10 Strategies When Drafting and Negotiating Digital and Technology Agreements

Phylliss DelGreco, VP & Associate General Counsel, New York Life

Janet Abrams, VP, Business & Legal Affairs, Viacom Media Networks

Daphne Turpin Forbes, Senior Attorney, Microsoft

Yoon H. Chang, Senior Associate Counsel, Walmart

Andrea R. Watson, Group Counsel, Intel Corporation

Discussion Topics

1. Due Diligence
2. Data Ownership and Management
3. Cybersecurity Risks
4. Indemnification
5. Limitation of Liability
6. Termination Rights and Transition Services
7. Audit Rights
8. Subcontractor Commitments
9. Business Continuity
10. Service Level Commitments; Service Credits

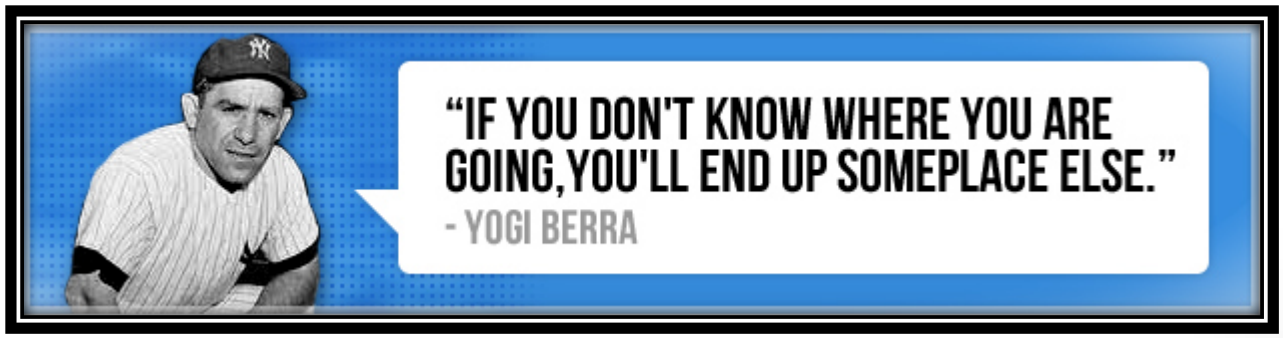
Due Diligence

1. Value Drivers
2. Checklists/

Questionnaires

3. Term Sheet

Ideally, every deal should use these three tools, in this order.



Data Ownership and Management

Ownership of data is assumed to belong to the entity that generated or purchased it. Data ownership is determined by the laws of the nation which the date is being used.

1) Who owns the data?
2) Is there any license of the data?
3) Restrictions on the use of data
4) Ownership of deliverables
5) Work for hire or work product

Cybersecurity Risks

- Companies driven by digitization, innovation and standardization mandates are now leveraging third parties in new ways and for more critical activities.
- The number of elements that come into play are exponentially greater than what we experienced in the past.
- The constant interplay with and between each of these elements creates constant risk.
- Bad actors adopt a “weakest link” methodology looking for points of vulnerability among the many elements.
- Regulated companies must now contend with Regs and Rules focused on Cybersecurity, Data Protection and Privacy, and Third Party Risk.

Indemnification

Indemnification is an agreement by one party (indemnifying party) to pay or reimburse for the losses or damages or liabilities incurred by another party (indemnified party). Indemnification provisions are a means of **shifting risk** between parties to an agreement.

The obligation to indemnify may apply to:

- Direct Claims
- Third Party Claims
  - Standard: infringement or misappropriation of IP (uncapped)
  - Not Standard: Data Security Breach (capped); Regulatory Claims (e.g. GDPR)

The indemnifying party will generally agree to Indemnify, Defend and/or Hold Harmless

Limitation of Liability

- Approach to Limitation of Liability will vary greatly from buy-side to sell-side
- Ensure any Caps on Liability are appropriate for the type of product and service
  - Fully understand how the product and service will be used
  - What data (if any) is in play
- Be smart when introducing a “Super Cap”
- Indirect Damages vs Direct Damages
- Carve-outs to Caps on Liability

Termination Rights and Transition Services

Term of Services - Defined duration or term (e.g., an initial term of two years, with certain renewal terms). Auto-renewal may apply.

Termination For Breach - Termination may happen for a number of reasons, including an inability of the service provider to resolve problems, meet commitments, or match the capabilities of competitors.

Termination for Convenience

- By Customer: Early termination fees may apply
- By Provider: Minimum notice required

Effects of Termination – Return or Destruction of Data

Transition Services - Ensuring service continuity during the transfer of responsibilities for service provision

Audit Rights

Why Audit Rights?

- To Mitigate Risks;
- To Evaluate the Efficiency of Controls; and
- To Continuously Improve Internal Processes and Procedures

Key Areas of Risks

- Identity and Access Management
- Data Protection
- Technology Risks
- Operations
- Regulatory

Subcontractor Commitments

- Independent consultants
- Written assignment with permission
- Background checks
- Permits, documentations, or license required including immigration
- Compliance with anti-corruption laws including FCPA
- Confidentiality include ISA
- Not joint employer
- Information Security addendum – how data is stored and transmitted
- Assignor responsible for behavior of consultants

Business Continuity

- Supplier's must have in place a disaster recovery and business continuity plan that ensures full recovery and restoration of operations in an appropriate timeframe based on criticality of the Services.
- The DR and BC Plan should include procedures for back-up/restorations of operations, applications and services including detailed, documented plan for responding to prolonged disruption in Services.
- Supplier' should maintain a secondary disaster recovery site separate from, and an appropriate distance from the primary Service location.
- Supplier's should have a plan in place for the transition back from the disaster recovery site to the primary Service location.
- RTO vs RPO - require both to be stipulated in the Contract

Service Level Agreements / Service Credits

What kind of support will the vendor provide for the product:

1. Type of support service – critical, medium, and phone support
2. Response and resolution times depending on the type of support
3. New releases and updates are at no additional cost
4. Remedy—service credits or percentage of monthly charge for support services
5. Termination right for failure to cure