



Cloud Customers' Bill of Rights

Information Law Group LLP - www.infolawgroup.com

Article I – Data Location Transparency. Cloud service providers shall reveal the physical location of the servers that will be processing their cloud customers' data, and shall provide reasonable advance notice if those locations change.

Article II – Security Transparency. Cloud service providers shall provide full information and access to documentation concerning their security policies and measures, including the ability for cloud customers to conduct periodic security assessments and obtain relevant security-related information and documents from the service provider; this information and documentation should address data integrity and availability as well as the confidentiality of customer data

Article III – Subcontractor Transparency. Cloud service providers shall provide cloud customers with notice as to which third parties will have the ability to access customer's data and for what purposes, including subcontractors, subcontractors of subcontractors and so on.

Article IV – Subcontractor Due Diligence and Contractual Obligations. Cloud service providers shall conduct reasonable due diligence and security assessments of subcontractors or other third parties that will have access to customers' data or systems, and shall enter into contracts with such third parties that hold those third parties to substantially similar obligations as in their cloud agreements with their customers; cloud service providers shall manage and similarly limit the ability of their subcontractors to utilize other subcontractors.

Article V – Customer Data Ownership and Use Limited to Services. Cloud customers shall have the right to solely "own" the data they put into a cloud service provider's cloud, and cloud service providers shall use their customers' information solely for the purposes of providing services to the customer, unless otherwise explicitly agreed.

Article VI – Response to Legal Process. Cloud service providers shall provide notice (within hours, not days) of the service of any subpoena or other legal process seeking their customers' data, and shall assist and cooperate with their customers in responding to such legal process.

Article VII – Data Retention and Access. Cloud service providers shall reveal their data search, retention and destruction practices; and shall develop and enable data search, retention and destruction capabilities in order to allow their customers to implement their data retention programs, efficiently effectuate litigation holds, and locate, collect and preserve relevant data, including metadata; cloud service providers shall build in processes and controls that allow for the efficient authentication of data.

Article VIII – Incident Response. In the event a cloud provider suffers a security breach, Cloud providers shall provide prompt notice of the security breach to their affected cloud customers; shall coordinate, cooperate and assist their customers with the investigation, containment and mitigation of the breach; and shall allow their cloud customers to conduct their own forensic assessment of the security breach.

Article IX – Indemnification and Limits of Liability. Cloud service providers shall engage their customers in meaningful discussions and negotiations around indemnification and limitations of liability arising out of security breaches, including consideration of exceptions to limits of liability for security breaches suffered by the cloud service providers.

© 2010, InfoLawGroup LLP