Companies of all industries are recognizing the need and benefit of moving some if not all of their IT infrastructure to a Cloud whether public or private. Along with this ever increasing movement is the need for better security, redundancy, connectivity, and plenty of power.

In today’s global economy, companies are putting equipment in Data Centers all over the world. While we would like for there to be some sort of standard, there just isn’t. This is why knowing exactly what you are getting into is so important.

Take security for instance... In Germany, “privacy protection” and “data security” are often lumped together or used interchangeably. This often leads businesses to vaguely fear outsourcing their IT resources and losing control of data. By contrast, in Anglo-Saxon countries, there is a clear distinction between the two terms.

In light of differences such as this, we know that not all service providers, or their contracts, are created equal. Companies must clearly differentiate between the technical security of their data and its legal protections before entering into contract negotiations with a provider.
For providers based outside of the US, it is very important to know if they are based in the European Union or the US. Because of the fact that US laws allow the government warrantless access to data stored in a US based providers cloud, many non-US companies are taking another look at their data center of choice.

Regardless of their location or size, businesses must carefully consider multiple aspects of their contracts before signing any deal with a cloud service provider.

Here’s a checklist of the key items your cloud computing contract should address:

- **Service-level agreement:** SLAs should include the amount of guaranteed “uptime,” the process and timeline for dealing with “downtime,” and the consequences for any failures to meet those requirements should be spelled out clearly. You will want to make sure that the remedy for unmet SLAs is beneficial to you the customer, and has teeth, otherwise the SLAs are not worth the paper they are written on. For example “free” service may not be very beneficial, in which case you would prefer to receive some sort of refund.

- **Data Security:** If a contract addressed the issue at all, it is likely to promise to provide only “reasonable” data security, or perhaps to adhere to “industry standard” security practices. While such promises sound good in the abstract, they are open to considerable interpretation and argument. It is preferable to specify an actual, specific, independent security standard and require that it be updated, and perhaps audited, regularly. In addition, for certain kinds of data (e.g., data subject to HIPAA, Gramm-Leach-Bliley, PCI DSS, or the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth), there may be specific security requirements that must be included in the contract. Ideally, the contract should also provide for regular SAS 70, Type II audits, with customer access to the results.

  Finally, the contract should require notice of any security/data breaches, and, to the extent that user notification is legally required, such notice should preferably be in advance of user notification (which should be the provider’s responsibility).

- **Emergency Security Issues:** Providers understandably may wish to have the right to “immediately” suspend an “offending use,” and
possible the service altogether, in the event of an “emergency” issue. The standard for what constitutes an emergency should be clearly defined, should not give much if any discretion or flexibility in its application, and, preferably, should incorporate a “materiality: of similar threshold.

- **Suspension and Termination of Service:** A cloud provider may want the right to suspend service or terminate it altogether upon certain events or conditions. These provisions may not be unreasonable in a contract, however they should be limited in scope and only to truly significant matters. They should provide for an opportunity to cure the alleged violations or some form of escalation rather than instantaneous implementation (except in the case of true emergencies), and give the customer an adequate amount of time to make alternative arrangements for its data or service. You will also want to have assurance that data will continue to be available to the customer, in a usable format, for at least a “commercially reasonable” period of time following any termination. Lastly, in the event of a termination, you will want to make sure that the provider will return or completely destroy any and all data once the transition is complete.

- **Privacy protection:** The BSI Federal Office for Security in Information Technology recommends defining privacy protection agreements. Certain data is not to be used for any purpose other than one required by law or not to be disclosed without proper authorization, such requirements should be included in the contract.

If a Cloud service provider is able to provide encryption of data in both transmission and storage, privacy concerns, and the need for other contractual protections, may be lessened or even eliminated.

- **Location of Data:** Some contracts expressly reserve the right to store customer data in any country in which they do business, and even if it is not addressed, providers may follow similar practices on the (generally legitimate) theory that what is not expressly prohibited is thereby permitted. Geographically dispersed storage tends to be beneficial from a data protection and backup perspective, but it can raise
export control (EAR/ITAR) issues in the context of research data. If this is important to a particular customer, language prohibiting “extraterritorial” storage should be included in the contract.

