

Business & Technology Sourcing

REVIEW

- 3 Bringing the Promise of Innovation to Reality in Outsourcing Contracts
- 7 Transition Services Agreements in Acquisitions and Divestitures:
An Introduction
- 10 Securing Benefits and Mitigating Risk in Software Development
and Implementation Agreements
- 13 Tools for Better, Faster and More Effective Contracting
- 17 Clear Skies or Stormy Weather for Cloud Computing: Key Issues
in Contracting for Cloud Computing Services
- 21 Cloud Computing May Violate German Data Privacy Laws
- 24 New EU Standard Contractual Clauses for Commissioned
Data Processing
- 28 When Barking Dogs Bite in *BSkyB vs. EDS*

About Our Practice

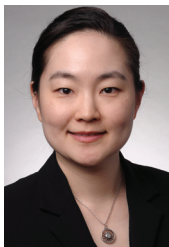
Mayer Brown's Business & Technology Sourcing (BTS) practice is one of the global industry leaders for Business Process and IT Outsourcing as ranked by Chambers & Partners, The Legal500 and the International Association of Outsourcing Professionals (IAOP). With more than 30 dedicated lawyers—many having previous experience with leading outsourcing providers and technology companies—the practice has advised on nearly 300 transactions worldwide with a total value of more than \$100 billion.



Kevin A. Rang
Chicago
+1 312 701 8798
krang@mayerbrown.com



Lindsay Blohm
Chicago
+1 312 701 7375
lblohm@mayerbrown.com



Jeanny Haw
Chicago
+1 312 701 8788
jhaw@mayerbrown.com



Lei Shen
Chicago
312 701 8852
lshen@mayerbrown.com

Editors' Note

Welcome to the Fall 2010 edition of the Mayer Brown *Business & Technology Sourcing Review*.

As we near the close of 2010, a year marked by a volatile global economy and changing political landscape, we take note of how these events are driving and shaping the sourcing and technology market. More than ever, companies are seeking to derive greater benefit from their outsourcing strategies, enabling them to operate more cost-effectively in today's global marketplace.

Our goal is to bring you smart, practical solutions to your complex sourcing matters in information technology and business processes. We monitor the sourcing and technology market on an ongoing basis and this review is our way of keeping you informed about trends that will affect your sourcing strategies today and tomorrow.

In this issue, we cover a range of topics, including:

- Key issues in cloud computing;
- Ideas of innovation and tools used for the contracting process; and
- Securing benefits and mitigating risk in software development and implementation agreements.

You can depend on Mayer Brown to address your sourcing matters with our global platform. We have served prominent clients in a range of sourcing, technology arrangements, e-commerce and transactions across multiple jurisdictions for over a decade.

We'd like to hear from you with suggestions for future articles and comments on our current compilation. If you would like to receive a printed version, please email us at marketing@mayerbrown.com. ♦

If you would like to contact any of the authors featured in this publication with questions or comments, we welcome your interest to reach out to them directly. If you are not currently on our mailing list, or would like a colleague to receive this publication, please email contact.edits@mayerbrown.com with full details.

Bringing the Promise of Innovation to Reality in Outsourcing Contracts

Paul J.N. Roy
Rohith P. George



Paul J.N. Roy
Chicago
+1 312 701 7370
proy@mayerbrown.com



Rohith George
Chicago
+1 312 701 8425
rgeorge@mayerbrown.com

Innovation is often considered the Holy Grail of outsourcing contracts. It is touted as one of the key benefits of engaging with providers who are expert in their fields and who have portfolios of customers from whom to draw inspiration. In reality, however, finding innovation beyond cost reduction has been elusive, and customers who expect it are frequently disappointed. Why has this been the case, and what can be done to bring the promise of innovation to reality? While we cannot provide definitive answers to those questions, we can offer insight based on observations of what some successful companies have done and offer alternatives for building innovation mechanisms into your contract.

Why Have Outsourcing Deals Failed to Produce Innovation?

Our research indicates that outsourcing contracts do not foster what customers call “innovation” because customers have not put a priority on innovation when they outsource. Instead, customers have focused almost entirely on immediate cost savings. Pricing, milestones and incentives are designed to reward the provider for “keeping the lights on,” but not for exploring new areas for efficiencies. Providers respond accordingly in their proposals, solutions, staffing and governance. The result is low cost solutions but also low levels of innovation.

Make Innovation an Essential Part of Outsourcing Deals

Reducing cost can justify outsourcing. However, many companies are losing the opportunity to get ideas and help that can improve their operations generally. Additionally, as companies outsource a greater portion of their internal operations, they increasingly lose the subject matter expertise that fuels internal innovation. Without the internal expertise needed to produce innovation, these companies must rely on their providers. There are instances where customers have brought some or all of an outsourced function back in-house precisely out of concern for innovation. As outsourcing grows to play a more prominent role in corporate strategy, so must innovation play a more prominent role in outsourcing contracts.

Outsourcing contracts do not foster what customers call “innovation” because customers have not put a priority on innovation when they outsource.

Where Has Innovation Worked?

We have seen cases where innovation by providers offers meaningful, lasting value to a customer. The innovation may be an improvement in the delivery of the provider’s services, but it may also be a change in the services that

allows the customer to improve other related functions that were retained by the customer. Or, the innovation may be entirely unrelated to the provider's day-to-day services.

From our experience, the most successful innovation arrangements contain clearly defined business objectives, a specific process for collaboration between customer and provider, and financial incentives that promote the development of innovation proposals and the implementation of resulting projects. These successful arrangements also include corresponding governance structures and management support.

Contract Structures for Innovation

There are several contract mechanisms that can be used individually or in combination to promote innovation in an outsourcing contract. These range from general commitments to specific undertakings with financial incentives.

COMMITMENTS TO TECHNOLOGY EVOLUTION

The most common innovation provision in outsourcing contracts is the general commitment to technology evolution. This requires the provider to keep its technology current with leading providers of similar services. In addition, the provider is obligated to conduct periodic briefings with the customer to discuss new technology opportunities that may apply to the provider's services and to develop proposals on specific technology when requested by the customer.

The difficulty in applying the technology evolution provision is determining when a new technology is a new service to be paid for by the customer, and when it has evolved into a standard that must be adopted by the provider without additional compensation. There is no clear demarcation, and there is plenty of room for differing opinions. There is also a risk that a provider will refrain from discussing potential innovations to avoid being compelled to provide them without additional charge. Consequently, this type of provision is more useful for protecting against stale provider assets than for ensuring innovation.

PROJECT PROPOSALS FOR SPECIFIC OBJECTIVES

A more precise approach to innovation is to obligate the provider to make project proposals to accomplish specific objectives (e.g., virtualization, user provisioning, green initiatives). Such a contract provision would also describe what the provider's proposals must include, such as a detailed project proposal and a financial benefit analysis. This approach is more likely to promote innovation because it provides specific targets for the provider's efforts.

The most successful innovation arrangements contain clearly defined business objectives, a specific process for collaboration between customer and provider, and financial incentives that promote the development of innovation proposals and the implementation of resulting projects.

One disadvantage to this approach is that it limits the objectives to those that can be identified at the time of contracting. In addition, this approach yields only project proposals, leaving the funding and valuation of the proposals to be determined. Therefore, while the project proposals can offer real value, the likelihood of value creation can be enhanced if proposals are combined with commitments for funding and cost savings.

SHARING OF PROVIDER'S INNOVATIVE TOOLS

As experts in their fields, providers use innovation to build tools and processes that help them perform their functions more effectively and efficiently. One relatively simple approach to innovation is for the provider to share some of these tools when the customer would benefit from their use. The kinds of tools that fall into this category include productivity, analysis and training tools. The provider would train the customer on the use of the tools and provide change management assistance to implement them.

One caveat to this sharing arrangement is that providers understandably will be concerned about protecting their most valuable tools. The customer

has a countervailing interest in maintaining a uniform environment for itself and its other third-party consultants and contractors. The contract protections would have to balance these two conflicting interests.

INNOVATION FUNDING

One way to ensure investment in innovation initiatives is to fund those initiatives. The outsourcing contract would specify a dollar amount that the provider will make available to fund innovation work. Some or all of this amount will naturally be factored into the provider's charges and will be passed on as charges to the customer. Thus, the customer must value the innovation benefit before adding this type of provision.

The provider, however, will probably not increase the customer's charges on a dollar-for-dollar basis, since part of this cost would displace marketing costs that the provider would otherwise incur. In addition, the provider would likely bank on some added revenues from the resulting projects.

One contract approach is to include a commitment by the provider to achieve defined levels of cost savings or added revenue.

A contract funding provision, then, would typically identify what can be funded and would specify the governance process for making such decisions. Potential innovation initiatives can range from workshops and technology reviews to spur creative ideas to consulting services designed to implement those ideas.

COMMITMENT TO COST SAVINGS OR REVENUE GENERATION

Process and funding do not, in themselves, ensure outcome. Hence, one additional contract approach is to include a commitment by the provider to achieve defined levels of cost savings or added revenue.

A few obvious complications arise: How can providers ensure an outcome such as net cost savings when they do not control what opportunities the customer will fund and implement? One way to address this gap is to credit the provider with net savings for a project, if warranted, even if the customer elects not to implement the provider's idea.

This approach is feasible for projects that yield hard cost savings, but it can be difficult, if not impossible, to assess the projected revenue or soft cost impact of innovations without empirical evidence. In either case, we recommend that the parties agree in advance on accounting rules and procedures to measure the cost or revenue impacts of projects.

Finally, in order for a commitment to cost savings or revenue generation to be meaningful, it must be attached to a financial consequence if the provider fails to achieve it. Such a consequence might take the form of a credit for some or all of the shortfall.

