MAYER·BROWN

Security and Privacy in the Cloud

Mayer Brown LLP: Cybersecurity and Data Privacy / Technology Transactions Practice Groups

November 14, 2017

Linda Rhodes
Partner
202-263-3382
lrhodes@mayerbrown.com

Brad Peterson
Partner
312-701-8568
bpeterson@mayerbrown.com

Joe Pennell
Partner
312-701-8354
jpennell@mayerbrown.com

Speakers

Linda Rhodes

Partner

Linda Rhodes is a partner in the Washington, DC, office of Mayer Brown's Technology Transactions practice. She focuses her practice on complex technology transactions, including business and technology sourcing and digital services. She is experienced in handling data security and privacy issues in the context of these complex transactions. She has represented a wide spectrum of clients, from emerging companies to large multinational corporations, in a variety of industries. Linda co-leads Mayer Brown's connected and autonomous vehicles initiative. *Chambers USA* notes that Linda "'has been incredible,' particularly highlighting her drafting skills and ability to explain complex concepts," and "is singled out for her 'hard-working, diligent' attitude."

Brad Peterson

Partner

Brad Peterson leads the Technology Transactions practice at Mayer Brown. As a corporate technology lawyer, Brad helps global companies work more effectively with their technology and operations suppliers, and he is one of the nation's most experienced and highest-ranked outsourcing lawyers. In the past five years, he has represented clients in increasing numbers of contracts with digital services providers, including cloud, data analytics, "as a Service" and automated process scopes and cyber security and privacy issues related to those scopes.

Joe Pennell

Partner

Joe Pennell is a partner in the Chicago office of Mayer Brown's Technology Transactions and Corporate & Securities practices. Joe focuses his practice on information technology and managed services transactions, including cloud computing, software licensing and implementation, and the outsourcing of finance and accounting services, IT infrastructure services and support, managed network services, and application development and maintenance. He is the Co-Chair of the ABA Section of Science and Technology Law's Cloud Computing Committee.

Mayer Brown's Technology Transactions Practice

- More than 50 lawyers around the world focus on helping clients develop and manage relationships with suppliers of critical services and technology.
- Our Technology Transactions lawyers have experience in 400 critical services sourcing deals with a total contract value exceeding $200 billion, including data, digital, outsourcing and software.

Recognized Market Leader

"Band 1" ranking
in IT/Outsourcing for
14 consecutive years (*Chambers* 2004-2017)

Named "MTT Outsourcing Team of the Year"
in 2014 and ranked in the top tier from 2010 through 2016

Ranked as one of the top law firms 2009 - 2016 on World's Best Outsourcing Advisors list for The Global Outsourcing 100™

Named 2016 "Technology Practice Group of the Year"

"They have current cutting-edge knowledge and are savvy about attuning their counsel to the needs of the client to arrive at a satisfactory solution to many sticky issues."
~ Chambers USA 2017

"They are very good at being able to communicate and synthesize information in a useful and easily understandable way."
~ Chambers USA 2016

"They're very practical in terms of trying to identify solutions and giving very good advice on areas where it's reasonable for us to compromise or, alternatively, where to hold our ground."
~ Chambers USA 2015

"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

Technology Transactions: https://www.mayerbrown.com/experience/Technology-Transactions/

Background and Nature of Cloud Solutions

- Cloud solutions have many advantages but also present challenges for complying with data privacy and cybersecurity regulations.
- Successful and compliant use of cloud computing requires businesses to fully evaluate:
  - The nature of the data;
  - The associated data privacy and cybersecurity laws; and
  - The structure and location of the cloud solution.

Background and Nature of Cloud Solutions, cont.

- A “cloud” solution generally refers to a type of service under which the Provider:
  - Utilizes shared computing resources,
  - to provide services over the Internet,
  - for multiple customers.
- Customer advantages include:
  - Little, if any, upfront investment; and
  - Ability to quickly change resource usage.
- Providers typically maintain the freedom to move data to maximize resource usage and have limited ability to customize public cloud solutions for any particular customer.

Impact of a Data Breach

The impacts of a data breach include:

- Expense to investigate and respond;
- Damage to brand/reputation and resulting lost sales;
- Disruption to management, PR, marketing and operations;
- Regulatory fines, sanctions or mandates;
- Shareholder derivative suits against directors and officers;
- Consumer class actions against the company; and
- Collateral damage to other companies, who then sue.

