



James River Consulting

Better IT & Services Contracting

www.jamesriverllc.com

A professional services firm specializing in IT and business services contracts, outsourcing, on demand, e-contracting, contracts processes, and contracts management staffing

# Newsletter

Q2 2010

TO RECEIVE BY EMAIL PLEASE REPLY TO [info@jamesriverllc.com](mailto:info@jamesriverllc.com) WITH "EMAIL NEWSLETTER" IN THE SUBJECT LINE

## Feature Article

### Using Contracts to Manage Risk and Compliance in a Complex, Uncertain, and Global Business World

I was recently sent a paper written by a Munich, Germany, information and communications technology (ICT) lawyer, Dr. Thomas Helbing ([www.thomashelbing.com/en](http://www.thomashelbing.com/en)), reporting on the implications for SaaS and Cloud Computing of the February 5, 2010, European Commission (EC) Decision on standard contractual clauses for the transfer of personal data to processors established in third countries (2010/87/EU available at <http://eur-lex.europa.eu>).

2010/87/EU is yet another refinement of the famous—some would say infamous—1995 EU Directive on data privacy. In a nutshell, 2010/87/EU recognizes that when data on EU citizens is transferred outside EU borders, it isn't done in a nice, neat package kind of way. Regardless of whether the data is transferred to a parent or subsidiary company or whether it goes to an IBM or Accenture or other outsourcing provider, access to the data can be had by many other associate providers such as remote infrastructure management services, hardware maintenance technicians, and auditors. Following a "chain is only as strong as its weakest link" rationale, the EC Decision requires third party services providers or "processors" outside the EU to obtain permission from the EU based "controllers" originating the data to allow non-EU third party "subprocessors" access to data. Additionally, the Decision requires processors to impose on subprocessors the same standard clauses required in the contract between the EU controller and the other country processor.

In agreeing to the clauses, subprocessors subject themselves to audits and to legal claims by EU citizens for unauthorized use of the data. As Dr. Helbing points up in his article, EU based companies who do not adequately administer the imposition of the Directive's data protection rules among processors and subprocessors are subject to administrative fines, in Germany up

to 300,000 Euros (about \$235,000 US).

The realities of SaaS, Cloud Computing and the ICT industry in general that the EC is now trying to grapple with—namely the complexity of business models and the global scope of business relationships—are the same realities James River Consulting addressed in a paper written in 2008 on disaggregated service levels in SaaS business models (See "SaaS Disaggregation (SaaS) at the Enterprise Level: An Analysis of 7 Prominent SaaS Companies and How Contracts Can Solve the Problem," James River Consulting, v.1.1, December 21, 2009 (PDF) at <http://www.jamesriverllc.com/resources>). SaaS and cloud computing are almost never confined to one provider and contract performance is almost never confined to one legal jurisdiction (except for example, as Dr. Helbing pointed out to me in our correspondence, Microsoft's localized European data centers). Without alignment of contract terms among all solution providers, SLAs in the customer facing document have little to no value, leading many SaaS and Cloud vendors to disclaim service levels altogether.

The US, too, has implemented data security laws that have implications for ICT services contracts. Massachusetts statute 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth requires data controllers to put in place a comprehensive information security program (CISP). The Mass legislature, anticipating that third party service providers will also have access to data, made it part of the law that data owners and licensees (the equivalent of controllers in the EU) must exercise oversight over providers by "requiring such... providers by contract to also implement and maintain... [a CISP]." Because the definition of service provider parallels that of an owner/licensee, logically the required contract language must flow down to other providers at lower tiers.

Tim Cummins, president of the International Association for Contract and Commercial Management (IACCM), in his blog "Commitment Matters" (<http://>

*(Continued on other side)*



## About James River

James River Consulting specializes in the development, negotiation, and management of IT and business services contracts with emphasis on IT and business outsourcing and on software-as-a-service/cloud computing/managed services. James River's offerings range from short-term staffing of contracts personnel, to sales contract processes, to e-Contracts, to competitive bidding, to SaaS and BPO contracts negotiation and management. James River's president, Eric Esperne, has over 15 years experience as an in-house legal counsel and director of contracts for both large and small IT companies.

Copyright James River Consulting LLC

8 Goldenrod Drive, Medway, MA 02053 703.850.7061-Mobile  
[eesperne@jamesriverllc.com](mailto:eesperne@jamesriverllc.com) [jamesriverconsulting@comcast.net](http://jamesriverconsulting@comcast.net)

## Feature Article continued

tcummins.wordpress.com>) often points up the complexity and uncertainty created by the globalization of business, as well as the inevitable conflict it creates for contracts involving multiple legal jurisdictions. From his perspective, Tim has observed reaction to globalization by corporate legal and contracts departments in the form of master agreements and contractual language obligating providers to follow a corporate “code of conduct.”

Business contracts are evolving into tools for enforcing laws and rules, sometimes in places and over companies that otherwise would not be touched by them. Contracts have always been about winning the most advantageous business terms for one side or the other. Addressing compliance has been an afterthought, and is usually handled in a single clause requiring blanket adherence to all applicable laws. The networked and global nature of ICT services has accelerated the need for making compliance an integral component of corporate contracting. Now, the financial, legal, and reputational impact of contract

terms not incorporating compliance, sometimes both upstream and downstream, is also of significant importance to shareholder and equity owner value.

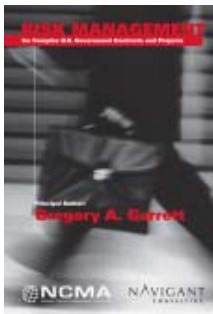
The question then becomes how to strategically, systematically and optimally implement compliance and risk management in contracts and contracting processes. Sometimes the answer is more explicit, as in the case of the EC’s standard data privacy clauses and rules for their application. But in most cases the answer is far from clear. Just as a CISP is needed for data security, a formal contracts compliance and risk management program (kCRM) is needed to meet the challenges of a complex, uncertain, and global business world. Is it enough to draft standard language and amend it to all contracts? Or is kCRM first and foremost a business development question to be taken up in the bidding and pre-negotiation phases of the sales cycle?

For more, contact Eric Esperne, President at 703-850-7061 or email him at [eesperne@jamesriverllc.com](mailto:eesperne@jamesriverllc.com).

## Company News

**Eric Esperne is Published in Two Groundbreaking Books on Contracts Management** Eric Esperne, JD, CPCM, President of James River, has authored chapters in two recently published books.

The first book, Risk Management for Complex US Government Contracts and Projects, is published by the National Contract Management Association (NCMA). The book serves as a course guide for dozens of National Education Seminars of the same title being presented to NCMA local chapters across the country (Eric gave the presentation to the Boston chapter in January, See Newsletter Q1 2010). Eric’s chapter is entitled “Chapter 7, Risk and Purpose Driven Outsourcing.” In the chapter, Eric presents a strategic, goal-based methodology for architecting outsourcing and services



contracts, and in particular contracts that will reduce transaction costs which can run high in large outsourcing deals.



The second book, Contract Administration: Tools, Techniques and Best Practices, is published by CCH Wolters Kluwer Law & Business. In “Chapter 13, The Future of Contract Administration: Purpose Driven Governance,” Eric lays out a decision workflow tool for affecting governance of outsourcing and services engagements that draws from both contractual and non-contractual methods. The book is sold through the Federal Contracts Training Center, founded by Gregg Garrett of Navigant Consulting.

Copies of the content in either chapter can be obtained by contacting Eric Esperne at [eesperne@jamesriverllc.com](mailto:eesperne@jamesriverllc.com).



# Newsletter

8 Goldenrod Drive, Medway, MA 02053