GAIN-SHARING

An additional incentive to promote innovation is gain-sharing. Gain-sharing provisions have been a staple in outsourcing agreements, but they typically have little effect because they usually are not accompanied by any specific commitment or process. These provisions have relied instead on the parties' future agreement on subject matter and scope. This caution in the use of gain-sharing is perhaps driven by cases where commitments to gain-sharing have resulted in a windfall for the provider when the provider shared in cost reductions that resulted solely from market shifts in commodity prices (e.g., reductions in telecom rates).

The final ingredient for innovation is the allocation of intellectual property rights.

More advanced gain-sharing commitments have been structured in ways that produce substantial benefits. One approach is to combine gain-sharing with the structured process described above for valuing cost savings and added revenue. The result would be a provider commitment to first generate a minimum savings without gain-sharing, then to share in savings when they exceed a higher threshold. Another approach is to define a precise scope for gain-sharing. For example, a provider might have the right to share in gains from re-negotiating certain third-party contracts or from modifying specific processes or technologies.

ALLOCATION OF INTELLECTUAL PROPERTY RIGHTS IN INNOVATIONS

The final ingredient for innovation is the allocation of intellectual property rights. If either party is concerned that its assets or competitive position will be compromised or forfeited by the collaboration, they will not volunteer their most valuable ideas or intellectual property, and the creative process will suffer. Conversely, a party that believes it could gain rights to valuable innovations will put more effort into creating those innovations.

Finding the right balance is difficult. The rules can be complex and can vary depending on the parties' business models and industries and their relative contribution to any particular development. We know from experience that this issue can be successfully tackled, but it must be addressed at the start and not as an afterthought.

Governance Structures for Innovative Outsourcing

Innovation is not something that the provider delivers. Rather, it is the result of a multi-disciplinary

creative and collaborative process that requires active participation by both provider and customer. The benefits of this process may cross organizational boundaries and may extend beyond the outsourced function. It is inherently unpredictable, and for every success there will be failures. Management needs to be prepared for this, and the governance process must be designed to support it with practices consistent with those used to foster innovation internally.

Conclusions

Innovation is an essential ingredient for corporate survival and growth. As companies expand their reliance on outsourcing, they also must integrate innovation as a critical component of their outsourcing relationships. Providers' success will also depend on their ability to be a source of innovation for their clients, as only those relationships that include innovation will survive in the long term. When combined with management support, the right contract provisions can provide the structure, process and commitment needed to bring the promise of innovation to reality. ♦

Transition Services Agreements in Acquisitions and Divestitures: An Introduction

Paul A. Chandler
Lindsay Blohm



Paul A. Chandler
Chicago
+1 312 701 8499
pchandler@mayerbrown.com



Lindsay Blohm
Chicago
+1 312 701 7375
lblohm@mayerbrown.com

When a company decides to pursue an acquisition or divestiture, there are many issues to consider. Far too often, the parties neglect considering, until late in the process, whether any post-closing services need to be provided under a transition services agreement (TSA). This article discusses the general context in which TSAs are required and provides tips for starting to gather and analyze TSA requirements to avoid unnecessary deal costs, delays and inefficiencies.

When is a TSA Required?

Because of the time and resources often required to complete a TSA, the parties should determine early on whether a TSA is warranted. Not every deal requires a TSA: the determination revolves around the interconnectedness of the seller and the target business, as well as the particular capabilities of each party. For instance, will the divestiture result in the buyer acquiring all assets (systems, service agreements, licenses, etc.) needed to run the target business (i.e., the “clean-break” scenario)? If so, is the buyer confident that it will be able to run the divested business without any help from the seller? Likewise, will the seller be able to run its retained business without assets or help from the divested business? If the answer to these questions is “yes,” then a TSA may not be needed. However, if either party will need assets or assis-

tance from the other party after closing, a TSA will be required.

TSAs vary widely in duration, based on the requirements of the particular deal. If the target business is largely autonomous, a TSA lasting several months may be adequate to deal with knowledge transfer and system migration issues. Conversely, in complex situations, where the target business relies on systems shared with the seller’s retained business, or where the buyer itself is unable to provide the required services, a multi-year TSA may be required. Multi-year TSAs give the buyer more time to de-couple from the seller and acquire its own capabilities for running the target business.

Not every deal requires a TSA: the determination revolves around the interconnectedness of the seller and the target business, as well as the particular capabilities of each party.

While TSAs often cover the provision of services from seller to buyer (known as a “forward TSA”), this is not always the case. In a “reverse TSA” situation, the flow of services is from the buyer (or target business) to the seller. Reverse TSAs are often required where critical assets or resources are to be transferred along with the target business, such as a data center used by the seller’s retained

business, or technical personnel used to support applications or systems used by both the target business and the seller's retained business. The issues of concern to the seller (as a service recipient) under the reverse TSA are generally analogous to those of concern to the buyer under a forward TSA.

TSA issues should be contemplated while the structure of the transaction is still in flux and before the buyer has been identified. For this reason, the seller's initial preparation is likely to be refined as the deal progresses. Nevertheless, there can be significant value in careful planning early in the deal process, in part because this enables the seller to present a workable deal package to the buyer, including information that the buyer will need to quickly assess any overlaps or gaps in assets and capabilities for running the target business.

TSAs Compared to Outsourcing Agreements

Both TSAs and outsourcing agreements commonly involve one party providing the other with services that may be critical to the operation of the service recipient's business. However, a key difference in TSAs is that the seller (as the service provider) is generally not in the business of providing those services. Moreover, the seller's information technology (IT) organization may lack the discipline and the industry standard processes of professional outsourcers. Likewise, the degree of service customization under a TSA is usually more limited than in an outsourcing agreement, particularly where the seller uses the same systems to service the buyer and the seller's retained business. For these reasons, the seller may only be willing to commit to provide the TSA services in the same manner that it provides similar services to itself.

A key difference in TSAs is that the seller (as the service provider) is generally not in the business of providing those services.

What Are the First Steps to Prepare for a TSA?

The seller and buyer should start gathering information relating to the TSA as early as possible in the deal process to help address potential issues before they

become major problems. Ideally, the seller and buyer would involve a wide variety of people with the relevant knowledge in early deal discussions. However, this is usually not practical because competing demands on resources and the need for confidentiality limits the number of people who can be involved. This complicates and delays the task of gathering information and developing solutions. The objective should be to strike a balance between limiting the "circle of knowledge" and involving the specialists needed to appropriately analyze requirements and resolve issues.

The objective should be to strike a balance between limiting the "circle of knowledge" and involving the specialists needed to appropriately analyze requirements and resolve issues.

THE FOLLOWING IS A LIST OF CONSIDERATIONS FOR INFORMATION GATHERING:

Systems and Services. The seller must identify the systems and services that are currently used to conduct the target business, including those which are critical to the target business. Depending upon the nature of the transaction, potential items to consider include:

- Implemented systems (e.g., enterprise resource planning (ERP) and human resource systems, claims/payment processing systems, web sites/e-commerce infrastructure, production/manufacturing control, databases, interactive voice response (IVR)/telephony systems);
- Interfaces and systems for interactions with third parties (e.g., banks, regulators, data providers, suppliers, customers);
- IT facilities and resources (e.g., data centers, support/development centers, call centers, offsite data storage sites, disaster recovery/hotsite locations);
- Service agreements (e.g., outsourcing services, managed network, data center collocation, disaster recovery/business continuity, landline/mobile telecom and personal digital assistants (PDAs), support/maintenance arrangements); and
- License/support agreements (e.g., application, database and operating system software).

For each item identified, the seller should also consider key issues:

- What technology platforms are used;
- Whether the system or service was developed internally by the seller's organization;
- Whether the system or service is "dedicated" (i.e., used exclusively to support the target business) or "shared" (i.e., used to support both the target business and other parts of the seller organization);
- What support model is currently used for the target business (i.e., by the target business itself [internal], by the seller or an affiliate of the target business [centralized], or by a third party through an agreement between the provider and the target business or the seller or an affiliate of the target business [outsourcing]);
- Whether it is feasible to assign to the buyer any third-party agreements used to support the target business, and/or whether consents are required to provide services under the TSA (either temporarily or on a long-term basis) to the buyer; and
- Whether there are commingled data or records that will be impractical for the seller to segregate (e.g. email or historical or archived data).

In addition, the seller should determine whether any of these items will no longer be required after the deal closes, including the costs that may result from terminating any associated contracts. Though these requirements may be buyer-dependent, doing this analysis early often helps the seller develop a more accurate picture of IT-related transaction costs involved in the deal.

Major Projects. The seller should identify major projects that are in process, or scheduled to be performed, for the target business, as well as the preferred disposition of these projects in view of the proposed deal. Considerations here could include: (i) criticality and complexity; (ii) the entities involved in performance; (iii) the current status, including remaining work and completion time frame; (iv) current and planned future investments; (v) practicalities of completion prior to closing; and (vi) potential costs and other impacts of termination prior to closing.

Personnel. The seller should determine which personnel support the target business (and, if applicable, which target business personnel support other parts of the seller's organization), including the employing entity, work locations, locations supported by such personnel, whether such personnel are to be retained by the seller or transferred to the buyer and whether any such personnel are critical or "key" personnel to the operation of any business.

The buyer should consider how the systems and services of the target business and the seller interconnect with its own technology sourcing model.

Evaluation of Buyer Requirements. The buyer's key task at the beginning of the transaction is to evaluate the seller's responses to the inquiries described above (through initial meetings with the seller and due diligence questionnaires), so the buyer has a better sense of the systems and services used to run the target business. The buyer should use this information to identify any potential overlaps and gaps in its own capabilities and systems. In the event of overlaps, the buyer should identify which overlapping item should be retained after closing. In the event of gaps, the buyer should identify how the inadequate or lacking systems or services will be addressed, such as through the buyer's current systems and services, TSA services or newly procured systems or services. In addition, the buyer should consider how the systems and services of the target business and the seller interconnect with its own technology sourcing model. Incompatibilities with the buyer's current systems should be identified and analyzed early in the process to identify alternative arrangements. The buyer should also assess sourcing options for the target business when the TSA ends.

