MAYER·BROWN

Issue 16 | Spring 2011

Business & Technology Sourcing
REVIEW

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 50 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.

Editors' Note

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

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

Lei Shen
Chicago
+1 312 701 8852
lshen@mayerbrown.com

Welcome to the Spring 2011 edition of the Mayer Brown *Business & Technology Sourcing Review*.

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:

- Resolving disputes in outsourcing contracts including litigation and effective due diligence;
- Key issues in service agreements for M&A transactions;
- Principles for compliance with laws for outsourcing; and
- European perspective on privacy laws and their role in outsourcing.

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; or 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. ◆

A Litigator's Perspective on Outsourcing Relationships

Robert J. Kriss
Brad L. Peterson

Robert J. Kriss
Chicago
+1 312 701 7165
rkriss@mayerbrown.com

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

Because of the typically long duration and high degree of interdependence between companies involved in an outsourcing relationship, it is important to seek as much clarity as possible in contracts and communications concerning disputes. Ambiguity and vague standards that are difficult to prove when disputes arise can lead to costly litigation and acrimonious relations between companies that rely on each other for their business success. We examine aspects of the outsourcing relationship and dispute resolution with a litigator's eye.

Two characteristics distinguish outsourcing relationships from many other commercial relationships—the high degree of interdependence between two otherwise separate companies, and the lengthy term of the contract. These characteristics have important implications for the drafting of outsourcing contracts and resolving disputes.

Parties to outsourcing contracts have strong business incentives to make the relationship work. The customer is turning over an important part of its business to be executed by an outsider, while the service provider is making substantial investments of time, people and money to address the special needs of the customer. As a result, termination of the relationship likely will cause both parties serious economic disruption. Furthermore, it is important that disputes be resolved quickly, fairly and in a manner that will not make it difficult for the parties to continue working together effectively.

Because of the long duration of outsourcing contracts, it is difficult to anticipate all the issues that may arise during the relationship, particularly as changes occur in each party's business. One approach is to develop general standards that can evolve as conditions change. However, generality results in uncertainty, uncertainty breeds disagreement, and disagreements threaten the stability of outsourcing relationships. Drafters of outsourcing agreements should not give up trying to address specific problems that can be anticipated just because they cannot anticipate all that may happen.

When disputes do arise, resolution should be a means to a larger end—preservation of an effective working relationship. Because outsourcing relationships develop over time, the parties have an opportunity to shape the record as it is being made through detailed correspondence. If both parties seize the opportunity, then the record likely will be reasonably clear and will allow for a fair and efficient resolution. If only one side seizes this opportunity, then it stands a good chance of prevailing over the other side.

Litigation Prevention in Drafting the Contract

There is a tendency to use vague terms in the contract to address unknown future circumstances. Examples include material breach; gross negligence; willful misconduct; direct, indirect, consequential damages; best efforts; generally accepted standards; and commercially reasonable efforts. These concepts are unclear in the case law and difficult to prove from an evidentiary standpoint.

As mentioned earlier, uncertainty breeds misunderstanding. It also engenders costly litigation because the parties will not be able to resolve their dispute through a summary judgment motion brought early in the case based upon legal, as opposed to factual, grounds. Unless the matter is settled, there likely will be significant discovery and an evidentiary hearing. The matter may be difficult to settle because uncertainty makes each side evaluate the likely outcome of the case very differently. What can be done to address the problem? One approach is to reduce the uncertainty by using a non-exhaustive list of specific examples. These can be useful if the subject matter of the dispute falls squarely within the scope of the examples, but examples also are useful in demonstrating the intent of the parties in resolving unanticipated problems.

For example, there is much confusion in the case law as to what is meant by direct versus indirect or consequential damages. Rather than leave the issue open to argument once a dispute has arisen, the contract might state: "Direct damages include but are not limited to the additional cost of securing an alternative service provider."

Contract provisions limiting liability or remedies may include exceptions for "gross negligence" or "willful misconduct." But these terms have no clear meaning in the law. Where is the dividing line between ordinary negligence and gross negligence? Use of the term "gross negligence" increases the likelihood of a contested issue of fact foreclosing the possibility of resolving the dispute on summary judgment. Also, does a deliberate breach of contract constitute willful misconduct? Different jurisdictions answer this question differently. To reduce uncertainty, consider using a better-defined term, such as "intentional tortious act."

In short, it is useful to review the terms of an outsourcing contract from a litigation perspective and consider how difficult it would be to persuade a judge or jury of the legal and factual merit of your position if a dispute were to arise. If there is uncertainty in either the law or the facts, consider what can be done in the contract to reduce that uncertainty.

[I]t is useful to review the terms of an outsourcing contract from a litigation perspective and consider how difficult it would be to persuade a judge or jury of the legal and factual merit of your position if a dispute were to arise.

Attention should also be paid to the dispute resolution process specified in the contract. The process can have a serious impact upon the morale of the parties and their commitment to making the relationship work. You do not want to win the battle and lose the war. The big picture is the relationship, and it will sour if the process is unfair or unnecessarily adversarial, or if disputes fester for a long time before they are resolved.

Finally, it is important to anticipate the scenario in which a third party sues the customer, but not the service provider, based upon conduct that is within the scope of services to be performed by the service provider. Many agreements contain "indemnity" and "duty to defend" provisions with respect to third-party claims. But often these provisions do not adequately take into account how such litigation would proceed. The claims may involve activities that are within the customer's scope, those that are within the service provider's scope, or activities where there is overlap between the activities of the customer and the service provider. The service provider's ability to pay a judgment may also be more limited than the customer's. As a result, the customer may not be comfortable relying upon the service provider to defend the suit.

Dispute Resolution Techniques

Disputes in outsourcing relationships often develop slowly over time, in which case there is ample opportunity to shape the record. A party's objective should be to obtain helpful evidence and admissions and avoid surprise by learning the other side's best arguments, and pinning them down to those arguments, long before formal dispute resolution begins.

For example, if a customer is concerned that a service provider may fail to meet a deadline for accomplishing a transformational project, the customer might send a letter to the service provider stating:

> We believe that you have not made commercially reasonable progress on the project and will be unable to meet the current deadline. Failure to implement according to the deadline will result in our suffering substantial losses. We wish to mitigate these losses by retaining a new service provider now unless you are able to provide specific, credible written assurances that you will meet the deadline.

If the service provider does not respond adequately, or at all, the customer will have substantially less risk in terminating the contract and/or arranging for an alternative service provider for the project. If the service provider responds to the letter but fails to perform as it promises, the probability of success in subsequent litigation against the service provider is high.

In short, it is important to document concerns in letters sent to the other party to create a clear record for subsequent dispute resolution. Similarly, it is important that no significant letter from the other side should go unanswered. In litigation, silence may be construed as an admission.

In preparing written communications, one should think about a juror or arbitrator reading the correspondence. It is important to maintain a reasonable tone and provide more background, including chronology, than might be necessary for the specific recipient of the communication. This way, if the matter is not resolved amicably, a fact-finder will have a better understanding when he or she reads the document in a trial or arbitration. The power of a well-written document in a litigation or arbitration proceeding cannot be overstated, particularly if the other side does not respond or does not respond persuasively.

