MAYER | BROWN

Software as a Service

What You Need to Know

June 2019

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

Lei Shen
Partner
+1 312 701 8852
lshen@mayerbrown.com

Rohith George
Partner
+1 650 331 2014
rgeorge@mayerbrown.com

Technology Transactions Practice

- More than 50 lawyers around the world are focused on helping clients develop and manage relationships with suppliers of critical services and technology

- Experience in 400 critical services that are sourcing deals with a total contract value exceeding $200 billion, including data, digital, outsourcing and software

DATA RIGHTS, USE, PRIVACY AND PROTECTIONS

DIGITAL SERVICES

OUTSOURCING

SOFTWARE DEVELOPMENT, LICENSING AND INTEGRATION

Market Recognition

"Band 1" ranking in IT/Outsourcing for 15 consecutive years
(*Chambers* 2004-2019)

"We have never been disappointed. They are worth their weight in gold." ~ *Chambers USA 2018*

"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*

Law360 **2016 Technology Practice Group of the Year**

Ranked as one of the top law firms 2009 - 2018 on World's Best Outsourcing Advisors list for The Global Outsourcing 100™

Named "MTT Outsourcing Team of the Year"
in 2014 and ranked in the top tier from 2010 through 2018

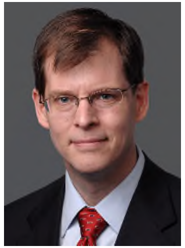
Cybersecurity & Data Privacy Practice

- **Comprehensive** and **integrated** approach to cybersecurity and data privacy challenges.
- Practice comprises **more than 50 lawyers worldwide** from disciplines that include litigation, regulatory, corporate, business and technology sourcing, government affairs and global trade, intellectual property, enforcement and employment.
- We build **tailored** teams and **leverage** our **broad** and **deep experience** across disciplines to help clients prioritize and manage their cyber risks and data privacy obligations in a proactive and coordinated manner across their enterprises with a focus on the following core areas:
  - Incident Preparation and Breach Response
  - Litigation
  - Strategic Counseling and Corporate Governance
  - Vendor and Supply Chain Management, Contracting and Data Transfers
  - Regulatory and Compliance
  - Policy and Advocacy

MARKET RECOGNITION

- *Law360*
  Cybersecurity & Data Privacy Practice Group of the Year 2018
- Three lawyers named "**Cybersecurity and Data Privacy Trailblazers**" by ***The National Law Journal***.
- Our lawyers are regularly named to ***Cybersecurity Docket's*** **"Incident Response 30,"** a list recognizing 30 of the "best and brightest Incident Response attorneys and compliance professionals in the industry."

Speakers



BRAD PETERSON

Brad Peterson is a partner in Mayer Brown's Chicago office. He leads Mayer Brown’s global Technology Transactions practice. Brad’s practice focuses on data, digital, outsourcing and software transactions with a particular emphasis on financial technology. His experience includes data licensing and analytics; digital services such as IaaS, PaaS, and SaaS; outsourcing of the full range of information technology (IT) and business process functions; and core systems modernization, ERP and other software licensing, development and integration transactions. His experience also includes projects in emerging technologies such as artificial intelligence (AI), robotic process automation (RPA), blockchain and other distributed ledger technologies (DLTs).

LEI SHEN

Lei Shen is a partner in the Cybersecurity & Data Privacy and Technology Transactions practices in Mayer Brown’s Chicago office. Lei advises clients regarding a wide range of global data privacy and security issues. She advises companies on navigating and complying with state, federal, and international privacy regulations, including with regard to global data transfers, data breach notification, the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Children’s Online Privacy Protection Act (COPPA), CAN-SPAM, and more. She also advises on e-commerce issues such as electronic contracting and signatures, as well as on issues concerning mobile privacy and emerging technologies, such as telematics services, Internet of Things, and big data.

ROHITH GEORGE

Rohith George is a partner in the Technology Transactions practice in Mayer Brown's Palo Alto office. Rohith’s practice focuses on helping companies negotiate complex commercial arrangements involving mission-critical technologies. This includes advising clients in the execution of major business transformations that involve the implementation and integration of technology solutions; in the acquisition, development, and/or licensing of rights in a wide variety of emerging technologies and related services; in the negotiation and execution of SaaS, PaaS, IaaS, BaaS and other XaaS agreements; in a variety of transactions involving the outsourcing of business process and technology functions and on IT issues relating to major corporate transactions (e.g., acquisitions, divestitures, strategic alliances, spin-offs, etc.), including assisting with front-end diligence, negotiation of transaction agreements, and post-closing transition and integration.