Conclusion

The issues described in this article are seldom focused on early in the process of divesting or acquiring a company. When they are left to the end of the deal process, unnecessary delays and costs may result. Proactively addressing these issues up front, as outlined above, can help avoid these problems. ♦

Securing Benefits and Mitigating Risk in Software Development and Implementation Agreements

Brad L. Peterson
Gregory A. Manter



Brad Peterson
Chicago
+1 312 701 8568
bpeterson@mayerbrown.com



Gregory A. Manter
Chicago
+1 312 701 8648
gmanter@mayerbrown.com

If you are contracting to have software developed or implemented, you likely are uncertain both about how you want the software to function and the work required to get it to function that way. That uncertainty can translate to scheduling and budgetary risks. However, those risks can be mitigated with the right deal structure (or heightened with the wrong deal structure) in your contract with the developer, systems integrator or other contractor. The available deal structures fall into the following three high-level categories:

- Assist
- Deliver
- Shared Risk

This article describes those three deal structures and the key contract provisions that help make each of them effective in securing benefits and mitigating risks.

Assist

Under the “assist” structure, the contractor works at your direction to assist you in completing the project. You pay the contractor on a time-and-materials basis. This structure is well-understood and offers the benefits of allowing you to start a project quickly, with only a limited view of the desired outcome, and make changes in scope and direction at your discretion.

With the assist structure, the risk of budget overruns and schedule delays is entirely yours. The assist structure’s time-and-materials pricing approach increases that risk by giving the contractor an incentive to provide an optimistic initial estimate (to win the business) and to expand the project (to increase its revenues). A well-crafted contract can mitigate that risk by allowing you to control scope, schedule and staffing. For example, it can give you the right to:

- Suspend or delay work or change the scope of services at your discretion
- Require the contractor to complete the project at committed hourly or daily rates
- Decide on the mix of on shore and off shore personnel
- Require the contractors to retain key individuals on your project for the duration of your project and limit turnover of non-key resources
- Receive reports and briefings, and inspect the ongoing work, as required to manage the project

To make the assist structure effective, you will need the knowledge and skill required to exercise this control and flexibility. Thus, the assist structure works best on projects where you know how to run the project and merely need to augment your staff. If you are relying on the contractor’s expertise in running the project and making key decisions, this structure provides little certainty on schedule or price.

Deliver

The “deliver” structure is the most direct way for a customer to seek certainty on schedule and price. Under this structure, you agree to pay the contractor a fixed fee for defined end results. Payments are made only upon achieving milestones (such as acceptance of deliverables). Making the contractor’s ability to charge for services depend on timely completion shifts the schedule and cost risks to the contractor. Because additional effort can reduce the contractor’s profits, the contractor has a strong incentive to complete your project quickly and efficiently.

Making the contractor’s ability to charge for services depend on timely completion shifts the schedule and cost risks to the contractor.

The primary risk in the deliver structure is that you will end up signing change orders that increase the fixed fee and extend the schedule because you failed to clearly and completely define your desired end results or because your desired end results changed mid-project. There is a further risk that the contractor will charge high prices for changes because you have few options but to enter into the change order. These two risks are heightened by the fact that the contractor has a financial incentive to under-scope the project initially (to win the business) and then to sell increases in required scope. Finally, there is a risk that the project will not meet your needs, even if delivered on time to specifications, because the specifications were inadequate.

In order to secure the benefits and mitigate the risks of the deliver structure, you will need to describe in detail the services to be performed, the deliverables and milestones that will result from the services, and the time frame in which those deliverables and milestones must be delivered or achieved. You will need clearly defined acceptance procedures with a right to accept or reject deliverables and milestones, either in your reasonable discretion or in accordance with acceptance criteria that will not be met unless your needs are met. Without these provisions, there is considerable risk of dispute over whether the contractor has achieved the milestones and thus earned payment.

You will also need specified change-control procedure, where changes to the scope or timeline are reported, with a threshold at which such changes will affect the schedule or the fixed fee. To the extent that your fixed fee is subject to change due to a scope change, those fee changes should be anchored in your contract by a committed rate card to be used either to track and pay for actual work associated with such change or to estimate work associated with such change to create an updated fixed fee.

These key contract provisions need to be clear and practical enough to be used for day-to-day management of the project. They also need to be drafted well enough to stand up in court, or in a less formal dispute resolution process. Otherwise, you will have agreed to pay a fixed price without obtaining the end results you need. However, drafting and negotiating these contract provisions require an investment in investigating your desired end results and negotiating and carefully drafting the contract provisions.

The primary drawback of the deliver structure is that the contractor will charge a risk premium. This premium covers the risk that the contractor underestimated the work. However, the risk premium also covers the risk that the customer will not do what the customer needs to do to make the implementation succeed, perhaps because the customer sees the schedule and cost risk as having been transferred to the contractor. Thus, you are to some degree insuring the project against the risk of cost overruns.

The primary drawback of the deliver structure is that the contractor will charge a risk premium.

Shared Risk

The “shared-risk” structure is designed to reduce overall risk by aligning incentives. For example, a shared-risk structure might include:

- A target budget for a well-defined process and result (with clear customer responsibilities)
- Clear allocation of control over scope, staffing and other key cost drivers
- A right to charge for hours spent up to the target budget at defined hourly rates

- A sharing of the “savings” if the project is completed under budget
- Bonuses for early delivery (if that provides business value) and credits for late delivery
- Hourly rates reduced in stages over the target price, perhaps even to zero at a “not to exceed” price
- Clear boundaries on chargeable and non-chargeable changes

The shared-risk structure reduces overall risk and creates a spirit of partnership by giving each party a clear financial incentive to complete the project on time and under budget. However, like the deliver structure, the shared-risk structure requires an up-front investment in defining the process and the outcome. In addition, the shared-risk structure will require more sophisticated contracting to address changes in scope and direction because those have greater implications with this more complex structure.

This structure requires the contractual elements from both the assist and the deliver structures. As with the assist structure, you are concerned about staffing because you share in the cost of turnover and excess staffing. As with the deliver structure, you will need a clear definition of the end result and an effective change control mechanism. Because it requires both ongoing governance similar to the assist structure and the up-front investment similar to the deliver structure, the shared-risk structure is best used for projects of particular importance.

The Right Structure for Your Software Project

The right structure for your project depends on your situation. In the right situation, each of these structures can secure benefits and mitigate risks.

Additionally, you can combine these three structures by phase. For example, you could use a shared-risk

structure, but hold back some payments for achieving milestones; or you could use the assist structure for the initial scoping phase (to get a quick start), the deliver structure for the design phase (because it's entirely within the contractor's control) and the shared-risk structure for the implementation and testing phases (to reduce risk). However, combining contract provisions from one structure with pricing from another structure can increase risk. For example, an assist structure without adequate control provisions in the contract would increase the risk of cost and schedule overruns.

The shared-risk structure reduces overall risk and creates a spirit of partnership by giving each party a clear financial incentive to complete the project on time and under budget.

Regardless of the structure you select, your contract should include standard services agreement provisions such as performance and conformity warranties, infringement indemnities, limitations on liability (including exceptions to those limitations) as well as provisions to protect the confidentiality of the project and your business data and the privacy and security of any personal data that may be accessed by the contractor.

Each of these structures has been used successfully when paired with contract provisions to secure the benefits of the selected structure. The best choice depends on your project, your skills, your risks and your contractor. Success comes from investing at the start in contracting for a value-maximizing deal structure. ♦

Tools for Better, Faster and More Effective Contracting

Paul J.N. Roy
Brad L. Peterson
Kavi C. Grace



Paul J.N. Roy
Chicago
+1 312 701 7370
proy@mayerbrown.com



Brad L. Peterson
Chicago
+1 312 701 8568
bpeterson@mayerbrown.com



Kavi C. Grace
Chicago
+1 312 701 8218
kgrace@mayerbrown.com

Large-scale outsourcing is inherently complex. So is the process of securing commitments in a large-scale outsourcing contract. By helping to manage this complexity, contracting tools can allow deal teams to build better contracts faster and at less cost.

This article describes tools that we have found to be particularly valuable when helping customers enter into large-scale outsourcing contracts. These and similar tools can make customers more effective and efficient in any sourcing process.

Identifying Deal Terms

Reaching early internal alignment on the business objectives helps the customer's deal team to focus its energy on the most valuable parts of the deal and ask for the right deal terms in its initial draft. The challenge in achieving alignment is that outsourcing often involves a large number of issues and stakeholders. We have found two tools particularly effective.

PRELIMINARY QUESTIONNAIRE

The first tool for identifying deal terms is a preliminary questionnaire to be completed by the members of the deal team. This questionnaire contains a detailed set of questions that are designed to reveal important deal terms, including both factual detail and the customer's primary objectives. Using a questionnaire to gather this

information allows recipients to take the time required to investigate the answers. This can provide more complete and accurate information. Also, later in the deal, the deal team will be able to go back to the responses to know who said what in case of any confusion.

The challenge in achieving alignment is that outsourcing often involves a large number of issues and stakeholders.

In sending out a questionnaire, there is a risk that the people who fill it out may not understand or answer the questions fully. As we are seeking to be faster without cutting quality, one of the key goals is to make sure the correct information is obtained. There are several ways to mitigate this risk. One is to be judicious about selecting people to fill out the questionnaire. Another is to tailor the questionnaire to the recipients and to ask about the underlying business interests instead of particular terms. A third is to include explanatory commentary.

INTERVIEW CHECKLIST

The second tool for identifying deal terms is an interview checklist. The benefit of an interview is that it allows both the questions and the answers to be refined and expanded during a detailed discussion. Ideas that might

merely be implemented if included in a response to a questionnaire can be examined and tested. In some cases, an interview provides the information required to follow up with a detailed questionnaire.