The power of a well-written document in a litigation or arbitration proceeding cannot be overstated, particularly if the other side does not respond or does not respond persuasively.

Controlling the flow of information also is very important when a dispute is developing. Consider designating a lead lawyer and business person and have all major communications with the other party flow through them. The team should be instructed to forward all e-mails from the other party to the team leaders and not to respond to e-mails without team leader approval. Also, it is critical to use a secure internal communication network and advise all participants that whatever they put in written form, electronically or hard copy, could be discoverable. Therefore, they should be given guidance as to what types of records to make and what types not to make.

Conclusion

Clarity is important in drafting outsourcing contracts and in addressing disputes that may arise during the relationship. Both parties have an interest in minimizing uncertainty in their relationship and avoiding disputes, or if disputes arise, in rationally resolving them as quickly and amicably as possible. Accordingly, if sufficient attention is paid to clarity at the time the contract is executed and when trouble first appears, the chances are good that disputes can be avoided or resolved without disrupting the stability of the long-term relationship. ◆

Effective Due Diligence Minimizes the Risk of Disputes in Outsourcing Transactions

Linda L. Rhodes

Linda L. Rhodes
Washington DC
+1 202 263 3382
lrhodes@mayerbrown.com

Effective, comprehensive due diligence is an essential component of any business and technology outsourcing transaction. A meticulous due diligence process conducted by both client and service provider will do much to mitigate both parties' risks and to facilitate certainty in pricing. It will also promote a smoother, better-defined and informed outsourcing relationship in which the potential for dispute is minimized. This article discusses why outsourcing clients and service providers should implement thorough due diligence prior to contract negotiations and provides an overview of key factors for investigation and analysis.

Due diligence involves:

- The customer's investigation and analysis (i) of those aspects of its business that it intends to outsource, which will help the customer to prepare for the request for proposal (RFP) and negotiation process and to determine if its objectives can be achieved through outsourcing: and (ii) of the service provider, in order to determine if the service provider's approach, solution and costs will meet the customer's needs.
- The service provider's investigation and analysis of the customer and its business, in order to develop a solution that will fit the customer's needs.

The results of the customer's due diligence of the business it plans to outsource will help form the RFP. Both parties will use the results of their due diligence efforts to determine appropriate solutions, charges, service levels, governance and other key aspects of the outsourcing transaction.

Customer Due Diligence

The customer should conduct due diligence on the business to be outsourced and with respect to the service provider.

The customer needs to have a complete understanding of those aspects, and the objectives to be achieved through outsourcing, to determine if an outsourcing solution will provide the desired results.

CUSTOMER DUE DILIGENCE OF THE BUSINESS TO BE OUTSOURCED

The customer should start its due diligence by investigating those aspects of its business that it intends to outsource. The customer needs to have a complete understanding of those aspects, and the objectives to be achieved through outsourcing, to determine if an outsourcing solution will provide the desired results. The best due diligence starts early. In fact, as a customer, the best time to start is before the customer even begins the RFP and negotiation process.

Customers should adhere to a practice of maintaining complete and accurate records of their findings. These should include:

- Physical assets, including servers, equipment and other tangible assets and the locations of each;
- Requirements of the business, including interoperability requirements between the customer's assets and networks being outsourced and other customer and third-party systems with which those assets and networks need to interact;
- Intangible assets, including the customer and third-party software used in the outsourced business; and
- Third-party contracts, including software licenses, maintenance and support contracts and other third-party contracts relevant to the outsourced business.

The customer should also determine which of its employees perform services for the outsourced business and identify policies and procedures that may have significant impacts on the solution.

The customer should use the results of its due diligence to build its base case. The customer should determine the costs it is currently incurring for the services, the requirements for the services and service levels, and whether the assets and employees associated with the outsourced business are also required for retained customer functions. This internal investigation and analysis is critical for building an effective RFP. The more complete and accurate the information provided in the RFP, the better the responses that the customer will receive from potential service providers.

CUSTOMER DUE DILIGENCE OF THE SERVICE PROVIDER

The customer should also conduct due diligence to determine if the service provider has the expertise and qualifications necessary to perform the services and meet the customer's objectives. Due diligence will also help the customer to fully understand the costs associated with the outsourced solution and to determine if the service provider's processes, procedures and approach will fit with those of the customer. The customer should probe the service provider on its proposed solution to confirm that it meets the customer's requirements and that the proposed processes and timelines can realistically be met.

To obtain the material needed to make an informed choice among potential vendors, customers need a strong RFP coupled with conversations with the service provider's relevant personnel. The RFP should require each potential service provider to explain, among other things: how it will meet the customer's requirements; its qualifications; the methods and processes it will use in performing the services; its staffing plan for the services; its use of onshore and offshore resources; and its pricing methodology.

Due diligence will also help the customer to fully understand the costs associated with the outsourced solution and to determine if the service provider's processes, procedures and approach will fit with those of the customer.

Service Provider Due Diligence

While the service provider should be an expert in performing the outsourced services, it will need to carefully review the particularities of the customer's business and the requirements for successfully handling the outsourced function.

SERVICE PROVIDER DUE DILIGENCE OF THE CUSTOMER'S BUSINESS

The service provider should review the customer's requirements, physical and intangible assets, and third-party contracts. The service provider should also review the current processes and procedures used by the customer (or by an incumbent service provider) to perform the relevant services and should meet with the employees who perform the services, functions and responsibilities to gain an understanding of their roles and responsibilities.

BASELINES

The service provider should conduct due diligence to determine the accuracy of, and fill in any gaps related to, the baseline numbers and costs that were provided by the customer or included in the RFP. Pricing under most outsourcing agreements is based upon unit(s) of resource consumption. As the resource units increase above specified amounts, the monthly charges increase by additional resource charges; and as the resource units decrease below specified amounts,

monthly charges decrease by reduced resource credits issued to the client by its service provider. In order for this process to work, it is important that the baselines be established using accurate information.

THIRD-PARTY CONTRACTS

Once the third-party contracts used in the outsourced business have been identified, those contracts will need to be reviewed to determine whether they can be used by the service provider in performing the services and/or whether third-party consents will be required. The definitive agreement should specify which party is responsible for obtaining those consents and who will bear any associated costs. The extent and criticality of consents required and alternatives when consents are delayed or are not obtained should be considered in the development of the solution.

REGULATORY REQUIREMENTS OF COUNTRIES IN WHICH THE CUSTOMER OPERATES

The service provider should know the legal requirements applicable to the services and should take responsibility for obtaining necessary regulatory consents and for complying with the laws of countries in which the services are to be provided.

SERVICE PROVIDER ACQUISITION OF ASSETS

In certain outsourcing transactions, the service provider may actually acquire assets of the customer, take assignment of third-party licenses and acquire employees used to perform the services prior to the outsourcing of the business. In any case, the service provider may need to utilize certain customer assets in order to provide the services. The service provider should consider whether the customer's assets are sufficient to meet the purposes they will serve.