MAYER | BROWN

Agenda

1. Key Commercial Contracting Issues
2. Customer-Facing SaaS Issues
3. Privacy and Security Issues

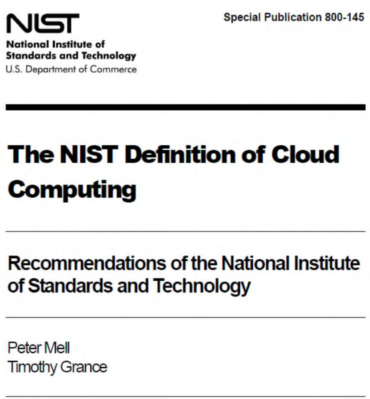
Key Commercial Contract Issues

What Is Cloud Computing?

NIST

National Institute of Standards and Technology Definition

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.



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance

Cloud Characteristics

- On-Demand Self-Service
- Broad Network Access
- Pool of Shared Resources
- Rapid Elasticity
- Measured Service

What is Software as a Service (SaaS)?

LAYER	CUSTOMER INTERNAL	IAAS CLOUD	PAAS CLOUD	SAAS CLOUD
Network	C	P	P	P
Storage	C	P	P	P
Server	C	P	P	P
Operating System	C	C/P	C/P	P
Applications	C	C	C/P	P
Data	C	C	C	C/P

C = Customer Controls
P = Provider Controls

What Drives Adoption?

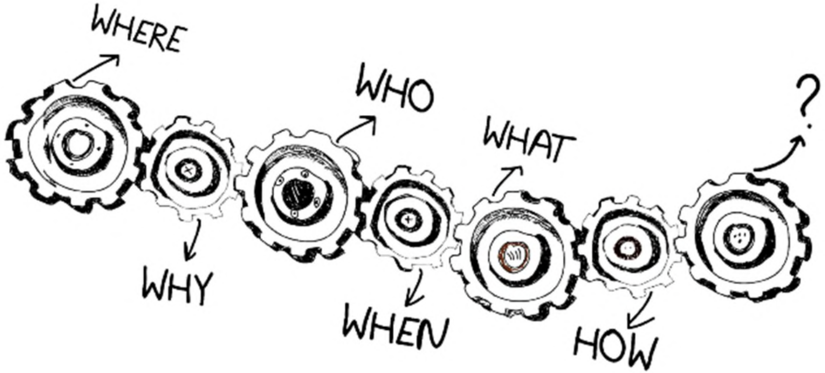
- **Speed** – already built
- **Cost** – low investment + economies of scale
- **Scalability** – cloud provisioning of increased capacity
- **Ease** – SaaS provider does most of the technical work
- **Capability** – now being used by external partners and internally for critical systems such as ERP and emerging technologies such as AI and blockchain

How are SaaS Deals Structured?

- The SaaS provider agrees to provide a “Service” as described under a link such as www.SaaS-provider.com/service/description
- The customer’s use is limited, including through “policies” under links
- The customer has no rights to the software in normal conditions
- The customer “owns” data that it stores on the SaaS provider’s systems and contract provisions govern the SaaS provider’s use and storage of the Customer’s data
- The customer pays capacity-based and usage-based fees
- Liability is limited

What are the Key Commercial Issues?
Use & Users

- Use is limited as in a software license based on locations, purposes, users, volumes, etc.
- Consider expansion to:
  - Broader enterprise
  - Customers and suppliers
  - Divested companies



- Consider exchange rights, reassignment and other rights
- Consider "indirect use" risk when using SaaS with other systems

What are the Key Commercial Issues? Pricing

- Pricing metrics are based on volumes such as number of users, transactions, records, or uses
- If SaaS provider has right to change pricing, consider:
  - Minimum notice requirements
  - Limitations on increases
- Minimum revenue commitments may apply
- Limit charges for additional services

