

Be a Better Negotiator of Cloud Contracts

Article

August 12, 2024 | *Legal Dive* | 5 minute read

The extensive – and expensive – impact of CrowdStrike’s update, which led to global system failures in July, has company leaders considering vulnerabilities from their cloud-based software and services.

Many executives think they have zero ability to negotiate important terms – such as blanket acceptance of updates – in their cloud contracts. That is simply not the case; the terms of those contracts should be negotiated to mitigate risk to the enterprise.

Here are four standard sets of terms found in cloud contracts that executives, working with their legal partners, should have top of mind when they’re negotiating terms.

Term 1: Service Performance Guarantees

Downtime of a cloud service can cause far-reaching disruptions to your business and operations, potentially leading to significant financial losses to the enterprise. Ensure the presented contract specifies sufficient performance levels given the relative importance of the availability of the cloud service, including uptime guarantees and penalties for non-compliance by the vendor.

The following are service level terms that are typically found in vendor forms:

1. Uptime guarantees: Establishes a minimum level of availability.
2. Penalties for downtime: Defines financial penalties or service credits for failing to meet the minimum level of availability.

Negotiating Clear Performance Metrics

Related People

Jeffrey

Partner

HOUSTON

+1.713.221.1439

jeff.andrews@bracewell.com

Related Industries

[Technology](#)

Related Practices

[Outsourcing](#)

[Technology Transactions](#)

[Intellectual Property](#)

To protect your interests, you must set meaningful performance metrics for the vendor and include those metrics in the cloud contract. Here are some terms to negotiate.

Uptime Guarantees

- Ask for availability metric to be set at least at 99.99 percent.
- Ask for service levels measuring resolution for incidents/problems based on their severity, and ensure the severity definitions correspond to the anticipated impact of those incidents/problems on your business and operations.
- Eliminate provisions requiring you to report defaults for credit – the vendor is monitoring their service delivery, and already knows when their service is not available.
- Narrow blanket exceptions for matters purportedly outside of the vendor's control that practically excuse most or even all service level failures.
- Include performance or service credits for non-compliance.

Monitoring and Reporting

- Require regular performance reports.
- Require real-time monitoring.

Escalation Procedures

- Define the steps to be taken in case of performance issues.
- Include contact points and escalation timelines.
- Add termination right for chronic service level failures.

Term 2: Unilateral or Forced Changes by Vendor

Cloud-based vendors often reserve the right to make unilateral changes to their services and the terms of their contracts. These changes can adversely affect your business and operations, such as changes to the service that eliminate or alter important features and functionality, and upgrades that require changes to your retained IT environment – and the costs associated with them.

The following are terms typically found in vendor forms that allow the vendor to make unilateral changes to their services and the terms of their contracts:

1. Changes to incorporated terms: Vendors typically reserve the right to make changes to terms and policies (e.g., use policies; service levels) incorporated into the contract by reference, in essence allowing them to unilaterally amend the contract.

2. Changes to services: Vendors typically reserve the right to upgrade or otherwise change their services at any time, making only subjective commitments that such changes will not materially change the features or functionality of their services, and often making not commitments that such changes will not adversely affect their customers.

Negotiating Unilateral Changes

Take steps to limit vendors' ability to make unilateral changes to their services or the terms of their contracts that may be costly or disruptive to your business operations.

Advance Notice

- Require a specified period of advance notice for any changes.
- Try to incorporate all policies as they exist upon signing.

Approval Rights

- Try to retain the right to approve or reject changes that adversely affect your business or operations.
- Seek commitments that changes cannot require you to incur additional fees or increase your costs.

Termination Rights

- Include the option to terminate the contract without payment of termination fees, if changes adversely affect your business or operations.

Term 3: Customer Data

In today's environment, understanding the protection being afforded your data, and the actual or potential use of your data, are both critical. Misuse of data or security breaches exposing customer information can lead to severe financial, reputational and legal repercussions. The contract should clearly define data safeguarding requirements and data usage restrictions. Unfortunately, most vendors side-step these issues in their form contracts, or address them in only a limited way that inadequately protect their customers.

The following are terms typically found in vendor forms that address data safeguarding and data usage:

1. Data use: Vendor contracts often allow them to use their customers' data "as necessary" to provide their services – but what is necessary, and who decides?
2. Data protection: If Vendors address what they will do to safeguard their customers' data, they typically only do so using qualified terms that lack

specific commitments. Vendors will not agree to comply with unique customer requirements, except with private cloud arrangements.

3. Compliance requirements: While Vendors may agree to comply with applicable data privacy laws and regulations, they often do not include provisions in their contracts that are sufficient to enable their customers to also comply with those laws and regulations.

Negotiating Data Protection

Be proactive and seek meaningful data protection clauses to safeguard your data and to define how vendors can use your data.

Data Usage Limits

- Specify what uses of customer data are permitted and not permitted.
- Prohibit use of data except in the performance of the contracted service.
- Specify that your data is always your confidential information and should be protected as such.
- Require the vendor to represent and warrant that it will not use customer data except as expressly permitted by the contract.
- If ancillary use is truly necessary, require data to be used only in an aggregate form not capable of identifying any person or entity.

Compliance Requirements

- Ensure the provider complies with all relevant data protection laws.
- Seek to incorporate the vendor's security and privacy policies by reference into the contract.
- Changes to the vendor's policies cannot be adverse to customer (in customer's sole discretion, if possible), and cannot result in them being any less robust than as of contract signing.
- If a data breach occurs, reserve the right to terminate.

Term 4: Termination Assistance and Return of Customer Data

Change is difficult, even when your organization has outgrown a provider's offering and capabilities and you need to terminate the relationship. Enterprise CIOs tell horror stories about vendors refusing to provide termination assistance and having data returned in an unusable format. Ensuring smooth termination and data migration is essential.

The following are terms typically found in vendor forms that address data safeguarding and data usage:

1. Data format requirements: Vendors often do not make any commitments regarding the format in which data will be returned.
2. Termination assistance: Vendors often do not make any commitments regarding any assistance they may provide in connection with termination, other than making customer data available for download.
3. Data retention and deletion: Typically, the only commitment vendors will make in connection with termination events is that they will make your data available for download for a short period of time following termination, after which it may be deleted.

Negotiating Smooth Migrations

Take steps to incorporate clauses that facilitate smooth migrations upon termination.

Data Return and Format

- Define the format in which your data must be returned, or at least specify that your data must be returned in an industry-standard, platform-agnostic format.
- Protect your access to your data by insisting that the vendor cannot withhold any your data as a means of resolving a dispute.
- Require the timely return of all or any portion of your data at your request.

Migration Assistance

- Require the vendor to assist with data migration, any assistance required to reasonably interpret that data, as well as other reasonable assistance you may request in order to ensure a smooth migration of services.
- Include timelines and responsibilities for both parties.

Data Deletion

- Ensure that the vendor retains your data for a sufficient period of time to enable you to completely download and transfer it back in house or to a successor provider, and that after that period of time they delete all remaining copies in their possession or control.
- Include processes for you to verify data deletion.

Conclusion

Navigating the complexities of cloud contracts requires a keen understanding of risks and effective mitigation strategies. By addressing the foregoing terms and conditions, you can create contracts that effectively protect your interests.

Article was originally published by Legal Dive on August 9, 2024.