Lack of Appropriate Due Diligence

A primary goal of an outsourcing transaction is for the service provider to develop a solution and perform services that meet the business objectives of the customer at charges that provide a profit for the service provider while meeting the customer's financial objectives. Failure to conduct accurate and complete due diligence can result in numerous unwanted consequences that jeopardize the ability of the parties to achieve this goal, including the following:

ASSUMPTIONS

The parties should seek to investigate all necessary matters in order to avoid the need for assumptions in the definitive agreement. However, the less the service provider knows about the outsourced business and the more gaps in its information, the more the service provider will attempt to include assumptions in its statements of work. Including assumptions in a statement of work (in particular where the assumptions are critical to the performance of the services) can greatly increase the risk of disputes between the parties as they attempt to negotiate changes to services and charges if the assumptions are not accurate.

TRUE-UPS

In extraordinary cases where there is a lack of complete and accurate information, a service provider may also request that the parties "true-up" baseline numbers (i.e., adjust the baselines and make corresponding adjustments to the charges, ARCs and RRCs) after the definitive agreement is signed. Leaving baselines subject to true-up can also lead to dispute as the parties deal with the impact
of changes in the baseline numbers.

CHANGE ORDERS

If a definitive agreement is not based upon accurate and complete information, there are likely to be a high number of change orders. If the customer has negotiated a strong contract, the risk of additional costs for changes resulting from a lack of information should generally be placed upon the service provider. However, the need for additional resources and efforts that result from factors that were unknown at the time a contract was signed may not be covered under the scope of the contract. As a result, disputes may arise as the parties discuss how to deal with these service and cost adjustments.

If the customer is required to cover the costs of changes in the solution arising from information discovered after the agreement was signed, the customer may no longer be able to achieve its outsourcing objectives. Even if the service provider must absorb the additional change-related costs, the customer will be faced with a provider looking to find ways to maintain a profitable relationship after absorbing those costs.

DELAYED GO-LIVE

A good contract will include appropriate incentives for the service provider to meet go-live dates, such as withholding of payment unless and until critical milestones are met and/or deliverable credits associated with a failure to meet critical milestone dates. However, if a lack of proper investigation leads to unexpected delays, the service provider may not be able to meet go-live dates, regardless of whether such incentives are built into the contract.

From the customer's perspective, the ability to institute penalties against a service provider, or even pursue damages against that provider, in the event go-live is delayed is no substitute for a smooth-running business. In addition, many of the consequential damages that a customer could suffer may not be recoverable under the terms of the contract.

Conclusion

While considerable effort is required for effective due diligence, the long-term benefits of thorough and complete investigation and analysis will certainly outweigh those efforts. In the long run, effective due diligence by both parties will reduce the risk of disputes between the parties and will result in a more successful relationship. ◆

Service Agreements in M&A Transactions

D. Michael Murray
Brad Peterson
Paul Chandler

D. Michael Murray
Chicago
+1 312 701 7321
mmurray@mayerbrown.com

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

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

Companies increasingly are relying on external providers to deliver essential business services. As a result, organizations involved in merger and acquisition (M&A) transactions find themselves embroiled in complex, time- and cost-consuming negotiations surrounding third-party services agreements. In this article, we discuss why and when these crucial negotiations should be conducted and how they can be effectively structured to promote transactional value, control deal expense and mitigate buyer-seller risk.

Services agreements are becoming more important in mergers and acquisitions (M&A) as companies increasingly rely on external providers for critical functions. Early attention to services agreements in M&A planning, due diligence and negotiations can increase deal value for, and mitigate risk to, both buyers and sellers. This article describes best practices for buyers and sellers in addressing services agreements in connection with M&A transactions.

Changing Business Structures Are Creating New Opportunities

Intense cost pressures have forced companies to reduce the costs of performing services[1] that support their core businesses, such as information technology, human resources, finance and accounting, procurement and facilities management. One effective way to reduce those costs is to outsource traditionally internal functions to service providers that can offer both economies of scale and service delivery centers with world-class tools and processes. Thus, a company being bought and sold in an M&A transaction (which we refer to as the target company here) is increasingly likely to depend on services being provided by multiple unaffiliated outsiders.

[D]eal teams can sometimes miss opportunities to preserve the value of existing agreements and mitigate the risk of leakage of all or some of the transaction's economic benefits to a third-party service provider.

M&A practice evolved in an era when "third-party services agreements" could generally be ignored until the transaction was nearly final. Even today, deal teams often focus on the M&A transaction first, leaving the services agreements and other post-closing operational details until the frantic rush to signing, or sometimes even as a post-signing or post-closing item.[2] In many cases, the people who know what services are needed and who can provide them are excluded from the

deal team until very shortly before, and sometimes even after, the M&A agreement is signed. As a result, deal teams can sometimes miss opportunities to preserve the value of existing agreements and mitigate the risk of leakage of all or some of the transaction's economic benefits to a third-party service provider.

In this regard, there are a number of opportunities to increase deal value and mitigate risk. These include:

- Existing third-party services agreements used only by the target.
- Existing third-party services agreements shared by the target and the seller.
- Steps that potential sellers can take to prepare for future M&A transactions.
- Steps that potential buyers can take to prepare for future M&A transactions.

Existing Third-Party Services Agreements Used Only by the Target

If the target of the M&A transaction is the only business in the seller's corporate group using a services agreement, the easiest approach is generally to have the target continue using the existing agreement (and being bound by the existing agreement) after the acquisition. However, services agreements often prohibit assignment or change of control. Savvy third-party providers can, and often do, use those prohibitions as leverage to exact a price for the ease of continuing the services agreement—particularly if the existing pricing is not favorable to the provider, or if it is costly to replace the agreement.

Replacing an existing services agreement creates operational risk and might be surprisingly costly due to early termination fees or minimum volume commitments. Similarly, adding the target as a service recipient under the buyer's existing arrangements may require lengthy negotiations with the buyer's third-party providers.

Replacing third-party providers on complex or large-scale services agreements often takes far longer than the M&A deal cycle and may require the involvement of people beyond the M&A team's "circle of knowledge." Rushed negotiations may result in substantial opportunity costs. In many cases, better pricing is available to customers that have the time to identify their true needs, conduct a robust sourcing process and make long-term commitments. For a large-scale agreement for a critical service, this process can take three to twelve months from start to finish.

Replacing third-party providers on complex or large-scale services agreements often takes far longer than the M&A deal cycle and may require the involvement of people beyond the M&A team's "circle of knowledge." Rushed negotiations may result in substantial opportunity costs.

The current service provider's leverage will grow as the closing date of the M&A transaction approaches and the buyer's options narrow. As a result, there is a risk that the current provider's demands will grow with its leverage.