What are the Key Commercial Issues? Operational

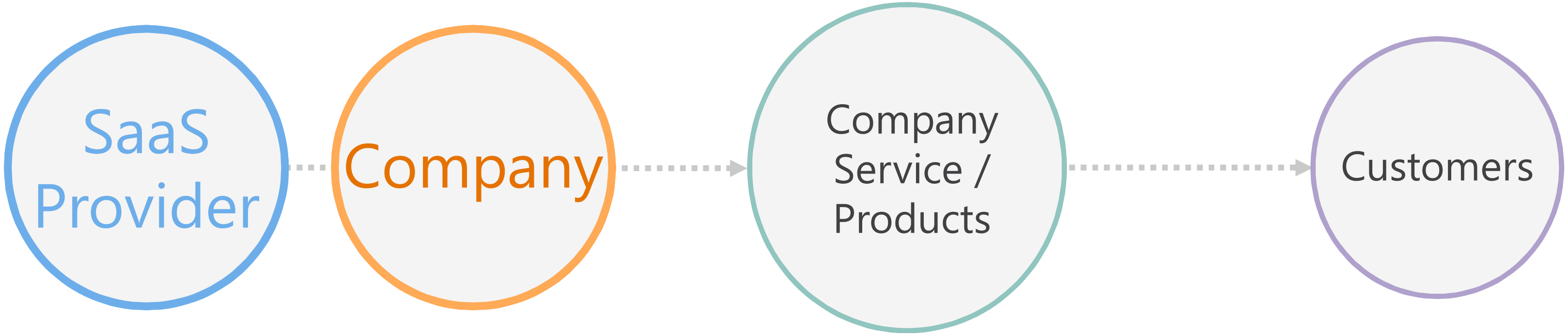
- Commitments on features and functions
  - Minimum functional requirements, e.g., for compatibility
  - Advance notice of and limits on disruptive change
  - Service level requirements and financial incentives for performance
- Governance rights, including discussion, audit and information rights
- Continuity:
  - Limits on suspension or termination of services, including in disputes
  - Disaster recovery/business continuity
  - Post-termination assistance

What are the Key Commercial Issues? Legal

- Provider rights to change contract terms by changing “policies” and “service terms” incorporated by reference through links
- Restrictions on transfer of controlled items across national borders
- Provider’s use of customer data, e.g., “to improve our Services”
- Representations and warranties, particularly on performance and people
- Indemnities
- Limitations of liability
- SaaS provider right to terminate or suspend services