Critical Risks with Cloud Deals: Third-Party Suppliers and Partners

- Your security is as good as your weakest vendor's security.
- Trusted contractors may subcontract vital roles.
- Liability caps may warp incentives.
- Breaches involving third-party vendors:

  Cogent Healthcare, Target, Lowe's, Goodwill Industries, Dairy Queen, TacoTime, Home Depot, Department of Veterans Affairs and Zoup – ranging from human error (inadvertent storage of data on a public website), to exploitation of security vulnerabilities by hackers, to compromised login credentials.

Laws and Regulations on Privacy and Data Security

- US laws are sectoral and also include state and FTC regulation on personal data.
- European laws are consolidated and include strict privacy regulations and restrictions on transfer of data outside of Europe.
- ROW laws are varied and in some cases more strict.
- The majority of privacy and security laws apply to the data owner, although more recent laws are placing responsibility on the processor and/or service provider.
- Most laws require "reasonable and appropriate" technical and organizational measures.
- Determination of what is "reasonable and appropriate," given the circumstances, can be challenging, but there is a trend to include more specific security requirements.

GDPR Impacts on Cloud Computing

- More sophisticated requirements between controllers and processors
- Privacy by design
- Record keeping
- Privacy Impact Assessments
- Enhanced data subject rights – transparency, right to be forgotten, data portability, rights to object to processing
- Breach notification in 72 hours (without undue delay for processors)
- Administrative fines of greater of 4% worldwide turnover or €20 million
- Direct remedies and proceedings for data subjects
- Approved transfer mechanisms largely continue but with possible challenge to model clauses and tightened use of consent and derogations

"Reasonable Measures" Include Care in Selection and Oversight of Third Parties

- **GLBA:** includes OCC Third-Party Relationships – Risk Management Guidance (Oct. 30, 2013); US FRB: "Guidance on Managing Outsourcing Risk" (Dec. 5, 2013); and FFIEC Cybersecurity Risk Assessment Tool (June 2015).
- **HIPAA:** requires Business Associate Agreements and regulations include Privacy and Security Rules.
- **SEC:** requires disclosure of material outsourcing relationships and risks that are relevant to cybersecurity and OCIE August 2017 risk alert
- **States:** For example, Massachusetts regulations require companies to take steps in selection and supervision of service providers; NYDFS Cybersecurity Regulations as applicable to TPS; California AG "reasonable security" means implement the Center for Internet Security's (CIS) Critical Security Controls.

Federal Trade Commission

FTC commonly includes in consent decrees:

- Designate dedicated data security personnel;
- Identify "material internal and external risks";
- Implement "reasonable safeguards" to control risks;
- **Develop "reasonable steps" to select secure vendors; and**
- Evaluate, monitor, and adjust regularly over 20-year period.