Existing Third-Party Services Agreements Shared by the Target and the Seller

If the seller and the target both depend on one of the seller's third-party services agreements, the target may be able to continue receiving services from the provider as a "service recipient" under the existing agreement, even after the buyer acquires the target. The seller would then invoice the target or the buyer for target's allocable share of the charges under the existing agreement.[3] This method has the benefit of preserving the value of the existing agreement, if it works. In considering this option, the parties should address questions such as:

- Does the seller have the right to designate the target or the buyer (as applicable) as a service recipient? If so, what are the associated costs (e.g., for set-up or third-party consents)?
- Will the terms of the existing services agreement meet the buyer's needs?
- Does the pricing permit the seller to allocate charges to the target or the buyer?
- Will the buyer have the right to require the seller to dispute charges or make claims for damages under the existing agreement?
- Will the buyer have the right to audit the provider? Audit rights may be required to comply with legal obligations or the buyer's policies.

- Who prevails if the buyer and the seller disagree on directions to be given to the provider (e.g., with respect to in-flight projects)?
- Which party will own the intellectual property (IP) developed by the provider in the performance of the services agreement?
- Will the seller be liable if the buyer fails to comply with the existing agreement? The risks of adverse consequences to the seller due to buyer noncompliance will be particularly troublesome if the existing agreement is critical to the seller's retained organization.
- Will the seller be liable to the buyer if the service provider fails to perform, or if the services are otherwise deficient? In other words, is the seller responsible for its third-party provider's services, or is the seller merely managing and passing through those services to the target or the buyer on an "as-is" basis?

Another approach is to negotiate a new contract with the provider to continue the service. This approach provides a much easier separation between the buyer and the seller and allows the buyer to assess the existing third-party provider against its competitors to obtain the most favorable pricing and other terms. However, this may result in the buyer losing value because the new services contract covers only its own volume. A new contract may also cause the seller to lose value because it may pay higher unit prices under the existing agreement (or even face termination or termination charges) because of the reduced volume. Time constraints often make this approach impractical.

In some cases, there is an easy path to obtaining a new contract with the service provider because the seller has a right to split the existing agreement in a way that preserves its value (i.e., "cloning"). Or, the seller may be able to create two new agreements that divide the service scope, revenue commitments, termination charges and other similar terms of the existing agreement (i.e., "cleaving").

Cloning can have unintended consequences. For example, it might have the effect of doubling minimum revenue commitments or of requiring the provider to dedicate a specific person or asset to multiple customers. Thus, cloning is generally used only for simpler services agreements.

Cleaving means reducing service volume baselines and minimum charges under both the existing agreement and the new agreement. But it also can mean allocating key personnel, intellectual property rights, rights to dedicated assets upon a termination and other key resources and assets between the existing and new agreements. New projects may also be required to separate service delivery facilities, teams and reporting capabilities for the buyer and the seller; to decouple the seller's confidential information from the buyer's confidential information; and to adapt to the buyer's unique needs or integrate with the buyer's systems.

Cleaving typically involves more negotiation than does cloning. The provider has likely scaled its service delivery organization for the combined volume under the existing agreement. As a result, the provider sees more economic benefit in providing services under two similar agreements, without the costs of negotiating a new agreement, than in any increase in per-unit charges that may result from the cleaving. At the same time, the service provider may see an opportunity to obtain provider-favorable terms and pricing in return for continuing to provide an essential service, particularly if the buyer has run out of time to find a different provider.

Steps that Potential Sellers Can Take to Prepare for Future M&A Transactions

Sellers can take steps to position themselves to maximize value and mitigate risk. These steps include:

- Developing an organization to support divestiture activities, with an "M&A Playbook" and a staff for supporting divested businesses.
- Maintaining a database of services agreements and the businesses that they serve.
- Ensuring that outside service providers are committed to (i) taking on work, shedding work, supporting divested businesses, and providing M&A support upon request; and (ii) permitting the seller to clone or cleave existing agreements.
- Ensuring that outside licensors, lessors and similar third parties have agreed to allow their software or assets to support divestitures, at least for a minimum time period.

- Including in the divestiture team, at an early stage, the people who will be responsible for arranging services to be provided by or for the seller.
- Analyzing the target's internal servicing capabilities, the services the target needs from shared contracts or from the seller's organization, any services the target provides to the seller's organization, the costs required to provide those services, the effect the divestiture will have on the seller's retained organization (including pricing impacts under existing services contracts), and how best to provide the needed services.
- Identifying projects under third-party services agreements that the buyer may not need and that should be put on hold pending a transaction.

Steps that Potential Buyers Can Take to Prepare for Future M&A Transactions

Buyers also can take steps to maximize value and mitigate risk. These include:

- Incorporating rights to expand services and obtain acquisition support into third-party services agreements.
- Developing an organization to support acquisition activities, with an "M&A Playbook" and a staff with responsibility for supporting acquired businesses.
- Identifying in advance any services that will need to be replicated or replaced, as well as the means to mitigate the impact of service failures.
- Documenting services and associated service levels that the buyer's own internal services organizations can perform for acquired businesses, and determining the expected timing needed to bring those services online for a target.
- Assigning to the acquisition team, at an early stage, the people the buyer will use to procure the needed services from a third party.
- Commencing negotiations with third-party service providers as promptly as possible.
- Leveraging best practices developed in outsourcing and large-scale agreements for critical services.

Conclusion

Dramatic changes in the ways that companies source core business functions require timely, substantial attention to services agreements in M&A transactions. Leaving these issues to the end of a deal can cause delays, squander value, increase risk and lead to disputes. The best time to begin developing services agreements is well before the target is identified. Integrating the approaches described in this article into contracting policies and overall M&A strategies and approaches can help both buyers and sellers to maximize value and mitigate risk in M&A transactions. ◆

Endnotes

1 In keeping with current terminology for strategy consultants and technology architects, this article uses the word "services" broadly to include back-office processes, functions and capabilities, including all of the underlying people, systems, technology, facilities and other resources, along with the set-up, operation and disengagement of those services.

2 In some cases, leaving service agreements to a later stage in the M&A process is a conscious decision driven by the seller, the buyer or both. Factors such as confidentiality, the buyer's familiarity with the target, limitations on internal resources and cost can drive such a decision.

3 For simplicity, we are assuming that the existing agreement is between the third-party provider and the seller. Typically, the principles stated here would also apply if the agreement were between the third-party provider and the target.

Identifying and Resolving US Export Control Issues in Outsourcing Deals

Carol J. Bilzi
Rebecca S. Eisner
Marina G. Aronchik
Kristy L. Balsanek

Carol J. Bilzi
Washington DC
+1 202 263 3202
cbilzi@mayerbrown.com

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

Marina G. Aronchik
Chicago
+1 312 701 8168
maronchik@mayerbrown.com

Kristy L. Balsanek
Washington DC
+1 202 263 3286
kbalsanek@mayerbrown.com

US domestic companies working to outsource functions to foreign suppliers or domestic suppliers with foreign locations and workers face a variety of compelling regulatory challenges. Among the more significant of these is the need to comply with US export controls. This article brings the issue of compliance with US export control laws into sharp focus. It clarifies salient features of the nation's export control law from a business perspective and recommends specific strategies that companies can use to define and address key compliance needs and to mitigate risk in the context of their outsourcing deals.