The interview checklist is a tool to avoid missing points in the interview. An interview checklist allows the lawyer to quickly identify the points raised in similar interviews, and also allows a team of interviewers to ask consistent questions. We recommend developing a comprehensive list of questions that can then be selected and tailored for the particular deal. We prefer to create the interview checklist for a specific deal from an over-inclusive comprehensive checklist.

Creating Initial Documents

Large-scale outsourcing contracts tend to include dozens of documents. Some of these documents contain specific legal terms and conditions while others have lists, diagrams or other data. Breaking a contract into many separate documents is efficient because it allows individual review teams to work on the separate documents in parallel. Also, different documents are best described with different software products (e.g., pricing in a spreadsheet application and terms in a word processing application). At signing, however, all of these documents need to fit together. We have found two tools particularly helpful in making the end-to-end process of creating a clear, consistent and comprehensive contract faster and less costly.

Breaking a contract into many separate documents is efficient because it allows individual review teams to work on the separate documents in parallel.

TEMPLATES

The most valuable accelerator is a well-designed, carefully reviewed suite of contract templates aligned with the initial questionnaire and interview checklist. Contract templates serve as a repository for best practices and help to build quality into the documents at the start (avoiding the need for corrections at the end). A good contract template quickly guides the team to decision points and is easy to adapt to the

deal. A collection of templates for the contract schedules speeds the gathering information required in a final contract, avoiding rework and delay close to signing. Strong initial drafts also help clients capture value in negotiations by winning the points that do not get negotiated because they are overlooked or seem too small to raise.

Strong initial drafts also help our clients capture value in negotiations by winning the points that do not get negotiated because they are overlooked or seem too small to raise.

Of course, templates can only take the deal team so far. They do not include the deal-specific facts. There is a risk that people will have difficulty knowing what to modify, or that they will assume that the templates represent the right answers instead of a starting point for review. Thus, the deal team also needs background, context and guidance on how to bring the templates in line with the facts of an individual deal.

GUIDE FOR DOCUMENT PREPARATION

A “guide for document preparation” is a tool to help the deal team through the document preparation process. The guide typically covers what data are needed for the contract, the organizational structure of the data and how to present the data in a contract document that is clear, complete and consistent with the remainder of the contract terms. Such a guide can prove invaluable in assisting the teams to quickly bring the pieces of the deal together, particularly when there are multiple deal teams working in parallel.

Negotiating the Contract

Once the contract documents have been distributed and the bidders have responded, the deal team will need to know, on an ongoing basis, about the progress on the deal, time to completion and outstanding issues. The following tools enable the deal team to answer these and other important questions and to respond effectively to management inquiries.

PROJECT PLAN

The contract negotiation is a project. We find that deal teams are more successful if they start with a thorough project plan that takes into consideration any dependencies on non-contract activities (e.g., due diligence, technical reviews, risk reviews, etc.). The form of the project plan can be as simple or as detailed as the customer feels necessary, depending on the circumstances. There is particular benefit in allowing people to schedule their time to turn documents, gather facts, obtain approvals and participate in negotiation sessions.

DOCUMENT TRACKER

The core of project management is deciding who will do what next and then following up to see what has been done. In large-scale outsourcing deals, teams are generally responsible for specific documents. As a result, we recommend the use of a “document tracker” that shows who is responsible for the next step(s) on each document. A good document tracker will provide each team with a centralized, regularly updated overview of progress on a document-by-document basis and will help each team member know what to do next.

The core of project management is deciding who will do what next and then following up to see what has been done.

ISSUES TRACKER

Although the document tracker will tell you the status of each *document*, it will not tell you which *issues* remain. As a result, we often use an “issues tracker,” which is an organized description of open issues. The best issues trackers express each issue neutrally enough so that the tracker can be shared collaboratively between the customer and supplier teams and can thus be used as a focal point for discussions.

Caution and discretion should be used when framing concepts in an issues tracker because a poorly framed issue might result in making a decision on the wrong question or the wrong facts. Ideally, the issues tracker will focus attention on the most important issues and will speed resolution of escalated issues.

RISK REGISTER

The issues tracker can tell you what issues are open, but it only addresses risks that are being allocated to each party in the contract. A “risk register,” on the other hand, is an internal tool of the customer’s that helps the core deal team assess how the deal team is mitigating risk and thus increasing value.

For each risk that the customer’s team identifies, there are generally four options available: (i) change the deal to eliminate the risk (for example, by removing a risky service from the scope); (ii) place the risk on the supplier through risk allocation clauses; (iii) retain the risk to be managed through governance; or (iv) place a value on the risk and factor it into the deal’s financial model. Any risk that is mitigated is reflected in the risk register to show how it was addressed and to detail the positive impact of its mitigation on the overall risk profile of the deal. This tool is of increasing interest as companies focus on risk in outsourcing in addition to the potential rewards when looking at value.

COLLABORATION TOOLS

The final category of tools for negotiation is collaboration tools. There have been tremendous improvements recently in this area. Data rooms can allow deal teams to share documents. Webex and other web meeting tools can allow a virtual meeting where everyone is on the same page because they are looking at the same words on the screen. Document repositories can provide robust version control and document integrity functions; and word processing software, such as Microsoft Word, offers change tracking and document comparison tools that allow people to present changes in a way that is easy to find and verify.

We have found that effective use of these tools requires the development of standards, procedures and process rules for recording and preserving issues and maintaining document integrity and version control. Experience shows us, too, that different tools work well with different corporate cultures.

Deciding Whether to Sign

In deciding whether to sign a sourcing contract, the customer must consider whether the value of the contract is greater than the value of alternatives that the contract precludes. Financial modeling indicates

value, but risk must also be considered. For the customer, the choice might be between two bidders, between a bidder and internal processing, or both.

The best tool here depends on the customer's decision-making process. For example, a customer approaching a difficult down-select in a competitive outsourcing process might use a side-by-side chart of key issues organized by bidder. A comparison chart could be built based on the issues tracker and risk register described above. This approach works particularly well when there are only a few issues separating the bidders.

Effective governance is critical to the success of an outsourcing relationship, and effective transition from the deal team is essential to the success of the governance team.

If there are a large number of issues separating the bidders' proposals, the customer might use a scoring matrix that combines a simple 1-2-3 score with a customer-reviewed weighting for each issue to produce a composite score. This tool can sometimes provide surprising results. In some cases, the final score will show there are no significant differences among bidders, even though the responses look very different on their face. In other instances, the tool can show there is a material difference. In any event, the scoring matrix tool can synthesize a large number of differences.

A customer choosing between internal processing and outsourcing might use similar tools. This can also produce surprises. A deal team that has focused on the risks in an outsourcing contract may be surprised to find that many of the same risks are present—and perhaps to a greater degree—with internal processing.

Another useful tool is a scorecard that evaluates risk in a more nuanced way than the 1-2-3 scoring matrix. For example, a scorecard might describe the outcome of negotiations on the incentives, commitments and options in the contract and place a value on each. A scorecard is particularly useful when working with a series of similar deals because it allows comparisons

across time and across deals. Ideally, the scorecard will produce an adjustment to the financial model.

Facilitating an Effective Transition

The final leg of the contracting process is the transition to the governance team. Effective governance is critical to the success of an outsourcing relationship, and effective transition from the deal team is essential to the success of the governance team. We believe the best practice is to have some overlap between the deal and governance teams, but our experience and research shows that this overlap is generally limited.

We have identified three tools as particularly useful in transferring knowledge about the contract from the deal team to the governance team. The first is a milestone list that includes all date-dependent activities and deliverables shown in any part of the contract. The second is a detailed or a high-level contract summary identifying key areas of the contract on which the governance team should focus in its day-to-day management of the relationship. The third is governance training that allows for interactions between the teams to ensure that the governance team can ask questions when information or contract provisions are unclear.

Tools are aids to successful contracting, not substitutes for experience and judgment, and they must be used with care to avoid creating misimpressions.

Summary

The specific contracting situation drives not only overall strategy, but also choice of tools. Tools are aids to successful contracting, not substitutes for experience and judgment, and they must be used with care to avoid creating misimpressions. However, we have found that tools can assist deal teams to maximize value and avoid pitfalls by helping to manage the inherent complexity of outsourcing and by increasing the speed, efficiency and effectiveness of the outsourcing contracting process. ♦

Clear Skies or Stormy Weather for Cloud Computing: Key Issues in Contracting for Cloud Computing Services

Rebecca S. Eisner
Daniel A. Masur



Rebecca S. Eisner
Chicago
+1 312 701 8577
reisner@mayerbrown.com



Daniel A. Masur
Washington DC
+1 202 263 3226
dmasur@mayerbrown.com

Cloud computing has been with us for years through technology outsourcing, online service models and application service providers. But an entirely new crop of providers and service offerings has changed the way customers are contracting for cloud computing services. This article addresses cloud computing benefits, risks and regulatory challenges, with suggestions for overcoming or mitigating those challenges.

What is Cloud Computing?

While there is no universally accepted definition of cloud computing, most agree that there are three service models, each with its own distinct features: software as a service (SaaS); platform as a service (PaaS); and infrastructure as a service (IaaS). There are also different delivery methods: a “private cloud,” where the resources used to provide the services are dedicated to one specific customer; a “public cloud,” where the resources are shared generally with the provider’s other customers; and a “hybrid cloud,” where multiple clouds (of the same or different types) are interconnected—for example, the majority of an entity’s processing may be performed in a private cloud but it may access data shared on an application in a public cloud.

While the definition of cloud computing may vary, there is agreement on its benefits. There are technical

advantages: the user gets on-demand computing services; computing resources such as storage, processing, memory, network and bandwidth are pooled across multiple users; and fluctuations in demand are more easily met. There are also time- and money-saving advantages, as customers do not have to invest in the hardware, software and network infrastructure needed to provide the same service. Cloud computing also increases the opportunity for collaboration and knowledge-sharing, as all files are available to designated users in a consistent format. Also, cloud computing services are available over a network, so they can be accessed from many locations.

