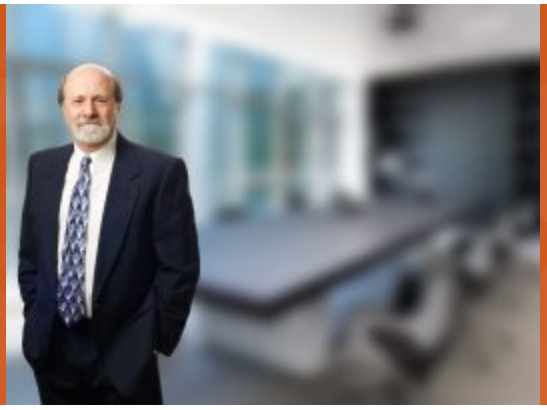
Head in the Clouds – A Cloud User's Contract Checklist

By:Howard G. Zaharoff
February 03, 2016



Negotiability

Clickwrap contracts usually contain provisions that are bad for Users.

Amendment

Can Provider amend the contract unilaterally?

- Best if all amendments require mutual agreement.
- User at least needs advance notice and right to terminate and migrate if dissatisfied with changes.

Interoperability

Users may require assurance that Provider's cloud program(s) will be kept interoperable with other key software in the User's computing environment.

- Increasing efforts to develop standards (e.g., by Cloud Security Alliance and Distributed Management Task Force) to facilitate interoperability and avoid "vendor lock-in."

Warranty, Liability and Indemnification

- What reps and warranties does Provider offer?
    - » Service levels (see "Performance Standards" below)
    - » Legal compliance: privacy, data protection, data breach, export controls, etc.
    - » High level privacy and security (logical and physical)
    - » No IP infringement
- What are the remedies for breach? (Are they exclusive?)
- Does Provider disclaim consequential damages? (Is this reciprocal? Are there appropriate exceptions, e.g., for violations of confidentiality and IP?)
- Does Provider cap its total liability? (Is this reciprocal? Are there appropriate exceptions, e.g. indemnification for IP infringement?)
- How does Provider address IP infringement by Provider system/service?
- Users should consider Cyber Liability Insurance to protect against fallout from data breaches.

Performance Standards

Is there a service level agreement (SLA) that assures reasonable performance?

- May not be negotiable (often fixed for all users)
- Avoid Provider right to amend unilaterally
- Ensure adequare remedies for breach (e.g., credits and/or right to terminate)

Support

What initial and ongoing support does Provider offer, e.g., user training, business hour support line, after hour support, ongoing training, etc.

Privacy and Security

Does contract properly address privacy, security (logical and physical), data integrity, access, data ownership/use and breach notification/correction?

- Users should seek express confirmation that they own their data and limits/controls over Provider's (and third parties') access and use of their data.
- Depending on industry and type of data, Users may require:

    » Knowledge of and/or control over where data is stored/processed – e.g., EU personal information may only be delivered to people/places with adequate protection

    » Proof of proper handling/integrity

    » Dependable physical security

    » Sophisticated data security, including encryption

    » Restrictions on use, access and processing

    » Satisfaction of special requirements, e.g., Business Associate Agreement (for health information protected by HIPAA)

    » Right to audit Provider's on-site practices and/or receive copies of Provider's internal and external audit reports (e.g. SOC 2 and SSAE 16)

    » Breach notification commitments (see next point)

- Mass. G.L. c. 93H and 201 CMR 17:00 impose "Special Standards for the Protection of Personal Information of Residents of the Commonwealth":

    » Users who store PI about Mass. resident must have WISP; heightened rules for electronically stored or transmitted PI, including encrypting PI that travels across public networks; and control of service providers:

    » Must take reasonable steps to select and retain providers "that are capable of maintaining appropriate security
    measures."

    » Must require such providers "by contract to implement and maintain such appropriate security measures for personal information."

Continuity

Are there assurances of ongoing access/service in the event of disasters, outages, data loss, bankruptcy/insolvency and other force majeure?

- Provider should have a Business Continuity Plan and make it available to User, addressing at least:
    - » Does Provider have backup servers or facility (perhaps hot site)?
    - » Is the software (source code and documentation) held by escrow agent? What are the conditions that allow release?
    - » Is all data backed up safely?
- Users may require continuing proof of Provider's solvency, with rights to terminate, obtain apps and retrieve data if standards not met.
- User should consider using multiple providers.

Subcontractors

Can Provider use subcontractors?

- Notice and identification
- Control over who, what and where

Term, Termination and Suspension

Under what circumstances can the User's rights be terminated or its access suspended? What if Provider breaches and the User terminates? (Is User assured access to backup system, migration, refunds, other protections?)

Transition (Exit Strategy)

Will Provider assist in migration to successor or in-house solution?

- Data provided in standard/selected format
- Transition services for a reasonable fee

Governing Law and Jurisdiction

The law that governs, and the place where claims are resolved, can have major impact on duties and disputes.