Customer-Facing SaaS Issues

Traditional SaaS Agreement

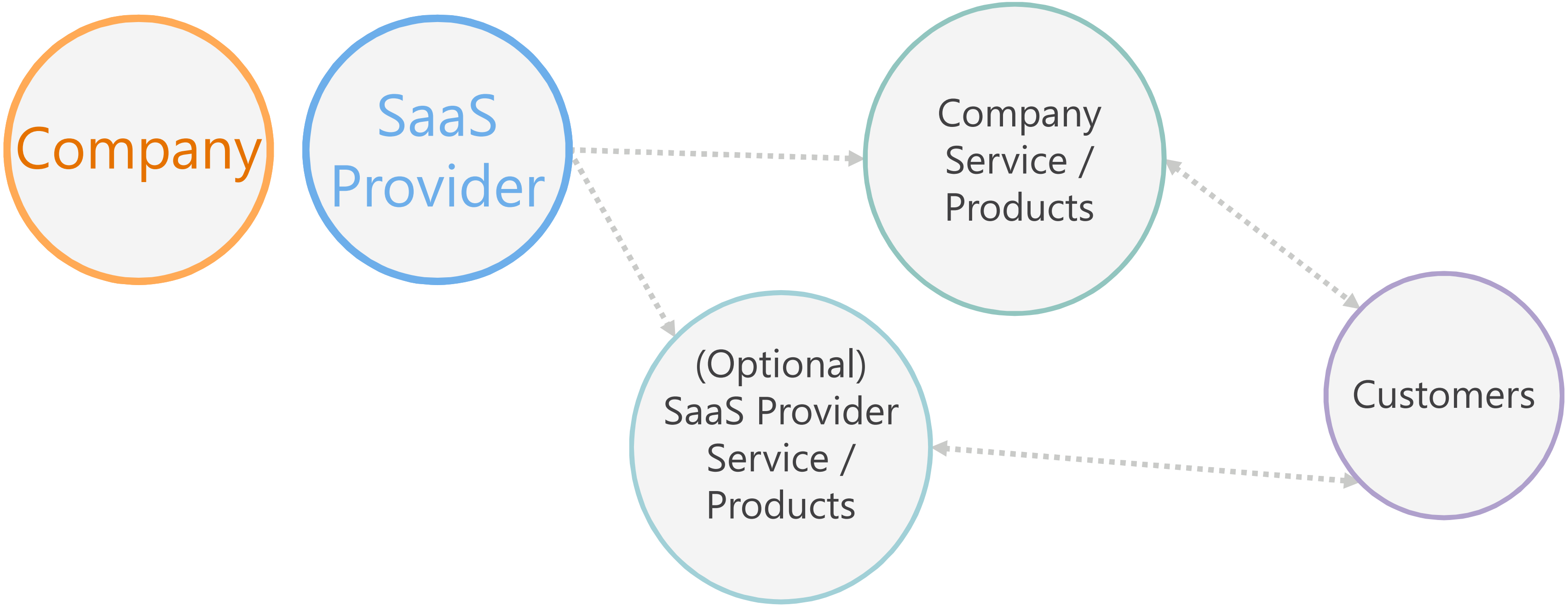

SaaS Provider

Company

Company Service / Products

Customers

Customer-Facing SaaS Agreement


Company
SaaS Provider
Company Service / Products
(Optional) SaaS Provider Service / Products
Customers

Sample Customer-Facing SaaS Deals

- White-labeled/“powered by” fintech lending platforms
- Multi lender platforms (marketplace/“many-to-many”)
  - Run by technology companies or even traditional banks
- Online casino gaming platform agreements
- Connected vehicles/in-vehicle telematics platforms
- Online food ordering/delivery platforms

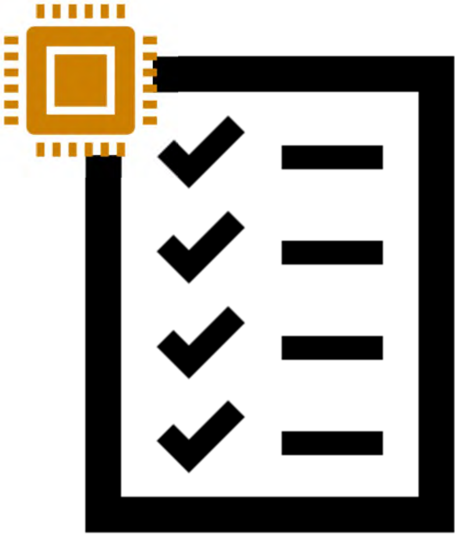
Key Customer-Facing SaaS Issues:
Scope of Services, Pricing and Service Levels

- Scope of Services
  - Detailed scripting may be required for (a) customer journey on SaaS platform and (b) SaaS provider personnel's interaction with customers
  - Detailed business requirements documents may be developed
- Pricing
  - SaaS provider compensation may be based on customer sales
  - Unlike back-office services, company's primary focus may not be on keeping charges low
- Service Levels – heavily focused on metrics measuring customer experience

Key Customer-Facing SaaS Issues: Control Over The SaaS Platform

- What rights does the provider have to change the SaaS platform?

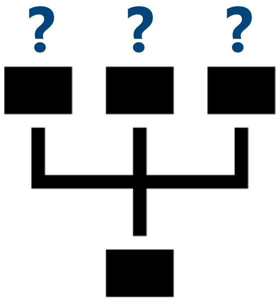
- What rights does the company have to require changes?