While the definition of cloud computing may vary, there is agreement on its benefits.

The Current State of Cloud Computing Contracting

Currently, the standard contracts offered by cloud computing providers are one-sided and service provider-friendly, with little opportunity to change terms. Few offer meaningful service levels or assume any responsibility for legal compliance, security or data protection. Many permit suspension of service or unilateral termination, and disclaim

all or most of the provider's potential liability. In addition, some cloud computing providers emphasize low-cost offerings, which leave little room for robust contractual commitments or customer requirements.

When contracting for these services, it is critical for a business to analyze its data, applications and business needs. Routine, non-sensitive data may allow use of a standardized, low-cost cloud computing service with few contractual protections. However, mission-critical data and applications require more robust service and contractual protections, which may increase the price of the service.

In those situations where standardized services and terms are not appropriate, where can business lawyers look for appropriate contractual protections? While there is no single form agreement that properly addresses all contractual needs, there are some good starting points. Traditional outsourcing and software licensing terms may be useful in creating an appropriate set of contractual clauses. These terms will need to address the regulatory and compliance challenges discussed below.

Routine, non-sensitive data may allow use of a standardized, low-cost cloud computing service with few contractual protections. However, mission-critical data and applications require more robust service and contractual protections, which may increase the price of the service.

Potential Operating Risks of Cloud Computing

On the operational side, cloud computing relies heavily on network connectivity. If network connections are down or slowed, the resources and data in the cloud can become unavailable. This risk is heightened with public and hybrid clouds where resources are not dedicated but shared. Depending on the nature of the cloud, resources that are supposedly abundant may in fact be heavily used and, therefore, less available. Another operational risk exists because of the lack of standards in cloud computing: there may be compatibility issues between the cloud and data and resources in a different cloud, or elsewhere in the customer's enterprise.

As with traditional outsourcing, a number of risks center on the fact that the business is giving up control. This lack of control can undermine many of the benefits sought from cloud computing as well as pose other risks to the business. The customer may need a change in the service to accommodate a new customer regulatory requirement. The cloud provider may not be willing to make the change if it costs money or changes a standard service. Gaining control of these issues in the contract with a cloud provider can increase the cost of the solution, and may reduce some of the cost benefits of using a cloud computing solution.

lack of control can undermine many of the benefits sought from cloud computing as well as pose other risks to the business.

Regulatory and Compliance Challenges

There are a number of regulatory challenges for cloud computing users and providers. This article gives a few examples, but does not address every regulatory concern. For example, businesses involved in government contracting often have obligations to classify and protect data. Restrictions on data disclosure and access, even on the location of data storage, will have to be considered in the context of any cloud computing solution.

The free movement of data among networks, data centers and storage devices may raise issues under a country's import/export control regulations. For example, a company using cloud computing services may not be aware that its export-controlled software is being exported through its use of the distributed cloud computing system.

Data retention and disposal requirements can also be challenging. For example, in the United States, when litigation is pending, threatened or anticipated, a party must preserve potentially responsive data in the form in which it was created by the company. Such data may have to be made available to the opposing party or the court as required by electronic discovery rules. It could be challenging to isolate and provide data in the cloud given the distributed and disbursed nature of cloud computing.

Privacy and Security Issues: The Largest of the Regulatory Challenges

Regulated personal information presents one of the largest challenges for cloud computing users and providers. Numerous industry sector specific privacy laws exist that must be addressed in cloud computing contracts. These include, for example, the Gramm-Leach-Bliley Act (“GLB”) for private financial information, and the Health Insurance Portability and Accountability Act and implementing regulations (collectively, “HIPAA”) for health and medical information. The Federal Trade Commission (“FTC”) has devoted significant attention to privacy issues, and security and prevention of identity theft have become a particular focus. Individual states have also taken notice of privacy and security issues, and have begun enforcement of such issues.

Regulated personal information presents one of the largest challenges for cloud computing users and providers.

Many US states have statutes and regulations that mirror the requirements of GLB and protect personal health information like HIPAA. Additionally, many states have passed data breach notification laws. As of April 2009, the majority of states, the District of Columbia, Puerto Rico and the Virgin Islands had enacted some form of database breach notification act protecting personal information. Additional state laws are presenting issues for cloud computing regulatory compliance as well. In 2008, Massachusetts issued comprehensive regulations requiring that personal information be encrypted when transmitted wirelessly or over a public network. The regulations also require a “written, comprehensive information security program.” The security program must be reasonably consistent with industry standards and contain administrative, technical and physical safeguards to ensure the security and confidentiality of records containing personal information.

Finally, there are industry specific standards that many businesses must follow, such as the Payment Card Industry (PCI) Security Standards. Companies that put cardholder data in the cloud will have to ensure that cloud providers also comply with PCI standards.

Europe and other parts of the world have stringent privacy regulations that in many cases have been in place much longer than those in the U.S. In many countries, personal data cannot be processed without the consent of the data subject. Additional requirements include limiting the use of the data to the reason for which it was collected (and the consent granted), allowing the data subject access to his or her personal data and allowing the data subject to correct personal data. In addition, some countries regulate the transfer of personal data (e.g., the European Union Directive 95/46/EC, as implemented through Member State legislation, relating to collection, use, processing and free movement of personal data). Failure to comply can lead to fines, penalties, interruption of business and, in some cases, imprisonment.

Regulatory and Compliance Issues With Cloud Computing: Managing the Risk Through Contracting

To manage privacy risks with service providers, a company must have regulatory, security and privacy processes in place with specific requirements pertaining to service providers. At a high level, these steps include: appropriate service provider diligence and selection; implementing regulatory, security standards and privacy requirements through appropriate operational requirements and contractual clauses; and monitoring performance and adherence to the standards and process.

Businesses that use cloud computing solutions where personal information will be collected, processed, accessed, stored or transferred must perform due diligence on the service provider at the contracting stage, as well as continue meaningful oversight during the term of the contract.

To manage privacy risks with service providers, a company must have regulatory, security and privacy processes in place with specific requirements pertaining to service providers.

And, while you cannot outsource responsibility for your compliance obligations, you should ensure that you and your provider understand the following topics (and have documented such understanding in the contract):

- The specific regulatory requirements to be performed by your service provider (with respect to privacy, for example, including how the service provider may and may not use personal information, confidentiality terms, how the provider should dispose of personal information, where data may be processed, stored and transferred, etc.);
- Your compliance and security requirements and the service provider's security practices to monitor and prevent compliance and security breaches and to protect your business;
- The process for reviewing any process or system changes that may impact compliance, security or privacy issues;
- Your reporting requirements for regulatory compliance;
- Your audit requirements;
- Your rights to approve any subcontracting by your primary service provider and requirements that subcontractors of all tiers agree to the same compliance terms;
- What you will do if your service provider suffers a security/privacy breach or lapse in compliance, including business continuity and disaster recovery plans;
- Responsibility for monitoring changes in applicable laws and regulations, and adjusting service requirements to meet such changes;
- Liability for breaches of laws, regulations and/or contractual compliance requirements; and
- Of the regulatory compliance requirements, which parts will be provided as part of the services, and which requirements may result in extra charges by the service provider.

Conclusion

Cloud computing offers benefits as well as risks. As cloud computing is a variation of outsourcing, it should not be surprising that many of the risks are the same as or similar to those in more traditional IT outsourcing. Many of the risks are mitigated the same way: appropriate due diligence up front, strong contractual protections that account for higher risk data and applications, and continued vigilant governance. While businesses may discover many beneficial uses of cloud computing, they will also have to determine which applications and data types are not appropriate for cloud computing unless the provider can modify the solution to meet the business' regulatory and other requirements. ♦

Cloud Computing May Violate German Data Privacy Laws

Guido Zeppenfeld
Tim Wybitul
Andrea Patzak



Guido Zeppenfeld
Frankfurt
+49 69 79 41 2241
gzeppenfeld@mayerbrown.com



Tim Wybitul
Frankfurt
+49 69 79 41 2271
twybitul@mayerbrown.com



Andrea Patzak
Frankfurt
+49 69 79 41 1067
apatzak@mayerbrown.com

The term “cloud computing” is generally used to describe services through which a company accesses software applications, databases, infrastructure and related services via the Internet or other networks. The use of cloud computing is growing substantially worldwide due to the cost savings and other benefits it provides. Due to concerns regarding personal data protection and transfers, German data protection authorities want to impose tougher restrictions and requirements on both cloud computing and other outsourcing arrangements involving personal data. Companies need to ensure that they are complying with these strict new requirements. Failure to comply with these laws may result in substantial fines, civil lawsuits and reputational damages.

The German Data Protection Authority’s Statements

The Data Protection Authority of the German Federal State of Schleswig-Holstein (the *Unabhaengiges Zentrum fuer Datenschutz Schleswig-Holstein* – “ULD”) recently published on its web site a white paper that covers data privacy aspects of Cloud computing. The opinions expressed in the ULD’s paper are not legally binding on companies operating in Schleswig-Holstein or other German federal states. However, the ULD’s published views indicate the manner in which the ULD will view and

examine cloud computing arrangements. The ULD views may also influence data protection authorities in other German states. In the paper, the ULD expresses concern that many transfers of personal data in connection with Cloud computing arrangements will not satisfy requirements under German data privacy laws. The ULD called out “Public Clouds” in particular, but the concerns are not limited only to Public Clouds.

Due to concerns regarding personal data protection and transfers, German data protection authorities want to impose tougher restrictions and requirements on both cloud computing and other outsourcing arrangements involving personal data.

The German Data Protection Act (*Bundesdatenschutzgesetz* – “BDSG”) implements the EU Data Protection Directive. Section 11 of the BDSG specifically addresses requirements that data controllers must follow regarding data processors. Section 11 previously did not apply to data controller to data processor transfers *outside of the European Union*. Now, however, the ULD has taken the position that Section 11 does apply to transfers of personal data outside of the European Union. The result is that, according to the ULD, reliance solely on the EU standard data

transfer clauses (one of the more common means for accomplishing a compliant data transfer) for data controller to data processor transfers in a cloud computing engagement is not enough to satisfy German data privacy laws. In addition to the standard clauses, data controllers will also have to comply with Section 11 requirements of the BDSG.