Compliance with US export control laws poses crucial challenges in outsourcing deals. Failure to comply with the US export control laws can have serious consequences for companies, including substantial monetary fines, loss of export privileges, disruption of business operations and reputational damage.

To minimize liability, US companies should determine at the outset whether their outsourcing deals involve any items, such as certain dual-use products, software or technology, or defense articles or services that the United States controls for export to foreign destinations or foreign nationals. If export restrictions apply, the company may need to obtain a license before exporting any items as part of the outsourcing transaction. License applications can take several weeks to complete and, in certain instances, may significantly delay an outsourcing deal if compliance issues are not adequately addressed at the outset.

Although it is critical for a US company to resolve issues arising under US export control laws before exporting or providing access to controlled items, it is often difficult to identify such issues in complex outsourcing deals. For example, export issues may arise in the outsourcing of (i) litigation support functions, in which foreign nationals are provided access to documents containing technical data, drawings and blueprints related to the manufacture of a product at issue; (ii) back-office support functions requiring the transfer of hardware and encryption software overseas; (iii) software application support and maintenance, where foreign nationals will have access to applications; (iv) research and

Although it is critical for a US company to resolve issues arising under US export control laws before exporting or providing access to controlled items, it is often difficult to identify such issues in complex outsourcing deals.

development to a joint venture located abroad, involving the transfer of US origin technology; (v) the preparation of patent applications when the US company provides technical data relating to its innovations to foreign nationals overseas; or (vi) the management of a data room by a non-US company for purposes of merger and acquisition due diligence, when a US company electronically transmits technical data to a server located outside the United States.

This article describes an approach companies can use to identify and resolve US export control issues in their outsourcing deals. Under this approach, the US company should first identify US export control issues during the early stages of an outsourcing deal. It should then negotiate and draft appropriate provisions in the outsourcing agreement to ensure compliance with applicable US export control laws and appropriate allocation of risk and responsibility with respect to such compliance. The article concludes with a summary of specific steps that a company can follow to help determine whether its outsourcing project raises export compliance issues and, if so, what it must do to address those issues.

Identifying US Export Control Issues in Outsourcing Deals

IS THERE AN EXPORT?

The first step in identifying US export control issues in an outsourcing deal is determining whether any US-origin items (which include products, software, technology and, in some cases, services) will be exported and/or re-exported within the meaning of US export control laws. The primary regulations governing the exportation of US-origin items are the International Traffic in Arms Regulations (ITAR) and the US Export Administration Regulations (EAR).

Although most people think of an export as the physical shipment of a product to a foreign destination, "export" within the meaning of the ITAR and the EAR covers a far broader range of activities and items, including:

- Hand-carrying controlled products abroad, traveling abroad with laptops loaded with controlled software and/or technology, or traveling to assist foreign customers with testing and/or repairs using controlled products.
- Shipping US-origin items from one foreign country to another (called a "re-export").
- Sending, transmitting or disclosing software or technology via mail, email, Internet, server access, facsimile, telex, video conference, webinars and/or telephone conversations.
- Disclosing to foreign nationals located in the United States certain technology through visual inspection or verbal exchange.
- Instructing or training foreign nationals in the design, production, operation or use of controlled products.
- Transferring registration, control or ownership to a foreign person of any ITAR-controlled aircraft, vessel or satellite, whether in the United States or abroad.
- Performing a "defense service" on behalf of, or for the benefit of, a foreign person whether in the United States or abroad.

[A]n export can occur even within the borders of the United States when certain controlled technology or source code is provided to a foreign national located in the United States.

It is particularly important in the outsourcing context to determine whether any "technology" or software will be exported. As illustrated by the examples above, an export can occur even within the borders of the United States when certain controlled technology or source code is provided to a foreign national located in the United States. US export control laws provide specific definitions of "technology." For example, under the EAR, "technology" is limited to specific information necessary for the development, production or use of a controlled product, software or technology, such as technical data (e.g., engineering designs and specifications, blueprints, plans, diagrams, models, manuals and written or recorded instructions) or technical assistance, including instruction, skills training, working knowledge and consulting services.

The release of such technology is "deemed" to be an export to the home country of the foreign national, even if such foreign national is located in the United

States. In this context, a "foreign national" is an individual who is not a US citizen, lawful permanent resident, political asylee, refugee or other type of protected individual. A company "releases" technology when it (i) makes such technology available to foreign nationals for visual inspection (such as reading technical specifications, plans or blueprints); (ii) orally exchanges such technology with a foreign national; or (iii) makes such technology available to a foreign national by practice or application under the guidance of persons with knowledge of the technology.

A "deemed" export, therefore, may occur in a wide range of scenarios, including where a company allows a foreign national to access technology or gives a foreign national the capability to develop or replicate an encryption item that is subject to export restrictions. Depending upon the nationality of the person receiving the technology and the type of technology involved, the outsourcing company may need to obtain an export license before releasing such technology to a foreign national.

ARE THE ITEMS TO BE EXPORTED SUBJECT TO CONTROL?

Once a US company determines that its outsourcing project involves an export, the company should consider whether the items are controlled for export under the ITAR or the EAR. The ITAR, administered by the US Department of State, Directorate of Defense Trade Controls (DDTC), applies to "defense articles" and "defense services."

Defense articles are items listed on the US Munitions List (USML), which is subject to change depending on US national security concerns and revisions to technical parameters. They may also include items that are specifically designed, developed, adapted or modified for military use. Any manufacturer or exporter of defense articles or services listed in the USML must register with DDTC.

Defense services include assisting foreign persons in the US or abroad in the design, manufacture or use of defense articles, furnishing technical data to foreign persons in the US or abroad and military training of foreign forces. Items controlled under the ITAR are described in various categories of the USML, and include firearms, weapons, satellites, military vehicles, toxicological agents, and military electronics.

The EAR, administered by the US Department of Commerce, Bureau of Industry and Security (BIS), applies to products, software and technology with both commercial and military use (commonly referred to as "dual-use" goods). Items controlled under the EAR are listed on the Commerce Control List (CCL).

The CCL contains five-digit alphanumeric Export Control Classification Numbers (ECCNs) for identification of specifically described items and their reasons for control. An EAR99 basket number is used for any items not specifically described.

The CCL includes ten product categories covering such items as materials, chemicals, electronics, computers, telecommunications, information security, navigation and avionics. Encryption items, including encryption technology and hardware and software with encryption functionality, are an important category of items on the CCL because most business software contains encryption capabilities and, therefore, outsourcing projects often involve the export of encryption items. The export controls related to encryption items are particularly complex and must be analyzed on a product-by-product basis.

WHAT IS THE DESTINATION AND END-USE OF THE ITEMS TO BE EXPORTED?

The third step a US company should take to determine whether its outsourcing project raises US export control issues is to identify the destination and end-use of controlled items outside of the United States. In addition, the company should identify any foreign nationals, including employees, consultants, contractors, guest researchers and visitors, to whom the items may be released in the United States.