Key Customer-Facing SaaS Issues: Customer Complaints

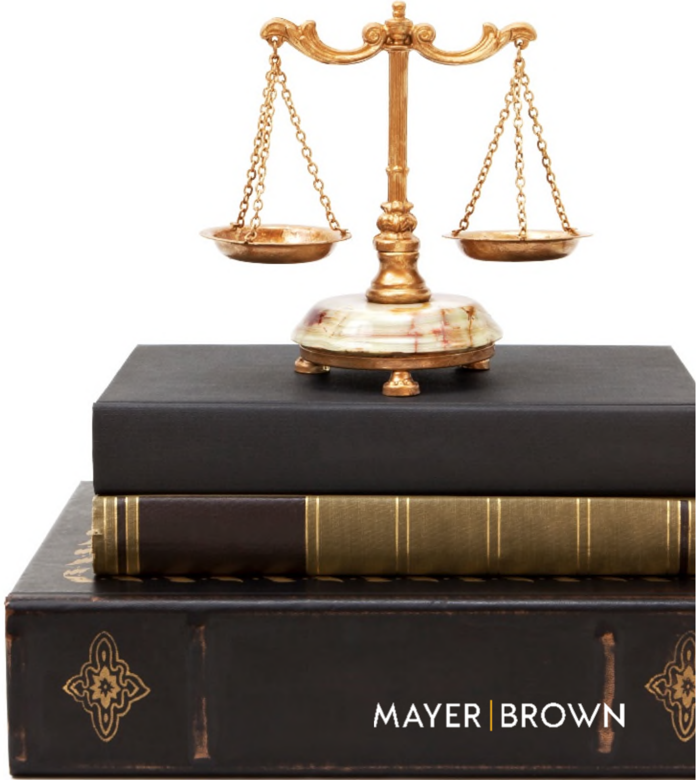
- Direct customer contact may increase the risk of a reputational or regulatory issue

- Which party will handle customer complaints?



Key Customer-Facing SaaS Issues: Compliance with Laws

- Your company will be liable for the platform's non-compliance
- SaaS provider will only want to comply with laws applicable to its provision of services
- Potential compromises:
  - SaaS provider must comply with company's compliance instructions
  - SaaS provider is responsible for contract breaches that result in company being non-compliant with any laws



Key Customer-Facing SaaS Issues: Antitrust, Non-Competition, And Exclusivity

- Can companies participating on a marketplace SaaS platform see other participants’ pricing or other competitively sensitive information?
- What reasonable restrictions can you apply to the SaaS provider’s contact with your customers?
- Can the SaaS provider sell its own products to your customers (e.g., “Turn-Down Program”)?
- What can be done (via contract or operationally) to prevent (and avoid the appearance of) collusion?

Key Customer-Facing SaaS Issues: Intellectual Property

- Trademarks and branding: company must reserve quality control/approval rights over mark usage
- Data ownership and use rights
  - What rights does the provider have to use data generated by company’s use of the SaaS platform?
- Ownership of developed IP
  - Can developed IP containing both parties’ sensitive materials be practically separated upon termination?
  - If not, do both of the parties (or neither of the parties) get post-termination ownership/use rights?

Key Customer-Facing SaaS Issues: Agency

- How is the SaaS provider allowed to market on the company's behalf?
- Clearly define the scope of any representative or agency authority granted to the SaaS provider in the agreement

Key Customer-Facing SaaS Issues: Liability Provisions

- There are no clear market standards for limitations of liability in customer-facing SaaS deals yet
- In the customer-facing context, standard back-office service contract assumptions and rationales about liability provisions may no longer apply
  - Example: lost profits arising from breach of contract may be considered direct damages under applicable state law
- Indemnities for SaaS provider’s sale of its own products to your customers
- Company may want to retain the right to control the defense of customer and regulator claims that are subject to indemnification by the SaaS provider