Neither the BDSG nor the data protection authorities provide any extensive guidance on what regular control means, or how it will be interpreted.

Regardless of whether the cloud computing provider is located inside or outside of the European Union, the ULD demands that companies using cloud computing services must take adequate measures to safeguard the integrity and security of the personal data processed. For example, companies must include contractual provisions with cloud computing service providers in accordance with the criteria for data controller/data processor relationships (*Auftragsdatenverarbeitung*) set forth in Section 11 BDSG—regardless of the location of the cloud computing provider or the services. In addition, according to the ULD, companies or qualified external third parties must exert “regular control” over whether cloud computing providers observe the restrictions of the BDSG. The control must cover the processor’s technical and organizational measures used to protect the data. Neither the BDSG nor the data protection authorities provide any extensive guidance on what regular control means, or how it will be interpreted. The ULD has suggested that companies can do this in at least two ways: they can obtain expert advice, in the form of audits or certificates provided by external experts, that the service provider observes the legal restrictions; or they can obtain a binding guarantee declaration by the service provider in which the service provider provides a comprehensive commitment to obeying the obligations imposed by the law.

Data Transfer to Countries Outside the European Union

When personal data is transferred outside of the European Union in connection with the cloud computing services, in addition to complying with Section 11 of the BDSG, the transfer must be accomplished by

one of the permitted means. One widely used method is to employ the EU-approved standard clauses for transfer of personal data. Until recently, the Safe Harbor Agreement was also a permissible means of accomplishing personal data transfers from the European Union to the United States. However, German data protection authorities recently announced that they no longer regard Safe Harbor certifications of US companies as a stand-alone basis for fulfilling German data privacy standards. (For more information about the stricter requirements set out for German companies regarding the Safe Harbor certification, see <http://www.mayerbrown.com/publications/article.asp?id=9156&nid=6>.)

The ULD gave examples of situations in which cloud computing arrangements could satisfy the German data protection and transfer laws. Please note that the ULD requires that the requirements of Section 11 of the BDSG are also to be satisfied in these arrangements. Some of the examples, however, bear little resemblance to actual business practices and cloud computing service offerings.

German data protection authorities recently announced that they no longer regard Safe-Harbor certifications of US companies as a stand-alone basis for fulfilling German data privacy standards.

1. OPTION OF TERRITORIAL RESTRICTION

A cloud computing provider may offer its customers the option to restrict data processing to countries that are part of the European Economic Area (EEA) or the European Union.

2. ADEQUATE LEVEL OF PROTECTION PURSUANT TO THE EU COMMISSION

Cloud computing services may be provided in and from any jurisdiction for which the EU Commission has deemed to have an adequate level of protection pursuant to Sec. 4b Subsec. 2 Sent. 3 BDSG.

3. STANDARD CONTRACTUAL CLAUSES PLUS ADDITIONAL MEASURES

The company using the cloud computing services may comply via (i) use of standard contractual clauses and (ii) satisfaction of the requirements of Section 11 of the

BDSG. As mentioned above, use of the standard clauses was thought to be sufficient to accomplish a compliant data transfer.

There are questions regarding the ULD's view and application of Section 11 of the BDSG to data transfers outside of the European Union. Previously, Section 11 was thought to apply to data processing within the European Union, and not to transfers of personal data for processing outside of the European Union. The ULD's application of Section 11 to data processing outside of the European Union extends the prior reach of Section 11. Despite these questions, other German state data protection authorities are likely to share the ULD's view and enforce these requirements.

4. QUESTION OF APPLICATION OF BINDING CORPORATE RULES

Though Binding Corporate Rules (BCR) have previously applied to intercompany and multinational affiliated company transfers of personal data, the ULD has suggested that BCR might be adapted to cover non-affiliated processors. This view is not yet officially approved by the EU Article 29 Working Group (the EU advisory body that coordinates data protection activities among the EU member states), and its application and use for transfers to third-party processors, including cloud computing providers, remains to be seen.

What Your Company Should Do

If you have existing cloud computing service arrangements, or other outsourcing arrangements involving personal data from Germany, you should review these arrangements with counsel to ensure that they continue to meet the requirements of the German

data protection authorities. If you are considering entering into a cloud computing service arrangement involving personal data from Germany, you should review the ULD requirements with German lawyers to ensure that you structure the arrangement, contracts and control measures in a manner that satisfies the new and revised requirements under German data protection laws. You should also monitor the developments both in Germany and other EU countries. As the use of cloud computing increases, other EU data protection authorities are certain to provide their opinions and guidance on personal data protection and cloud computing.

Other Related Data Protection Developments in Germany

The ULD white paper is only one of several recent developments in personal data protection. There have been several scandals involving large German companies disregarding binding BDSG provisions. Recently, the joint coordination committee, in which all German data protection authorities align their regulatory actions (the so-called *Duesseldorfer Kreis*), passed strict control requirements for companies transferring personal data to Safe Harbor-certified data recipients in the United States. In addition, the German government is currently preparing new legislation regarding employee data protection.

Generally, the importance of data privacy as one major part of corporate compliance in Germany has increased substantially during the last few years, and it can safely be assumed that this trend will continue. As a consequence, companies operating in Germany need to stay current with these developments, and review their data privacy compliance programs. ♦

New EU Standard Contractual Clauses for Commissioned Data Processing

Tim Wybitul
Andrea Patzak



Tim Wybitul
Frankfurt
+49 69 79 41 2271
twybitul@mayerbrown.com



Andrea Patzak
Frankfurt
+49 69 79 41 1067
apatzak@mayerbrown.com

A company wishing to transfer data outside of the European Union (EU) has different possibilities to guarantee a data protection level similar to what it has in Europe, which would make the transfer permissible. Of these, the European Commission's standard contractual clauses have proven valuable, as they are not subject to the authorization requirement by the supervisory authorities.

However, the European Commission has passed new standard contractual clauses for commissioned data processing, the use of which is compulsory for new commissioned data agreements as of May 15, 2010. Prior agreements must be adjusted if the manner of the commissioned data processing changes. For the first time the new standard contractual clauses permit subcontracting; this is, however, subject to stringent requirements.

Recently, the EU passed new standard contractual clauses for the transfer of personal data to commissioned data processors located in countries outside of the European Union (EU) and the European Economic Area (EEA)—so-called third countries. As of May 15, 2010, the former contractual clauses provided by the EU Commission may no longer be used. The EU standard contractual clauses are probably the most-used instrument in order to

legitimize the transfer of personal data to third countries. This overview shows which requirements are set out for cross-border data transfers and how companies can fulfill these requirements.

Meaning of Commissioned Data Processing for European Companies

It is often an economic necessity for German companies to transfer personal data to recipients in third countries. Reasons for this need include outsourcing projects, centralized databases and joint ventures.

However, the European Commission has passed new standard contractual clauses for commissioned data processing . . .

When European companies enter into information technology (IT) outsourcing agreements with service providers in third countries, the service provider often gets access to personal data (e.g., data on the instructing company's employees). From a legal point of view such facts present a transfer of personal data into a third country. According to Sections 4b and 4c of the Federal Data Protection Act (*Bundesdatenschutzgesetz*, or BDSG), such cross-border transfers are only permitted under strict provisions.

The Term “Transfer”

Transferring is providing data to a third party. A third party is any person or agency which is not part of the transferring company. In business, third parties are, for example, employees of other companies or other persons from outside of the principal company. The German data protection laws stipulate the same requirements for the transfer of data within the same group of companies as for every other transfer; it does not recognize a privilege for the group of companies.

A transfer can also be both passing personal data to a third party and keeping data available for a third party to view or to request on demand. The data is transferred to the third party as soon as the third party views or demands the data.

Even if a transfer of personal data is permissible within Europe according to the BDSG’s common standards, this does not mean that the transfer automatically would be permissible to a third country without an adequate level of protection.

Stringent Requirements for the Permissibility of Transfers

German data protection authorities examine the permissibility of a data transfer into third countries via a two-level evaluation.

FIRST LEVEL PERMISSIBILITY EXAMINATION

In the first level evaluation, the data protection authorities will determine whether the planned transfer of personal data to a third party would be permissible according to the BDSG’s common standards. Generally, the BDSG prohibits handling personal data, unless a statutory regulation or a valid consent by the affected person permits this handling of data.

A typical example of transferring personal data in accordance with the BDSG’s common standards is if the transfer is required to maintain the legitimate interest of a company according to Section 28 Subsec. 1 Sent. 1 No. 2 BDSG. Additionally, there may not be any reason to assume that the affected person whose data is being transferred has a legitimate interest in excluding the transfer which

outweighs the company’s interest. The company must have a legitimate economic interest for the transfer. For example, lowering costs can certainly be such a necessary business reason.

Furthermore, a transfer according to Section 28 Subsec. 1 Sent. 1 No. 2 BDSG can only be effected if it is “necessary” to maintain the economic interest. That means that the transferring company can only transfer the data that is truly necessary to realize the legitimate business purpose.

The most important part of this legal examination is to determine whether the interests of the persons affected by the transfer are adequately protected. At this time the authorities weigh the company’s interests against those of the person whose data is to be transferred.

In practice, for example, it is recommended that companies look for precedents for permissible transfers (such as from adjudication, or activity reports by the state’s supervisory authorities) and to use these standards as an orientation.

If all of these requirements are fulfilled, then the transfer to another company in Germany, the EU or the EEA are permissible. The transfer to another company in a third country is, however, only permissible under stringent requirements. These are detailed below.