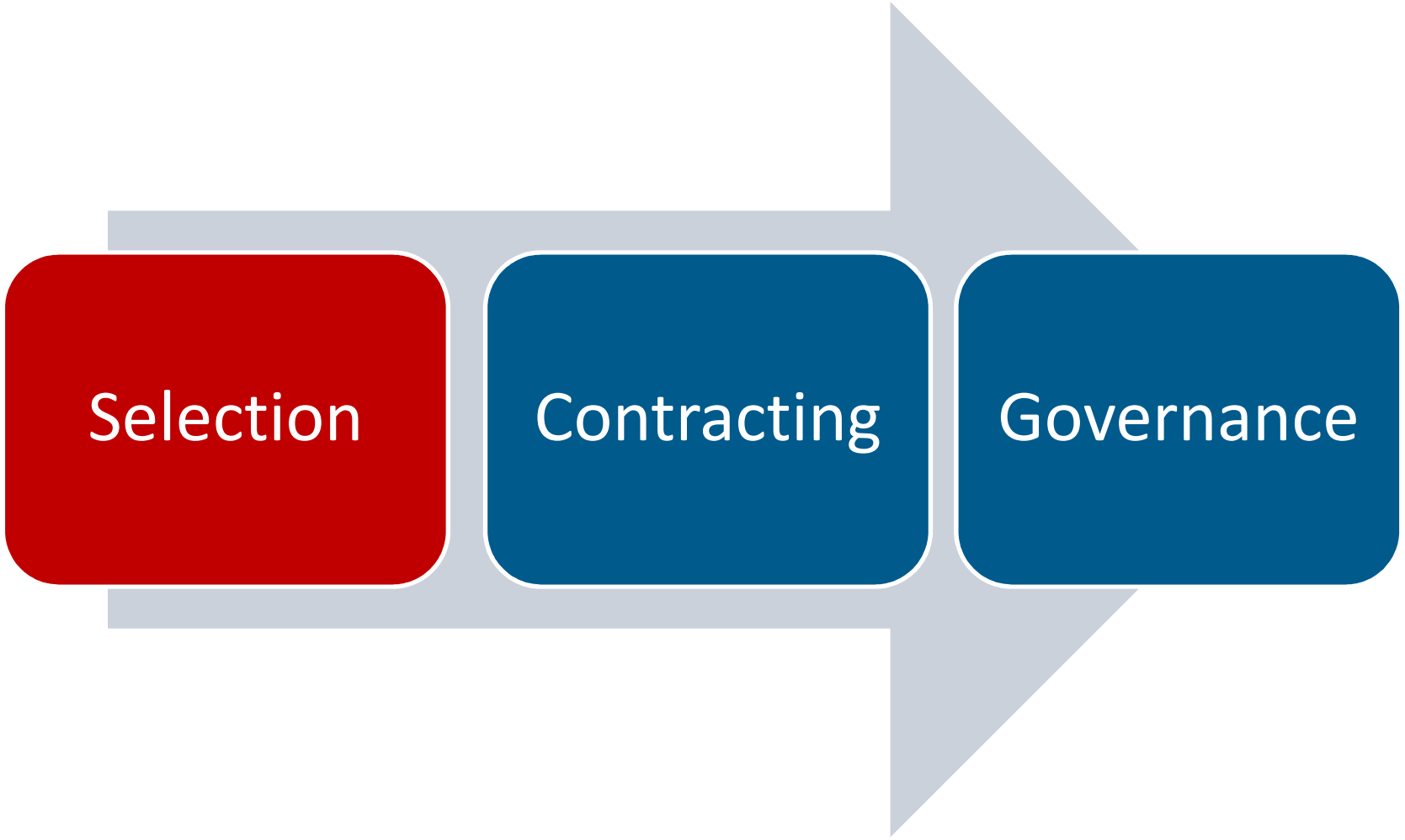
- See "Start with Security" publication from FTC (June 2015) and new blog series "Stick with Security"
- FTC cases involving breach by a third party: Lenovo (2017), GMR Transcription (2014), Upromise (2012)

New York Department of Financial Services

- New York Department of Financial Services, final regulations mandate cybersecurity standards for many institutions operating in NY (banks, insurance, insurance professionals, etc.) (eff. March 1, 2017).
- Regulations are comprehensive and address everything from access controls to encryption to data disposal and employee training.
- Regulations overlay on TSPs; most of the provisions that are applicable to covered entities, in that covered entities must develop written policies and procedures designed to ensure security of systems or data in the control of, or accessible by, TSPs.
- TSPs must meet minimum cybersecurity standards to do business with covered entities.
- TSP requirements take effect March 1, 2019.

Impact of Third-Party Access to Cloud Data and Blocking Statutes on the Structure of Cloud Solutions

- Third Party Access by Means of Legal Process:
  - Concerns around third party access to cloud data are driving the structure of cloud solutions.
    - Recent litigation suggests that the US government's ability to access US data stored outside the United States is in a state of flux. A recent second circuit court of appeals held that held that a US law enforcement agency could not use the Stored Communications Act to issue a search warrant for e-mail content stored on servers outside of the United States, whereas a third circuit district court held to the contrary.
    - Data that is stored in the United States is subject to the territorial jurisdiction of U.S. authorities, regardless of its ultimate origin.
    - Shifting to cloud-based storage is unlikely to impact the rights and obligations of private litigants.
  - Accordingly, multi-national customers are using several cloud instances or multiple providers around the world.
- Blocking Statutes:
  - Many countries that have passed "blocking statutes," which limit or prohibit exporting certain information outside the country.
  - Customers are using cloud instances in those countries with such statutes.