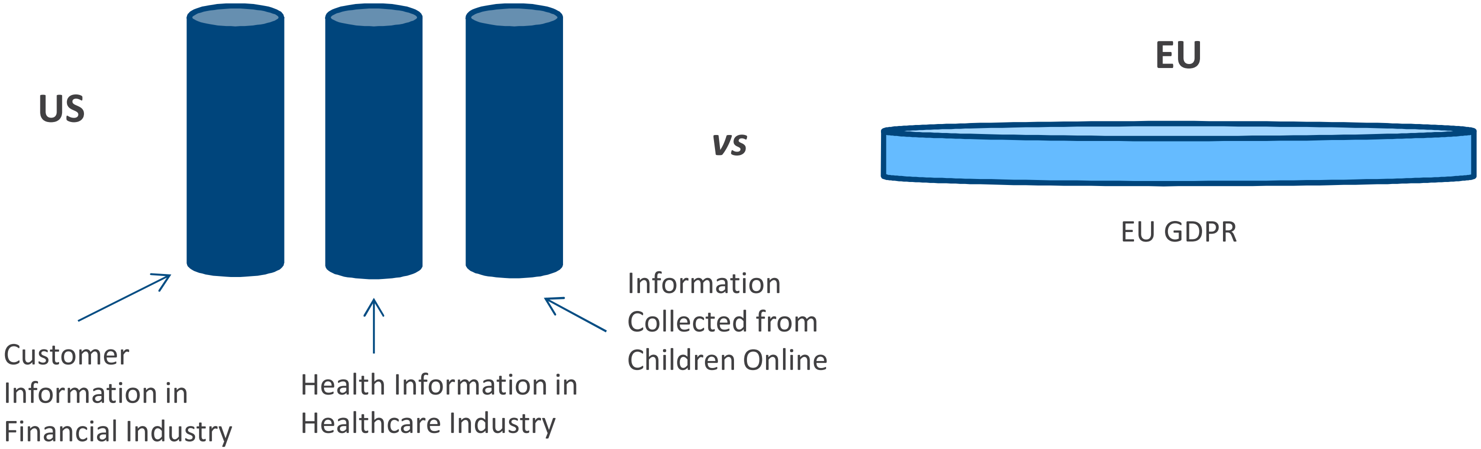
Privacy and Security Issues

Key Data Privacy Considerations

1. **What types of data will you be storing with the SaaS provider? What data privacy laws are applicable to that data?**

Overview of Privacy Laws – US vs. EU

- US privacy laws are sectoral rather than overarching like EU
  - **Federal**: GLBA, HIPAA, COPPA, FERPA, etc.
  - **State**: state data breach notification laws, CCPA, state security laws, etc.


US
vs
EU
EU GDPR
Customer Information in Financial Industry
Health Information in Healthcare Industry
Information Collected from Children Online

MAYER | BROWN

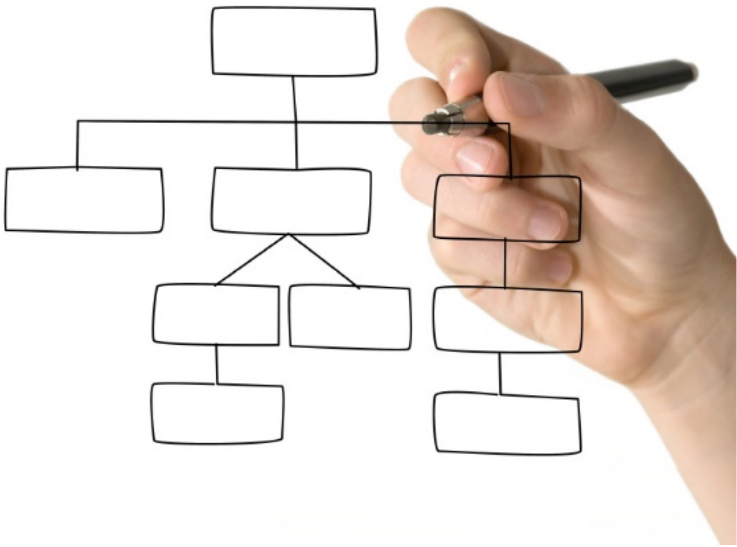
Overview of Privacy Laws – Personal Data

	U.S.	EU
DEFINITION OF PERSONAL DATA	• Varies from very narrow to very broad • **NARROW** data breach notification laws, HIPAA, etc. • **VERY BROAD** CCPA and CCPA-like laws	• **BROAD**

Overview of Privacy Laws – Personal Data

Examples of Types of Personal Data to Consider:

- EU personal data
- Data subject to data breach notification laws
- Financial data
- Health data
- Biometric data
- Children’s data
- Many others



Key Data Privacy Considerations

1. What types of data will you be storing with the SaaS provider? What data privacy laws are applicable to that data?

2. **Where will the SaaS provider be storing, accessing and transferring the data?**

Location Considerations

Where will the SaaS provider be storing, accessing and transferring the data?

Consider:

- Data transfer restrictions (e.g., GDPR, LGPD)
  - Includes transfers from customer to the vendor and also from the vendor to the vendor's affiliates and subcontractors
- Data localization restrictions (e.g., China, Russia)
- Remote-access considerations
- Other countries (e.g., embargoed countries)

Key Data Privacy Considerations

1. What types of data will you be storing with the SaaS provider? What data privacy laws are applicable to that data?

2. Where will the SaaS provider be storing, accessing and transferring the data?

3. **How will the SaaS provider be using/processing the data?**

Data-Use Considerations

How will the SaaS provider be using/processing the data?

