions may be influential)

Legal and Regulatory Overview – US

- General security of personal information laws (e.g., Arkansas, California, Indiana, Maryland, Massachusetts, Nevada, Rhode Island, Texas and Utah)
- Standard: reasonable security procedures and practices appropriate to the nature of the information
- Massachusetts regulations far exceed most other laws and regs.
  - Create duty to protect and have detailed system requirements
  - Require a written security program
  - Requires that companies oversee service providers by selecting providers who are capable of maintaining appropriate security measures consistent with the Massachusetts regs
  - Requires that service provider contracts require them to implement and maintain appropriate security measures
  - Requires encryption of personal information across public networks, wireless networks and portable devices (laptops, hard drives, etc.)

Legal and Regulatory Overview – US



OCC Risk Management Highlights

- A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships
- A bank should ensure comprehensive risk management and oversight of third-party relationships involving critical activities*

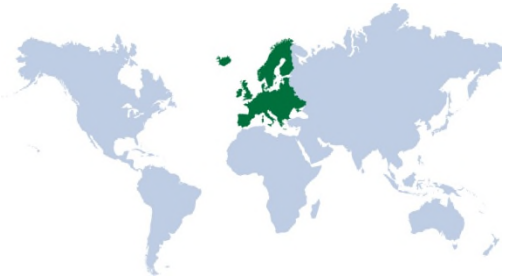
**** Asterisks represent areas that present challenges in cloud computing contracting, due to limited control, transparency, and general ability to comply with regulatory requirements***

Legal and Regulatory Overview – US

- An effective risk management process throughout the life cycle of the relationship includes
  - plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party
  - proper due diligence in selecting a third party*
  - written contracts that outline the rights and responsibilities of all parties
  - ongoing monitoring of the third party's activities and performance*
  - contingency plans for terminating the relationship in an effective manner*
  - clear roles and responsibilities for overseeing and managing the relationship and risk management process
  - Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management*
  - Independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks*
  - OCC rights to examine and provide oversight of the functions performed by third parties to the same extent as if performed by the bank*

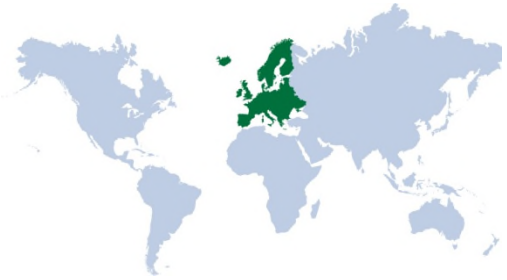
**** Asterisks represent areas that present challenges in cloud computing contracting, due to limited control, transparency, and general ability to comply with regulatory requirements***

Legal and Regulatory Overview – Europe



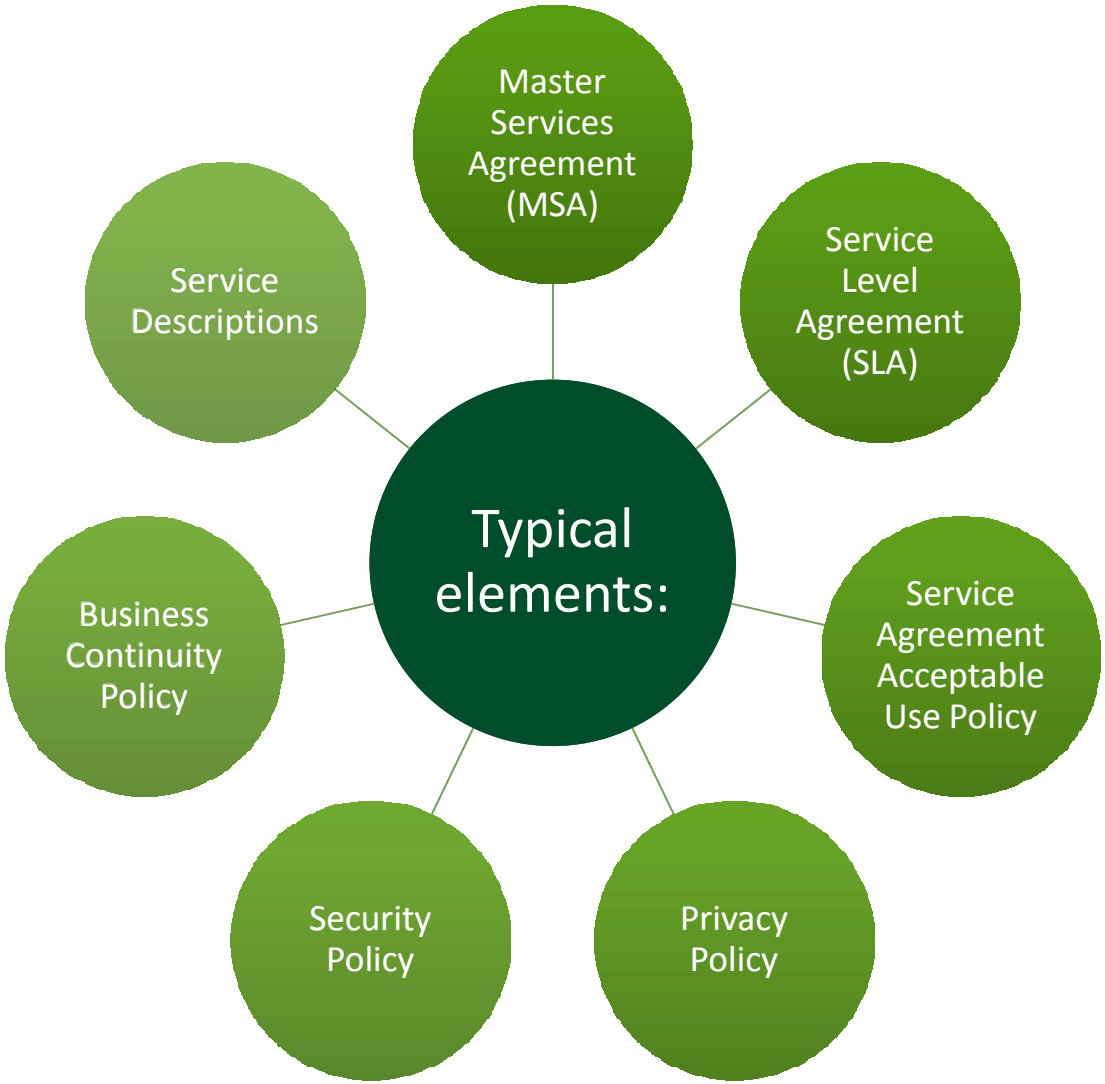
- Financial Services Regulatory
  - MIFID – (sysc 8.1 Rules in the UK)
  - FCA – considerations for firms thinking of using third party (off the shelf) banking solutions – July 2014
- Cloud Contract Standardization Initiatives
  - Cloud Service Level Agreement Initiative
    - ISO and EU
    - EU DG Connect Cloud Select Industry Group (C – SIG) e.g. C-SIG Draft Cloud Service Level Standardisation Guidelines June 2014