- **Sub-contracting:** Both parties must agree whether and in what form the provider may subcontract out certain services. Cloud providers should only retain subcontractors with the same level of protection as themselves. In certain industries, such as healthcare, subcontractors must also meet regulatory requirements like HIPAA.

- **Unauthorized or Inappropriate Use:** Contracts may attempt to make customers responsible for affirmatively preventing any “unauthorized” or “inappropriate” use of the cloud service by others, or perhaps to use “best efforts” or “commercially reasonable efforts” to do so. Customers will hold that these services are “in the cloud” and therefore largely outside of customer control, so for the customer, it would be preferable to provide only that the customer will not “authorize” or “knowingly allow” such uses. Such contracts also may require the customer to notify the service provider of “all” unauthorized or inappropriate uses of which it becomes aware. Particularly with respect to cloud providers with broadly stated AUPs or terms of service, such expansive obligations may be burdensome and unnecessary. It may be preferable to replace “all” with “material” or some similar, higher threshold.

- **Ownership of Data:** The contract should expressly make clear that all data belongs to the customer (and/or its users) and that the provider acquires no rights or licenses, including without limitation intellectual property rights or licenses, to use the data for its own purposes by virtue of the transaction. It also may be useful to provide that the service provider does not acquire and may not claim any security interest in the data.

- **Warranty Disclaimer:** At a minimum, the contract should warrant that the service conforms to and will perform in accordance with its specifications (which should themselves be as detailed as possible, to avoid misunderstandings and disagreements) and that it does not infringe any third party intellectual property rights. Without those two warranties, there is no enforceable assurance that the service will in fact do what the provider’s marketing people claim it will do or that the provider even has the right to provide service to the customer. In addition, if the customer is sued for infringement, the customer will have no recourse against the service provider.

- **Indemnification:** Contracts rarely include any form of indemnification benefitting the customer, but such protection can be critical in at least two areas. These are infringement of third party intellectual property...
Checklist for a Watertight Cloud Computing Contract

rights and inappropriate disclosure or data breach. Both are largely, if not entirely, in the cloud provider’s sole control, and both of which can be extremely costly to defend and remedy. If a provider refuses to accept liability for either of these issues on the grounds that it is a “black hole,” the customer should take great warning about the provider’s lack of confidence in its own service and look elsewhere. Ideally, the provider would indemnify the customer for all of its acts and omissions.

- **Automatic Renewal:** Typically contracts include terms for services to auto-renew unless a customer gives prior notice. This is standard practice in the industry, however, it is a good idea to require the provider to send a reminder to the customer when it needs to make a decision about the renewal and give notice of any termination.

- **Exit strategy:** The early return of data must be clearly spelled out. This is especially important if the provider goes out of business or merges, for example. Exit strategies should also entitle clients to recover data from subcontractors if they have any doubts about them.

---

ACT Data Solutions – Colocation and Data Center Consultants

ACT Data Solutions represents over 100 top tier cloud providers nationwide and works with organizations to identify the best fit providers to fill their needs. This process includes locating quality providers, coordinating interaction, soliciting proposals, professionally analyze them, highlight strengths and weaknesses, negotiate pricing and create an environment of highly competitive bidding. ACT charges no fee for this service to clients, but receives a standard commission from whichever cloud provider is chosen. Very similar to how a real estate agent earns a commission. The aim of ACT’s consulting services is to provide professional unbiased expertise and reduce the amount of valuable time and costs spent by organizations and individuals. ACT works in conjunction with small businesses up to fortune 100 companies. To schedule a no cost Cloud discovery call please click below or call **678.878.9400**

---

**LEGAL NOTICE**

This Contract Review Checklist has been prepared for informational purposes only and is not for the purpose of providing legal advice. Your use of this document does not create an attorney-client relationship between ACT Data Solutions, LLC and you. You should not act upon the information set forth herein without seeking professional counsel.