Consider:

- Use restrictions under applicable data privacy laws
- Use restrictions when data was collected
  - User consent
  - Privacy policy
- SaaS provider’s ability to use data for its own benefit/profit
  - Improvement of services/security analysis
  - Data analytics/benchmarking
  - Issues

Key Data Privacy Considerations

1. What types of data will you be storing with the SaaS provider? What data privacy laws are applicable to that data?

2. Where will the SaaS provider be storing, accessing and transferring the data?

3. How will the SaaS provider be using/processing the data?

4. **How will the SaaS provider be returning or destroying the data upon termination of the services?**

Data Return / Destruction Considerations

How will the SaaS provider be returning or destroying the data upon termination of the services?

Consider:

- Data destruction requirements
  - Industry standards
- Length of retention of data
- Protection of retained data

Key Data Privacy Considerations

1. What types of data will you be storing with the SaaS provider? What data privacy laws are applicable to that data?
2. Where will the SaaS provider be storing, accessing and transferring the data?
3. How will the SaaS provider be using / processing the data?
4. How will the SaaS provider be returning or destroying the data upon termination of the services?
5. **Will the SaaS provider be subcontracting any of the data processing?**

Subcontracting Considerations

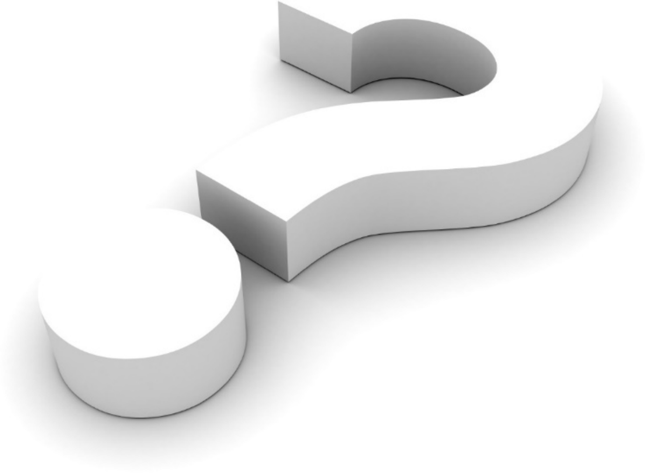
Will the SaaS provider be subcontracting any of the data processing?

Consider:

- Approval rights for subcontractor
- Flow-down of data protection and security terms
- Data-transfer requirements
- Liability

Key Data Security Considerations

1. **What types of data will you be storing with the SaaS provider? What data security laws are applicable to that data?**



Data Security Considerations

What types of data will you be storing with the SaaS provider?
What data security laws are applicable to that data?

Consider:

REGULATED DATA TYPES	DATA SECURITY LAWS
• EU personal data • Financial data • Health data • Biometric data • Account login information • Other types of data	• State security laws • EU GDPR • HIPAA • GLBA • MA data security • NY DFS • Other countries (e.g., China) • Many other laws

Key Data Security Considerations

1. What types of data will you be storing with the SaaS provider? What data security laws are applicable to that data?

2. **What data breach notification requirements will the SaaS provider agree to?**

Data Breach Notification Considerations

What data breach notification requirements will the SaaS provider agree to?

Consider:

- Scope of notification
- Time to notify
- Information provided
- Cooperation
- Liability

Key Data Security Considerations

1. What types of data will you be storing with the SaaS provider? What data security laws are applicable to that data?
2. What data breach notification requirements will the SaaS provider agree to?
3. **What data safeguards and protocols will the SaaS provider apply to the data? What audit rights do you have?**

Data Safeguards Considerations

What data safeguards and protocols will the SaaS provider apply to the data? What audit rights do you have?

Consider:

- Certifications and industry standards
- Encryption and other safeguards
- Other security requirements
- Audit rights

Compare to:

- Data security laws and requirements applicable to data
- Customer's data security requirements for its vendors

Americas | Asia | Europe | Middle East

mayerbrown.com