SECOND LEVEL PERMISSIBILITY EXAMINATION

Even if a transfer of personal data is permissible within Europe according to the BDSG’s common standards, this does not mean that the transfer automatically would be permissible to a third country without an adequate level of protection. Here, Section 4c BDSG states far more stringent requirements than those that apply to intra-German or intra-European transfers. Therefore, an adequate data protection level through additional means must be created in order to permit the transfer, or there must be an exception regulation, which permits the data transfer even without a previous creation of an adequate data protection level.

Companies often use the standard contractual clauses passed by the EU Commission in order to fulfill these requirements. In contrast to those binding company provisions named in Section 4c Subsec. 2 Sent. 1 BDSG Binding Corporate Rules [BCRs] the EU standard

contractual clauses do not need to be authorized from the responsible supervisory authority in order to facilitate a permissible data transfer into third countries.

The previous standard contractual clauses for commissioned data processing in third countries are no longer applicable for agreements concluded as of May 15, 2010.

These binding standard contractual clauses seek to establish a uniform standard in order to facilitate cross-border data transfers into third countries in a timely manner without bureaucratic delay. In the past, data protection supervisory agencies held different positions on whether standard contractual clauses needed to be presented to the supervisory authority individually or even needed to be examined and authorized at all.

The so-called *Düsseldorfer Kreis* determined that by using the standard contractual clauses completely and unchanged, there is neither an obligation for authorization from nor an obligation for disclosure to the supervisory authorities. The *Düsseldorfer Kreis* is the joint panel for the data protection supervisory authorities of the individual federal states. In Germany, the representatives of the supervisory authorities for the private sector are organized at state level and together form the *Düsseldorfer Kreis*. Therefore, usually the decisions rendered by the *Düsseldorfer Kreis* are decisive for the supervisory authorities.

The Different Types of Standard Contractual Clauses

Prior to the new standard contractual clauses decision, the EU Commission had decided on three sets of standard contractual clauses. The first two, dated June 15, 2001, and December 27, 2004, refer to “normal” transfers to another competent authority in a third country. The third set of standard contractual clauses for the transfer of personal data to commissioned data processors, dated December 27, 2001, deal with data transfer to data processing service providers that process data in commission for the data controller. Section 11 BDSG covers making personal data available to commissioned data processors in an intra-German or intra-European connection. Such a

commissioned data processing in third countries is, however, not envisioned by Section 11 BDSG.

The previous standard contractual clauses for commissioned data processing in third countries are no longer applicable for agreements concluded as of May 15, 2010. However, agreements with the old standard contractual clauses which are already concluded remain valid and do not need to be automatically amended to fit the EU Commission’s decisions. If, however, the contracting parties wish to agree upon changes to existing agreements regarding commissioned data processing in third countries, or if the principal wishes to award a subcontract, then the parties must conclude a new agreement using the new standard contractual clauses.

New Requirements for Cross-Border Commissioned Data Processing

REQUIREMENTS FOR SUBCONTRACTOR RELATIONS

Currently, under certain circumstances, the agent can enter into subcontractor relations on the basis of the new standard contractual clauses. That was not ruled in the previous standard contractual clauses for the transfer to commissioned data processors in third countries. The lack of such a regulation in the old standard contractual clauses was severely criticized. Such subcontracting is, however, subject to certain permissibility requirements:

- Before entering into a subcontract the principal must agree to it in writing.
- This agreement must obligate the subcontractor in the same manner that the agent in the main agreement is obligated.
- The agent must remain fully liable to the principal for all contractual violations by the subcontractor. Agent and subcontractor must agree upon a so-called third party beneficiary clause (*Drittbegünstigtenklausel*), under which affected persons must also be able to assert claims for damages against the subcontractor, if necessary.
- The law of the country in which the principal is based must also be the applicable law, just as in the old standard contractual clauses. The data protection laws applicable to the principal must now also apply to data processing by the subcontractor. If a German company transfers data to an agent in a third

country who, in turn, passes on some of the data to a subcontractor, then German law also applies to the agreement between the agent and the subcontractor.

- Additionally, the contractual relations with the subcontractors must be carefully documented. The agent must both inform the principal and obtain written authorization prior to a subcontracting, and must also provide the principal with additional copies of the subcontracts.
- Finally, the principal must annually maintain a current index of the agreements with subcontractors and make this index available to the relevant supervisory authorities. It is not clear whether this can be merely a list of the existing subcontracts, or whether the index must also contain the respective clauses. However, it can be assumed that the agent does not need to disclose the agreements with the subcontractors. According to the opinion of the *Düsseldorfer Kreis* the principals do not need to disclose to the supervisory authorities the standard contractual clauses between principal and agent. Therefore, this suggests that a subprincipal does not need to disclose the standard contractual clauses executed with the sub-agent, which must contain the same provisions as those of the concluded standard contract clauses of the relationship.

APPLICABLE LAW FOR THE DATA PROCESSING CONTRACT

The standard contractual clauses only refer to data protection law provisions. A complete agreement regarding commissioned data processing in a third country must also cover substantial economic aspects, which the principal and agent can determine in the remaining agreement.¹ The wording of the standard contractual agreement and the recitals by the EU Commission prescribe that the standard contractual clause (which refers to data protection in transfers) is subject to the law of the country in which the principal is based. Now, data processing contractors are also subject to the principal's applicable data protection laws. However, it is possible to have the other (economic) provisions be subject to another legal system by making the standard contractual clauses a separate appendix to an outsourcing or service agreement. This appendix can then—regardless of the main agreement—be subject to the law of the country in which the principal is based. It remains to be seen what

position the supervisory authorities will take regarding this procedure.

Implementation of the New Standard Contractual Clauses in Contractual Changes

The supervisory authorities will probably apply a more stringent measure regarding whether the old standard contractual clauses may be further used or the new standard contractual clauses must be implemented because there was a minor change to the existing agreement. It can be expected that every amendment of the agreement will be assessed as a contractual amendment within the meaning of the EU Commission's decision.

Existing contractual clauses should be examined to determine if changes to contract terms, appendices or amendments can require the use of the new clauses.

Whether such a minor change applies to agreements that consist of numerous contracts is not easy to answer, especially regarding comprehensive IT service agreements which, for example, deal with data processing in an EU/EEA foreign country. Such agreements usually consist of a master services agreement and numerous appendices, which define the subject matter of the agreement more closely regarding definitions, statements of work, service level agreements, pricing terms and other comparable provisions.

Effects on Companies

Companies should respond to this changed legal situation by thoroughly examining whether and how they should use the new standard contractual clauses. Existing contractual clauses should be examined to determine if changes to contract terms, appendices or amendments can require the use of the new clauses. Companies must also ascertain the scope of the contractual changes. Failure to take these steps can cause penalties, claims for compensation damages and, above all, substantial injury to reputation if it appears the company is not serious about data protection.

Endnote

- ¹ EU Commission, Decision 2010/87/EU, recital 4, ABL. EG Nr. L 39 dated February 12, 2010, 5(5).

When Barking Dogs Bite in *BSkyB vs. EDS*

Mark A. Prinsley
Oliver Yaros



Mark A. Prinsley
London
+44 20 3130 3900
mprinsley@mayerbrown.com



Oliver Yaros
London
+44 20 3130 3698
oyaros@mayerbrown.com

Information technology (IT) projects that go seriously wrong can be costly, as UK satellite TV broadcaster Sky found out when its contract with EDS to design, develop and integrate a new customer relationship management system overran by more than three years and cost Sky some £217 million more than it had anticipated (from a baseline budget of £47.6 million). The recent high-profile judgement in the English case of *BSkyB v. EDS* highlights not only specific issues involving misrepresentation, but also a number of wider concerns relating to the procurement process with implications for the IT and outsourcing industries.

Background

Sky sought to obtain a new customer relationship management system that would provide improved service to its call centre customers. Electronic Data Systems (EDS) won the invitation to tender in 2000 but performed poorly at implementing the new system and meeting the 18-month timeline agreed upon with Sky. Sky ultimately took over EDS' role in 2002 but only finished the project in March 2006 at a total cost of about £265 million.

Sky launched legal proceedings in 2004, claiming damages of £709 million for EDS' fraudulent misrepresentations that led Sky to select and contract with EDS, negligent misrepresentations that had led Sky to

renegotiate the contract in 2001 and breach of contract. EDS sought to rely upon an entire agreement clause in the contract to exclude pre-contract representations, and a limit of liability clause which capped its liability at £30 million. Because liability for fraud cannot be limited or excluded under English law, proving fraudulent misrepresentation was vital if Sky was to recover more than £30 million.

The recent high-profile judgement in the English case of *BSkyB v. EDS* highlights not only specific issues involving misrepresentation, but also a number of wider concerns relating to the procurement process with implications for the IT and outsourcing industries.

Credibility of EDS' Key Witness

Critical to Sky's case was the allegation that Joe Galloway, a managing director who led EDS' response to the tender, was dishonest in his conduct with Sky. By way of example, Sky's counsel demonstrated that although Mr. Galloway had said in his witness statement that he had obtained an MBA from Concordia College, St. John in the US Virgin Islands, it was in fact possible to buy an MBA from Concordia College's website. Sky's counsel actually did this in the name of his dog Lulu, obtaining

a certificate and transcripts that gave Lulu better results than Mr. Galloway's. Mr. Galloway asserted that he had not bought his MBA online but, rather, had taken flights from a nearby island to St. John to attend classes at the university for a year while working on a project there for Coca Cola. However, these claims were rebuffed with evidence that was no Concordia College, Coca Cola office or airport on St. John.

Sky also showed that before it selected EDS, Mr. Galloway had sent Sky a rate card spreadsheet containing errors that would have led to EDS making significantly lower profits from the project than he had calculated. After EDS had been selected and Sky sent to EDS the draft letter of intent to appoint them, attaching this rate card, Mr. Galloway realised his mistake and forwarded to Sky a fabricated email. The email contained a corrected rate card spreadsheet, representing a substantial increase in costs to Sky, which Mr. Galloway said had been sent to Sky soon after the original rate card in an attempt to make it appear that he had spotted the error and tried to rectify it before the selection of EDS.