Whether the export of an item controlled under the EAR requires an export license depends upon the ultimate destination and end-use of that item. If an item is controlled for export under the ITAR, it will need a license for all destinations and end-uses, unless a license exception applies. In addition, US sanctions laws prohibit US companies from any business dealings with certain countries, individuals and entities. US laws also prohibit the export of US-origin items to certain prohibited countries and parties.

Addressing Issues Relating to US Export Control Laws While Negotiating and Drafting an Outsourcing Agreement

If an outsourcing project raises US export control issues, there are generally three steps the US company should take to ensure compliance with applicable export laws. First, if the classification, destination, end-use or end-user of items that the US company will export as part of its outsourcing transaction requires an export license, and if no license exception is available, then the company must apply to the BIS or the DDTC for a license. Such a license must be obtained in advance of any exportation. License applications may take between four and twelve weeks for approval. Typically, any license that is granted will have a duration of about two years.

Second, the US company needs to create an export control policy, including a technology control plan for personnel working on the project, to ensure appropriate access to controlled items. Finally, and once work under an outsourcing agreement commences, the US company must continue to ensure compliance with all US export license obligations. It must also maintain all classification and export documentation for record-keeping purposes, confirm the export license expiration date, and prepare necessary renewal applications.

When negotiating an outsourcing agreement that raises US export control issues, the US company should consider whether it will maintain the above obligations related to ensuring compliance with US export control laws, or if it will delegate such responsibilities to the supplier. As a general matter, the "exporter of record" is ultimately responsible for compliance with US export control laws. The exporter of record is the person in the United States who has the authority of a principal person in interest to determine and control the sending of items out of the United States. Often, each party to an outsourcing agreement assumes the export compliance obligations for any items it supplies to the project that will be exported.

Alternatively, the US company may consider delegating to the supplier the responsibility to comply with applicable export restrictions, but that will not completely relieve the US company of its legal obligations under the EAR or the ITAR. The advantages of this approach include short-term cost savings for the US company, such as elimination of the need to classify items, to determine whether an export license is needed, or to apply for a license prior to commencement of work under an outsourcing agreement. Another reason to require the supplier to handle this responsibility is that it will be easier for the supplier to maintain the technology control plan mentioned above, as the supplier is in control of supplier personnel who access and use the technology.

However, the US company will face significant risks in the event that the supplier fails to fulfill its obligations with respect to ensuring compliance with US export control laws. The company may be able to recover from the supplier the amount of monetary fines imposed by the US government. But adequate remedies for the company's potential loss of export privileges, disruption of business operations and reputational damage stemming from its failure to comply with export control laws are difficult to ascertain and recover from the supplier.

In the event that, after weighing these considerations, the US company prefers to impose on the supplier the burden of ensuring compliance with US export control laws, the relevant contract provision should reflect certain key understandings. These include:

- Certain items or transactions under the outsourcing agreement may be subject to US export controls and/or sanctions.
- Neither party to an outsourcing transaction will directly or indirectly export or re-export any items in violation of applicable US export control laws.
- The supplier will identify the specific export control status of, and will be responsible for obtaining all necessary export authorizations for, the export or re-export of any items under the outsourcing agreement.
- The supplier will ensure that its subcontractors obtain all necessary export authorizations and maintain the necessary internal compliance controls.
- The supplier will agree not to subcontract any portion of the outsourcing services to prohibited countries or entities and will not employ nationals of such prohibited countries to provide services to the US company.
- The supplier will be responsible for implementing all necessary internal compliance controls, including the technology control plan.

- The supplier will provide the US company, at the company's request and at least annually, a certification of compliance with US export control laws.

[I]t is crucial for the US company to secure a commitment from the supplier to provide all information necessary for the company to achieve and maintain compliance with US export control laws.

If the US company decides, either at the outset of negotiations or as a result of a compromise with the supplier, to maintain primary responsibility for ensuring compliance with US export control laws, the company should nevertheless draft the relevant provisions of the outsourcing agreement with care. For example, it is crucial for the US company to secure a commitment from the supplier to provide all information necessary for the company to achieve and maintain compliance with US export control laws. This information should include the countries of citizenship for all supplier personnel who may be performing services under an outsourcing agreement, whether in the United State or from abroad.

Steps to Determine Whether Your Outsourcing Project Raises Export Concerns

The checklist below will help US companies to identify and resolve US export control issues in an outsourcing deal:

1. Determine whether the outsourcing project involves an export of products, source code, software, technology, defense articles or defense services.
2. Classify each item with the appropriate ECCN or USML Category.
3. Determine the item's export destination and end-use.
4. Determine whether any controlled technology, source code, defense articles or defense services will be released to foreign nationals in the United States.
5. Screen all parties to the transaction against the list of prohibited persons maintained by the US government.
6. Determine whether an export license is required. If so, confirm whether a license exception applies.
7. Ensure that contractual language adequately covers the responsibilities of the parties, given applicable export controls and licensing requirements.
8. Obtain an export license when necessary.
9. Create, design and implement a US export control policy with procedures specific to technology, security, record-keeping, training and reporting.
10. Create a technology control plan for personnel working on the project to ensure appropriate access to controlled items, including separate work areas with restricted access control and separately controlled technology within the server network, password protection for individual documents, protected databases and other computer security measures.
11. Train all relevant persons in compliance with US export control laws.
12. Comply with all export license conditions.
13. Ensure that the exporter or its agent adequately completes and submits all required shipping documentation and Automated Export Sytem (AES) records.
14. Maintain all classification and export documentation for record-keeping purposes.
15. Confirm the export license expiration date and prepare necessary export license renewal applications.

Conclusion

The specific nature of export restrictions arising in a complex outsourcing project drives the overall strategy and the time necessary for the resolution of such issues. Issues can arise with any company employing or interacting with foreign nationals wherever located, or engaging in business activities outside the United States. Early identification of challenges arising from US export control laws and effective allocation of responsibility for resolving compliance-related concerns will help the company select the most appropriate supplier for a particular outsourcing need. Proactive consideration of the laws will also help the company reach early internal alignment on this important issue, set up necessary internal controls to ensure compliance with US export control laws, and avoid delays in the negotiation of an outsourcing agreement and commencement of work under the agreement. ◆

New Requirements for Data Protection Officers in Germany

Tim Wybitul

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

Germany is noted for its rigorous efforts to protect sensitive personal information in the course of business operations. Today, for example, many companies that operate in Germany are required to appoint highly qualified data protection officers responsible for ensuring the security of data and the integrity of corporate data management procedures. This article describes the roles and responsibilities of the position and helps managers to determine if their organizations must employ data protection officers under German law.

Many enterprises in Germany, including subsidiaries of international companies, are obligated to formally appoint a data protection officer (*Datenschutzbeauftragter*, or "DSB"). However, German law governing this area is not always clear, leaving many small and mid-sized companies wondering whether they are legally obligated to do so. Despite this ambiguity, failure to comply with the law can have significant ramifications, as mistakes made with regard to data protection can result in administrative fines and substantial damage to corporate reputation.