Legal and Regulatory Overview – Europe

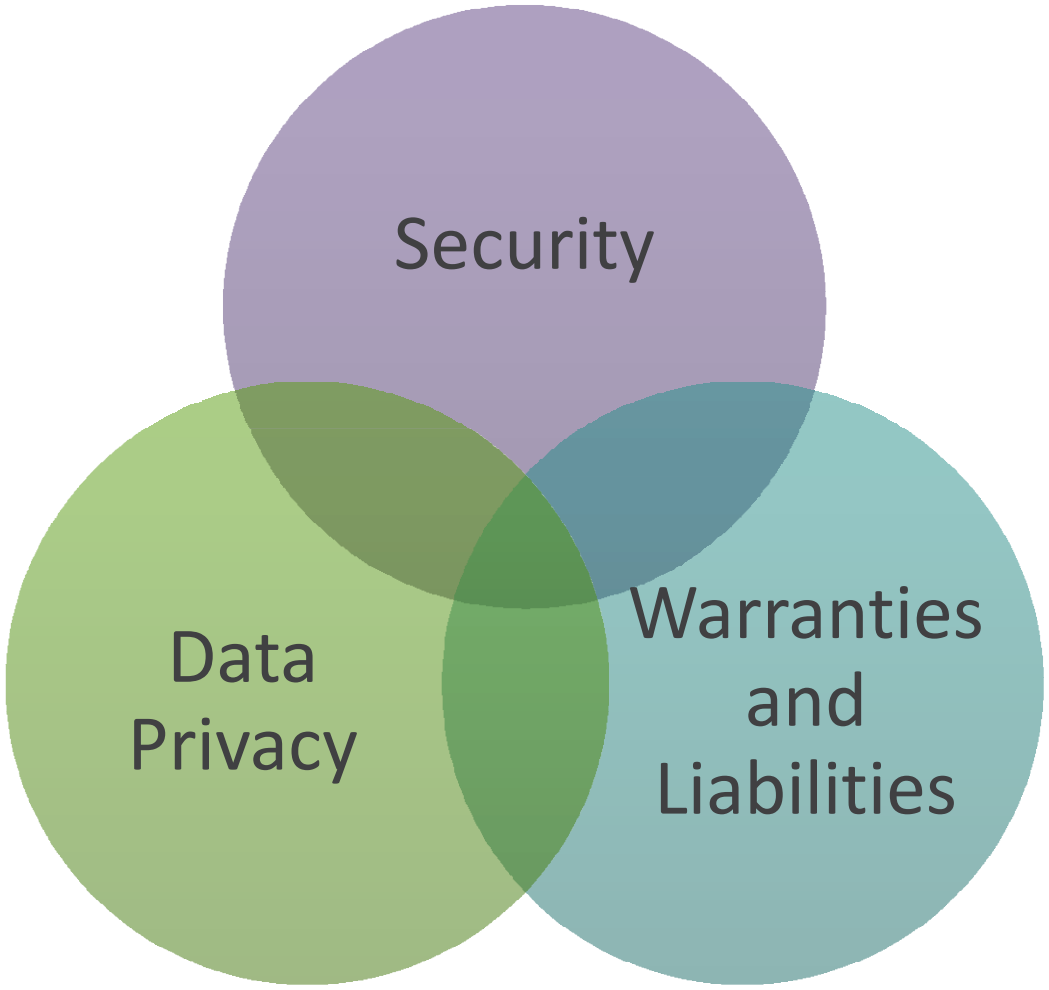


- Data Privacy
  - EU Article 29 Working Party Opinion on Cloud Computing
  - ICO Guidance on the use of Cloud Computing
  - Impact of Proposed EU Data Privacy Regulations
  - EU Approval of Microsoft Office 365 Data Export Terms
  - C-SIG Initiative – Data Protection Code of Conduct for Cloud service providers – submitted to Article 29 Working Party

Cloud Computing Contract Structure



Three Key Legal Areas

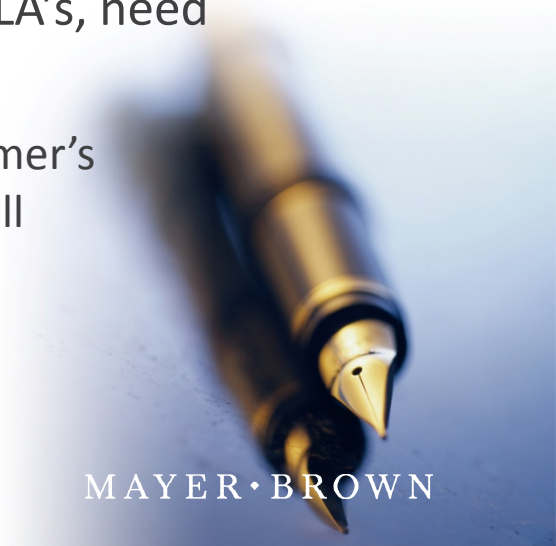


Contractual Issues: Security

- Standards - all reasonably practicable steps
- Due diligence at cloud provider selection stage and regular review
- Contractual or other controls over cloud provider and extent to which they are effective on cloud provider's sub-contactors
- Encryption
- Data breach reporting and handling

Contractual Issues: Warranties and Liability

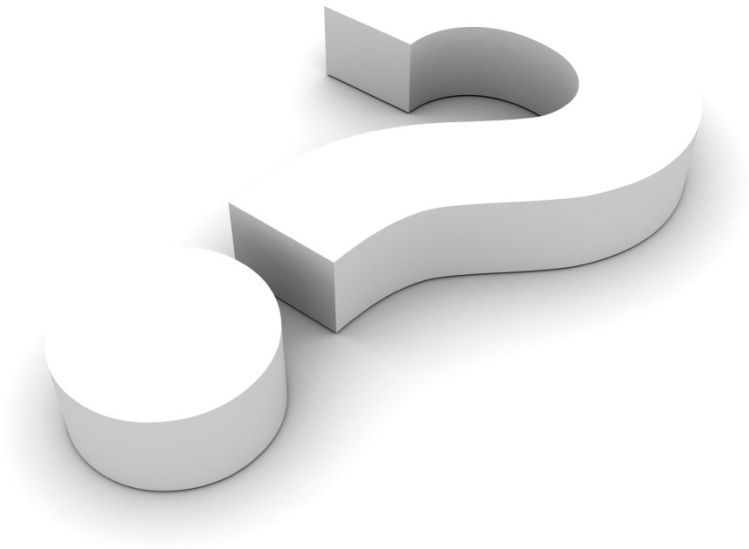
- Limitations – capped damages (12-24 months or more), exclusions are key!
- Consequential damages – typically fully excluded, or with limited exceptions
- SLA credit sole remedy – common problem, difficult to overcome – try language that permits damages if some other claim under agreement can be made
  - **Watch out:** The "sole and exclusive remedy" language is often buried in technical service level agreements (versus legal terms)
- Reps and warranties – need more than just meets the SLA's, need performance warranties and others
  - **Watch out:** Without performance warranties, the customer's ability to bring claims for damages for service failures will be severely limited



Contractual Issues: Data Privacy

- Data Protection codes of conduct, standards etc which the service complies with – *e.g. ISO 27018 – code of practice for use of PII in public clouds acting as PII Processors (August 2014)*
- Nature of the data being processed and purposes for which it is processed
- Obligations to delete personal data once no longer needed for the purposes for which it is processed
- Notice of requirements in relation to Supplier's obligations to disclose personal data to law enforcement authorities
- Sub-contracting
- Basis upon which transborder data flows are permitted

Questions



Rebecca Eisner
Partner
+1 312 701 8577
reisner@mayerbrown.com

Sara S.M. Or
Partner – Hong Kong
+852 2843 2268
sara.or@mayerbrownjsm.com

Mark Prinsley
Partner - London
+44 203 130 3900
mprinsley@mayerbrown.com

MAYER·BROWN