The evidence led the judge to the conclusion that Mr. Galloway had shown "an astounding ability to be dishonest," that his "credibility was completely destroyed by his perjured evidence over a prolonged period" and that his evidence could not be relied upon alone.

Misrepresentation

Despite the judge's conclusions, Sky still needed to demonstrate that it had relied upon dishonest representations that Mr. Galloway had made on behalf of EDS.

The court found that the entire-agreement clause in the contract excluded contractual liability for any representations made by EDS before entering into the contract, but in the absence of express wording to the contrary, did not exclude liability for negligent misrepresentation.

Sky submitted that EDS had made five major misrepresentations, but the court only found one allegation of fraudulent misrepresentation to be proved: that while EDS had represented to Sky that EDS had

carried out a proper analysis of how long it would take to complete the project, Mr. Galloway had in fact, despite leading the estimating process, approached the whole question in a cavalier fashion while aware that no proper attempt had been made to assess whether the project could be completed in the timescales proposed.

The judge concluded that Mr. Galloway ignored the need for analysis, proffering timescales which he thought were those Sky desired without having a reasonable basis for doing so. The judge further held that Mr. Galloway had known that the timescales were inadequate because he had initially disagreed with them as insufficient in an earlier EDS draft, but still allowed their use in EDS' response to Sky. The judge found that Mr. Galloway's conduct "went beyond carelessness or gross carelessness and was dishonest . . . he acted deliberately in putting forward the timescales knowing that he had no proper basis for those timescales. At the very least he was reckless, not caring whether what he said was right or wrong." Sky relied on this misrepresentation in awarding the contract.

The fact that Sky only succeeded in proving one of its allegations demonstrates the difficulty of establishing fraudulent misrepresentation under English law.

Entire-Agreement Clause

The court found that the entire-agreement clause in the contract excluded contractual liability for any representations made by EDS before entering into the contract, but in the absence of express wording to the contrary, did not exclude liability for negligent misrepresentation.

Judgment

The finding of fraudulent misrepresentation circumvented the £30 million liability cap and the entire-agreement clause. EDS was ordered to make an interim payment of £270 million when judgment was handed down in January 2010. In June 2010 it was reported in the press that the parties had agreed to settle, with EDS making a total payment of £318 million to cover Sky's damages, costs and interest.

Comment

The fact that Sky only succeeded in proving one of its allegations demonstrates the difficulty of establishing fraudulent misrepresentation under English law, even where a leading employee of the supplier has clearly been dishonest. If Sky had failed to prove fraudulent misrepresentation, the company could only have recovered a maximum of £30 million, a fraction of the costs that they allegedly incurred. In any event, Sky recovered approximately 45 percent of the £709 million in damages claimed.

This case demonstrates the need for customers to carefully investigate proposed suppliers and their responses while running a procurement process, and to ensure that any cap on liability is sufficient for the losses that the customer might experience as part of the project. Suppliers should ensure that correct procedures are in place for carefully considering invitations to tender and diligently preparing their responses. Suppliers should also identify all pre-contract representations that they want to exclude and expressly reference them in entire-agreement clauses. ♦

Author Profiles

PAUL J.N. ROY

Partner

Paul Roy represents clients in a broad range of onshore, nearshore, and offshore information technology and business process outsourcing transactions. He regularly advises clients on the outsourcing of IT infrastructure services and support, application development and maintenance, network management and support and help desk/call center services. Paul also advises clients on the outsourcing of finance and accounting functions, HR/employee services, CRM and financial services operations, among other business process functions.

ROHITH P. GEORGE

Associate

Rohith George is an associate in the Business & Technology Outsourcing practice, with experience specifically in business process and operations outsourcing arrangements, information technology transaction, and facilities management outsourcing arrangements. In addition, Rohith has assisted clients with data transfer and privacy issues, electronic contracting and signatures and web site design and review.

PAUL A. CHANDLER

Counsel

Paul Chandler represents clients in connection with the outsourcing of information technology functions and business processes. He assists clients that are working to develop, license, market, distribute and acquire rights in a wide variety of technology-related products, services and intellectual properties, including computer software and hardware, databases, online services and telecommunications systems. Paul also represents clients interested in forming technology joint ventures and other strategic alliances.

LINDSAY BLOHM

Associate

Lindsay Blohm is an associate in the Business & Technology Outsourcing practice. She has acted as the lead associate on various large-scale information

technology outsourcing and business process transactions. She also represents clients in licensing and other technology transactions and reviewing/revising statements of work for technology (hardware and software design and development) projects.

BRAD L. PETERSON

Partner

Brad Peterson is a partner in the Business & Technology Sourcing Practice in Chicago. His practice focuses on business process and IT outsourcing transactions, alliances, and information technology transactions, including software license and implementation agreements. With a background in the IT industry, an MBA from the University of Chicago and a JD from Harvard Law School, he provides practical, business-oriented advice on technology contracts.

GREGORY A. MANTER

Senior Associate

Gregory Manter is a senior associate at Mayer Brown LLP in Chicago, practicing with the Business and Technology Sourcing Group. He represents clients in a wide variety of information technology and business process outsourcing transactions and other information technology licensing and development transactions. He has represented customers in numerous software implementation agreements, including several large ERP implementation agreements. He is a graduate of the Duke University School of Law, where he also received an L.L.M. in International Law.

KAVI C. GRACE

Associate

Kavi Grace is an associate in the Business & Technology Sourcing practice, focusing on the areas of business process, operations and technology outsourcing, consulting, software development, e-commerce and information technology transactions. He regularly drafts and negotiates a broad range of agreements involving outsourcing arrangements, consulting services, software distribution and technology development services.

REBECCA S. EISNER

Partner

Rebecca Eisner has represented clients in complex global and offshore technology and business process outsourcing transactions and has experience with restructuring and renegotiating outsourcing transactions, in-sourcing, managing acquisitions and divestitures in outsourcing transactions and the termination of outsourcing agreements. Rebecca's privacy and data security work includes advising clients on privacy and data transfer issues affecting corporate initiatives, such as divestitures, global data programs, and global technology solutions.

DANIEL A. MASUR

Partner

Daniel Masur represents national and international clients in a broad range of onshore, near-shore and offshore information technology and business process sourcing transactions involving global and niche outsourcing providers, offshore captives and various hybrid structures. He is recognized as one of the leading lawyers for outsourcing by Chambers, Legal 500 and Best Lawyers in America.

GUIDO ZEPPENFELD

Partner

Guido Zeppenfeld heads Mayer Brown's German Business Technology Sourcing practice and is responsible for the firm's German Employment & Benefits practice. In the course of his work, he advises and represents client organizations in connection with all legal matters regarding the management of human capital, including restructuring measures and outsourcing projects. His practice also includes compliance with privacy laws and protection of personal data under German and EU law.

TIM WYBITUL

Partner

Tim Wybitul advises companies on data privacy and compliance and regarding internal or regulatory investigations. In addition, he supervises internal investigations and coordinates and leads resulting litigation. Among other things, he has been leading a team of attorneys since 2008 which assists a large

Swiss bank with regards to cross-border investigations initiated by SEC, DOJ and IRS. He has extensive experience in representing international enterprises in court proceedings. Tim has released numerous publications on data privacy and general compliance topics. He is an associate lecturer at the German University for Professional Studies, Berlin.

ANDREA PATZAK

Associate

Andrea Patzak is an associate in the Frankfurt office. Her experience includes the representation of national and international clients in connection with German and European data protection matters and compliance projects. She advises clients on the implementation of IT business models in the German market relating to e-commerce and Internet law. Her experience includes drafting of and advising on e-commerce, information technology and telecommunications agreements as well as advice on copyright and trademark law.

MARK A. PRINSLEY

Partner

Mark Prinsley is head of the Intellectual Property & IT group in London as well as the outsourcing practice. He is named as a leading individual in the areas of business process outsourcing, information technology and intellectual property by Chambers' UK and Global guides. Mark's practice concentrates on non contentious intellectual property including, in particular, IT project, outsourcing and privacy and data security work.

OLIVER YAROS

Associate

Oliver Yaros is a senior associate in the IP/IT practice of the London office. He has acted on large business process and IT outsourcing projects for clients in the human resources, financial institutions, chemicals industries. Oliver has also advised on data protection matters, intellectual property matters including patent, trade mark, domain name and copyright disputes.

About Mayer Brown

Mayer Brown is a leading global law firm with offices in major cities across the Americas, Asia and Europe. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant portion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest investment banks. We provide legal services in areas such as Supreme Court and appellate; litigation; corporate and securities; finance; real estate; tax; intellectual property; government and global trade; restructuring, bankruptcy and insolvency; and environmental.

OFFICE LOCATIONS

AMERICAS

- Charlotte
- Chicago
- Houston
- Los Angeles
- New York
- Palo Alto
- São Paulo
- Washington DC

ASIA

- Bangkok
- Beijing
- Guangzhou
- Hanoi
- Ho Chi Minh City
- Hong Kong
- Shanghai

EUROPE

- Berlin
- Brussels
- Cologne
- Frankfurt
- London
- Paris

ALLIANCE LAW FIRMS

- Spain, Ramón & Cajal
- Italy and Eastern Europe, Tonucci & Partners

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.

© 2010. Mayer Brown LLP, Mayer Brown International LLP, Mayer Brown JSM and/or Taül & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. All rights reserved.

Mayer Brown is a global legal services organization comprising legal practices that are separate entities (the Mayer Brown Practices). The Mayer Brown Practices are: Mayer Brown LLP, a limited liability partnership established in the United States; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales; Mayer Brown JSM, a Hong Kong partnership, and its associated entities in Asia; and Taül & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek specific legal advice before taking any action with respect to the matters discussed herein.