German data protection laws are also somewhat vague regarding the necessary qualifications and skills of DSBs. Further, the internal structures and support an enterprise must provide to its DSBs in order to comply with German law are not precisely specified. Appointing a DSB who is not sufficiently qualified, or failing to provide that person with adequate structures or resources, may result in fines of up to EUR 50,000.

German data protection authorities have published a resolution regarding minimum requirements for DSBs. The so-called "Duesseldorfer Kreis" has stipulated the required skills and framework for the proper work of DSBs in Germany. The Duesseldorfer Kreis is the joint coordination body of German data protection authorities at the state level, and its resolutions have considerable influence over enterprises operating in Germany.

Criteria for Appointing a DSB

Section 4f, Subsection 1 of the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, or "BDSG") requires privately held companies to appoint DSBs if they permanently employ ten or more persons in the automated processing of personal data—the use of computers to process automated personal data is also covered. This obligation also applies to companies that employ 20 or more people to work with non-automated data processing or to process data that infringes so intensely on personal rights

that, pursuant to Section 4d, Subsection 5 of the BDSG, the DSB is statutorily required to conduct a formal prior examination of the permissibility of this data processing. This can be the case when particularly complex processing systems or newer technologies are used.

Primary responsibility for adhering to the provisions of the BDSG lies with the company's management. If, for example, the managing directors of a GmbH (*Gesellschaft mit beschränkter Haftung*, similar to a Limited Liability Company) do not fulfill the requirements for appointing a DSB, then each managing director risks administrative fines of up to EUR 50,000. While the responsible agencies do not normally impose the maximum fines, additional administrative fines can be imposed against the company itself pursuant to Section 130 of the German Administrative Offenses Act (*Ordnungswidrigkeitengesetz*).

Mandated DSB Responsibilities and Qualifications

The BDSG stipulates that the DSB must "work toward" fulfilling the provisions of the BDSG and other German data protection laws. One of the DSB's many tasks is to advise the company's management with regard to potential data privacy breaches or data protection compliance issues and to point out where data privacy could be improved.

Irrespective of the branch or size of the company in question, each DSB must have profound knowledge of Germany's data protection laws.

Section 4f, Subsection 2 of the BDSG states that in order to adequately complete these tasks, the DSB must, at a minimum, fulfill several legal, technical and organizational qualifications. The BDSG does not clearly specify these qualifications, but the Duesseldorfer Kreis has made clear that DSBs must demonstrate competence in several key areas of practice.

KNOWLEDGE OF DATA PROTECTION LAW

Irrespective of the branch or size of the company in question, each DSB must have profound knowledge of Germany's data protection laws. This includes knowledge of the constitutional rights of individual data subjects and of the company's employees.

Additionally, the DSB must be aware of those BDSG provisions that are applicable to her or his enterprise. Among other things, these provisions include specific technical and organizational stipulations regarding data security (e.g., Section 9 BDSG).

In addition, the DSB must be familiar with the accepted principles of data protection in Germany. These include: (i) the principle of adequacy and the obligation to avoid and restrict personal data where possible, pursuant to Section 3a of the BDSG; (ii) the principle that data may generally not be processed unless permitted by a legal justification under Section 4, Subsection 1 of the BDSG; (iii) the principle that personal data may only be collected for specified, explicit and legitimate purposes and may not be processed in a way incompatible with those purposes (*Zweckbindungsgrundsatz*); and (iv) the principle of transparency, according to which data subjects must, to the extent possible, be informed of the processing of their data.

BUSINESS-SPECIFIC KNOWLEDGE

Data protection regulators may require other qualifications of the DSB, depending on the business sector in which she or he operates, the employing company's size or IT infrastructure and the nature and sensitivity of processed data.

Comprehensive knowledge of special legal provisions pertaining to data protection is required of the DSB if this is relevant to the employing company. For instance, the DSB of a financial institution should be aware of Section 25c of the German Banking Act (*Kreditwesengesetz*); in turn, the DSB of an insurance company must be well acquainted with Section 80d of the German Insurance Supervision Act (*Versicherungsaufsichtsgesetz*).

Furthermore, the Duesseldorfer Kreis demands knowledge of information, telecommunications and data security technology. Among other things, these areas of knowledge refer to the physical security of IT structures, cryptography, network security, spyware and adequate protection measures. In some business sectors or companies, understanding of practical data protection management may be necessary as well.

The Duesseldorfer Kreis's resolution lists examples of such practical skills, including executing controls,

advising company management and coaching employees, providing data protection strategies and recording data protection-relevant company activities. Moreover, the resolution requires the creation of process registers (*Verfahrensverzeichnisse*) pursuant to Section 4g, Subsection 2, Sentence 2 of the BDSG. It also demands knowledge of log file analysis and risk management and of the analysis of security concepts, works agreements (*Betriebsvereinbarungen*) and video surveillance. Finally, the resolution requires the DSB to cooperate with employee representative bodies.

If a company is uncertain whether it is obliged to appoint a DSB, it can seek advice from the responsible German state data protection supervisory authority. In case of doubt, this is the best procedure to follow.

There may be scenarios in which a DSB must demonstrate basic economic knowledge. Unfortunately, the Duesseldorfer Kreis does not provide examples that specify when this qualification is applicable. Moreover, the data protection authorities stipulate that a DSB should have adequate knowledge of the enterprise's technical and organizational structure. Hence, the DSB should be aware of relevant organizational and process charts and of the internal organization of the enterprise.

Regulated Data Processor Categories

Germany's data protection regulators take a broad view when defining the categories of employees to which the BDSG applies. To a large extent, the definition encompasses every employee who works with a computer to compile, process or use personal data.

Thus, it is not only IT technicians who are included in this group, but also clerks who have computers available to them. Employees in personnel or financial areas, as well those who process orders, generally work with personal data in the scope of automated data processing and, consequently, fall under Germany's data protection regulations.

This broad definition also applies to employees who, for example, enter personal data in a bank's branch office, an insurance company's office or an HR department. In this context, it is irrelevant whether the data is entered by a bank teller, by a customer service representative when opening a new account or placing an order, or by a person working in a client's office. Automated data processing within the meaning of the BDSG also applies if a person enters data into his or her own computer and later transfers that data to the employer's system.

If a company is uncertain whether it is obliged to appoint a DSB, it can seek advice from the responsible German state data protection supervisory authority. In case of doubt, this is the best procedure to follow.

When Managers Must Assume DSB Responsibilities

Regardless of the number of persons involved in an organization's data processing functions, all companies that process data posing special risks to the rights and freedoms of their employees or business partners must appoint a DSB. According to specialized literature, examples of such risky functions include video surveillance and chip card use, as well as procedures that are generally non-transparent to the affected persons. Companies that are active in the areas of market or opinion research or that transfer data as a matter of business (e.g., credit information agencies) must always appoint a DSB.