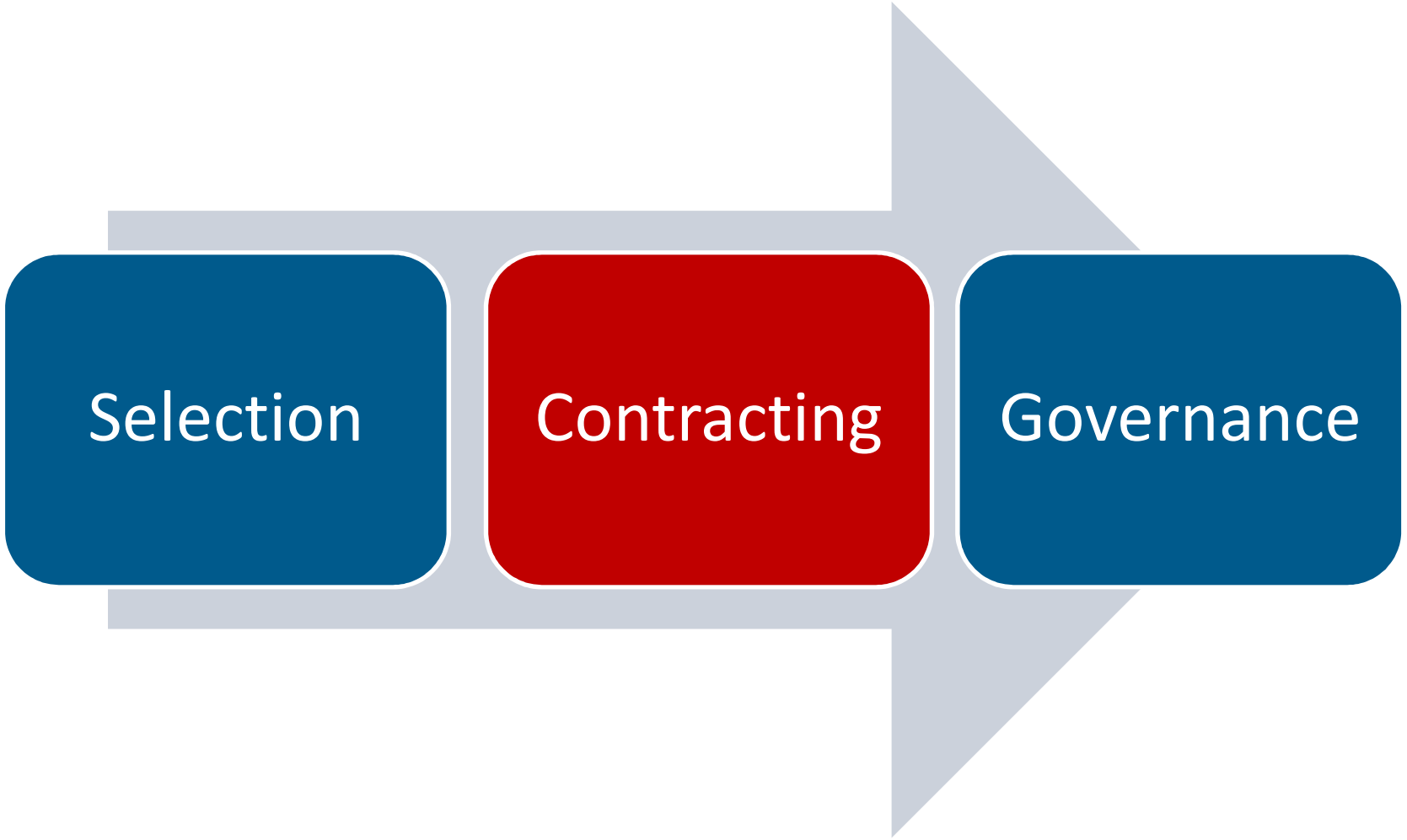

Selection
Contracting
Governance

First Steps

- Review your written information security plan.
  - If you don't have one, advocate for one.
- Review your data breach response plan.
  - If you don't have one, advocate for one.
- Review cyber goals and objectives set by the Company Board.
- Identify subject matter experts and stakeholders.
- Identify relevant laws, policies and standards.
- Create (or identify) data security questionnaires by category or data risk level.

Key Steps in Selection of Cloud Providers

- Determine what data will be accessed or stored by supplier.
- Categorize that data by risk level (sensitivity, volume, legal/contractual obligations).
- Review bidder's security measures under your policies.
- If applicable, send questionnaires regarding security.
- If applicable, commission security reviews and audits.
- Review completed questionnaires, WISPs, DBRPs and audit reports from bidders and remove suppliers with inadequate security capabilities.
- Estimate cost of ongoing security review for business case.


Selection
Contracting
Governance

Contracting Preparation

- Understand the cloud provider's technical and business model well enough to identify points where the provider can make commitments
  - For example, public cloud providers have more limited flexibility
- Assess risks in cloud provider's privacy and data security and identify ways to reduce risk (such as limiting the data going to that cloud or adding other security)
- Assess risk of locations used by supplier and ways to mitigate
- Identify areas where cloud provider may use your data to build its product (e.g., if the provider offers aggregated data from all of its customers as a service), and whether you seek to prevent that use

Contracting Approach

- Negotiation based on your form or preferred terms
  - Provides best results assuming adequate leverage
  - Works best using a cloud form not a general services or professional services form
- Negotiating the negotiable elements of provider's forms
  - May be your only choice for some public cloud providers
  - Focus on identifying solvable problems, not on specific language
- Preparing a "risk memo" assuming provider terms
  - Inform the go/no-go decision
  - Provide a list of risks to mitigate through other means

Data Security and Privacy Terms Checklist for Cloud

✓	General security and confidentiality covenants for Customer Data
✓	Compliance with industry standards (ISO 27001, NIST, FEDRAMP, PCIDSS)
✓	Audit reports (SOC 1 and SOC 2 Type II, SOC 3)
✓	Compliance with privacy and data security laws
✓	Data locations (processing and storage) and data transfers (including remote access)**
✓	Customer's written information security policies**
✓	Physical and operational security measures
✓	Security incident reporting (definition of PI recently expanded) and time period – GA Supplier w/in 24 hours; FL – notify in 30 days)

** Indicates challenges in obtaining these commitments in public cloud area

Data Security and Privacy Terms Checklist for Cloud

✓	Restrictions on subcontracting**, including flow-down of obligations
✓	Background checks and personnel screening **
✓	Data minimization and compliance with records retention policies **
✓	Limitations on access to systems
✓	Adequate cyber-liability coverage on a primary basis **
✓	Restrictions on secondary uses of data (including aggregated, derived or anonymized data) **

** Indicates challenges in obtaining commitment in public cloud

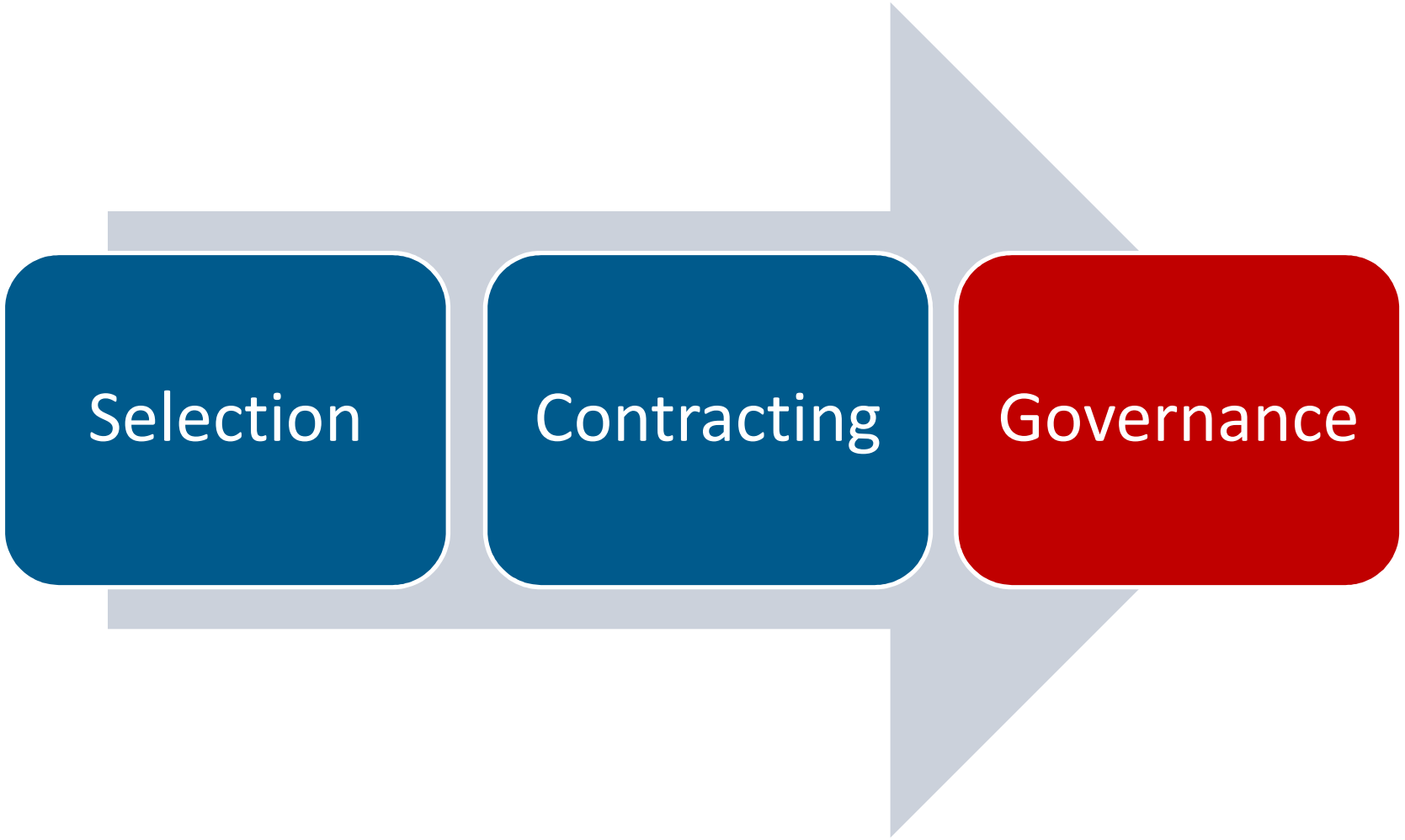
Data Security and Privacy Terms Checklist for Cloud (not public cloud)

✓	Right to change policies and standards to respond to changes in laws or new threats **
✓	Right to obtain commitments directly from personnel**
✓	Right to require use of new technologies such as biometrics, when available**
✓	Right to do security audits, including penetration testing**

** Indicates challenges in obtaining commitment in public cloud

Data Security and Privacy Terms Checklist for Cloud

✓	Reimbursement for cost of audits that detect security failures
✓	Breach notification requirements and reimbursement for costs of security breaches, such as data breach notification to consumers
✓	Reimbursement for customary additional actions, such as investigation, call centers, credit monitoring services, credit card replacements, etc.
✓	Reimbursement for forensic investigations and breach identification costs
✓	Reimbursement for fines and penalties (HIPAA up to $50,000 per violation; Privacy Shield $40,000 per violation; GDPR up to 4% of annual turnover)
✓	Other damages, perhaps subject to a liability waiver or cap (includes consequential damages and direct)
✓	Termination rights triggered by breaches (e.g., deeming a data security incident involving loss of sensitive data a material breach)
Key issue: Is contracting party responsible if contracting party fails to prevent security incidents or only if contracting party causes the security incident	


Selection
Contracting
Governance

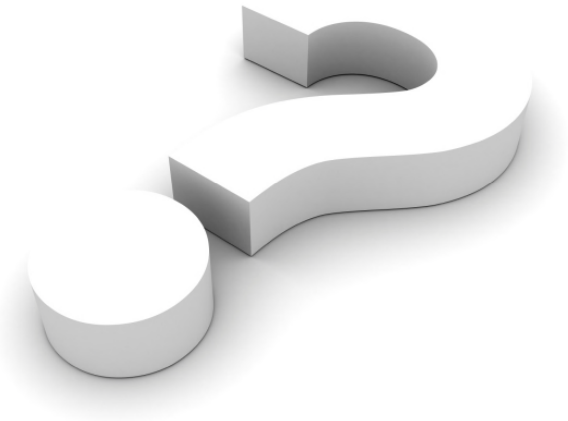
Following up in Governance

- Security team explicitly takes responsibility
- Implementation of risk mitigations identified during contracting
- Follow-on questionnaires and certifications and ongoing monitoring
- “Data map” showing which contractors have access to which data
- Security audits
- Review of audit reports and follow up on exceptions or identified vulnerabilities
- Rigorous policing of access rights (particularly those where User IDs are generally shut off, based on a feed from the HR systems)

Conclusion

- Privacy or data security breaches can have high impact.
- The legal and regulatory framework is complex and depends on your industry, where you do business, what data you have and other factors.
- Cloud contracts may involve particularly high risks.
- The best path to reduce those risks is diligence in:
  - Selection of secure cloud suppliers
  - Contract negotiation
  - Governance

QUESTIONS



Linda Rhodes
Partner
+1 202 263 3382
lrhodes@mayerbrown.com

Brad Peterson
Partner
+1 312 701 8568
bpeterson@mayerbrown.com

Joe Pennell
Partner
+1 312 701 8354
jpennell@mayerbrown.com

Reminders and Upcoming Webinars

- A recording and link to the materials from this program will be distributed by email to you in the next day or two.
- For those applying for CLE credit, please note that certificates of attendance will be distributed within 30 days of the program date.
- Watch for our next webinar invitation coming in the next week or so. We will deliver a GDPR and the Cloud Update on December 6.
- To submit topic ideas for future programs, please email us at TechTransactions@mayerbrown.com.

MAYER·BROWN