The BDSG's provisions are applicable even if a company's data processing functions involve fewer than the minimum number of employees stipulated as a criterion for appointing a DSB.

The BDSG's provisions are applicable even if a company's data processing functions involve fewer than the minimum number of employees stipulated as a criterion for appointing a DSB. In this case, management must take on the DSB's tasks. Furthermore, companies that are not required to appoint a DSB must report all automated data processing procedures to the responsible data protection supervisory authority prior to their implementation. If management does not abide by this obligation, then every manager is liable to receive an administrative fine of up to EUR 50,000. As the obligation to report all automated data processing procedures is fairly complex, it may be wise to appoint a DSB for that reason alone.

In essence, companies that have not yet appointed DSBs should thoroughly examine whether they are

obligated to do so. Experience has shown that many companies are not aware of their statutory obligations. However, ignorance of the law is no defense; and German courts generally consider such ignorance to be legally unremarkable (because avoidable) mistakes of law. Conversely, if a company appoints a DSB prior to the supervisory authorities' discovery of previous non-compliance issues, then it is extremely unlikely that a punishment will ensue.

Requirements Regarding DSB Independence

The DSB fulfills a special role in a German company. In order to enable the DSB to autonomously fulfill the role's supervisory and advisory functions, she or he must report directly to the company's management (Section 4f, Subsection 3, Sentence 1 BDSG). The DSB, moreover, must not be bound by company instructions regarding questions of data protection (Section 4f, Subsection 3, Sentence 2 BDSG). In addition, the DSB's independence is safeguarded by mandatory dismissal protection.

Companies must enable their DSBs to fulfill their tasks and responsibilities without encountering conflicts of interest. Companies must safeguard this protection by implementing organizational and contractual provisions that are published both internally and externally.

Pursuant to the BDSG (Section 4f, Subsection 3, Sentence 3 et seq.), a company may not discriminate against an employed (internal) DSB based on the fulfillment of his or her functions. According to the data protection authorities, this protection also applies to the appointment of an external DSB (e.g., a specialized lawyer).

The DSB's service contract must generally safeguard the autonomous fulfillment of her or his legal assignments. This can be accomplished by agreements between the company and its DSB on respective notice periods, payment modalities, disclaimers and documentation obligations. The Duesseldorfer Kreis recommends a contractual period of at least four years, or a minimum of two years when initially appointing an external DSB. Companies must ensure that external DSBs are enabled to provide their services in an adequate manner and, as appropriate or necessary, to deliver their services onsite at the company itself.

The BDSG provides that companies must generally pay for the training and continuing education of their DSBs. Hence, if a company appoints an employee as DSB, it must bear the expenses for the required training. However, where an external DSB is appointed, training costs may be part of the agreed contractual compensation. The considerable training and education requirements mandated by the data protection authorities may increasingly lead companies to appoint external DSBs, rather than internally employed DSBs, as a cost-saving measure.

Required Organizational Framework

The data protection authorities provide several specifications regarding internal corporate structures that are necessary to fulfill BDSG mandates. For example, the enterprise must authorize its DSB to enter all relevant locations and to have access to all documents necessary to complete the tasks. In addition, the DSB must be part of all data-related project proposals and decision processes. This could result in a development where the internal position and the relevance of the DSB may be increased.

Consequences of Noncompliance

The basic requirements of DSBs that are now set forth in the BDSG were not always fulfilled when data privacy controls were conducted in German enterprises by data protection authorities. Under current German law, however, minimum DSB qualifications and standards of independence have been defined more precisely.

Failure to meet these specifications may pose significant risks for enterprises operating in Germany. A company that appoints a DSB whose qualifications, reliability or position within the enterprise do not comply with the legal requirements may be punished with administrative fines pursuant to Section 43, Subsection 1, Number 2 of the BDSG. Moreover, German data protection authorities have a strong tendency to review corporate violators of the BDSG more closely for additional data protection infringements.

Summary and Recommendations

The demands of the German data protection authorities are extensive. In particular, the professional knowledge and skills required of DSBs mandates a high degree of specialization and training. If the qualifications of the DSB are deemed insufficient, high administrative fines and serious damage to the corporate violator's reputation may ensue.

Germany's data protection authorities have determined that the functions and responsibilities of a company's DSB are influenced by a variety of factors, including company size and organizational structure, business- and sector-specific considerations, and the nature and sensitivity of the data that is processed. Consequently, large enterprises and companies that process sensitive data or considerable quantities of data must fulfill stringent regulatory standards.

Enterprises operating in Germany, then, are generally well-advised to appoint DSBs who fully satisfy the nation's demanding legal requirements. Moreover, they should take vigorous and continuous action to ensure that their internal structures are compliant with the specifications issued by German data protection authorities. ◆

European and German Privacy Laws and Cross-Border Data Transfer for E-Discovery in the United States—Are These Systems Compatible?

Mark C. Hilgard
Tim Wybitul
Andrea Patzak

Mark C. Hilgard
Frankfurt
+49 (0)69 79 41 2161
mhilgard@mayerbrown.com

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

Andrea Patzak
Former Associate

European companies involved in litigation in the United States often struggle to balance conflicts between EU and US approaches to data privacy protection. Although European companies must comply with their national regulations regarding data privacy in court proceedings, they may be obliged to disclose information protected by EU statutes in the course of a US litigation. This article presents the US and EU judicial perspectives toward data protection and offers practical solutions to help European companies engaged in US litigation to fulfill court-ordered disclosure requirements while simultaneously maintaining EU data privacy standards.

Introduction to US Discovery and European Data Privacy

It is not unusual for companies doing business in Europe to be involved in US litigation proceedings. In the course of such litigation proceedings, US courts may require companies to disclose certain information, including the personal data of employees, customers and other persons.[1] European data privacy law generally prohibits the transfer of personal data to another legal entity, not to mention if such an entity is domiciled in another country.[2] This prohibition leads to a potential conflict between the European and US systems. It also causes difficulties for companies facing an obligation to transfer personal data when defending against or raising claims in a US trial while simultaneously having to comply with European data privacy laws.[3]

Failure to comply with requests for such information can lead to companies facing severe sanctions.[4] On the other hand, violations of European data privacy laws following the disclosure request may lead to damage claims, fines or, in severe cases, criminal prosecution.[5] This article aims to suggest possible solutions for that dilemma.

The United States and Europe take differing approaches with regard to discovery and data privacy. While data privacy plays an important role in Europe, discovery is not a significant issue. Conversely, in the United States, discovery is a significant component of litigation proceedings and there is less protection of data used in the private sector.[6]

Some civil law countries, including Germany, have introduced laws intended to restrict cross-border discovery of information for disclosure proceedings in foreign jurisdictions (so-called "blocking statutes").[7] In some cases, US courts have rejected the idea that such provisions provide a defense against discovery in relation to US

litigation.[8] However, in other cases, US courts have acknowledged the foreign party's interest in obeying its national law and have agreed that this supersedes the opposing party's interests in requesting such evidence.[9]

Is There a Justification for Data Disclosure?

In order to understand the conflicting approaches in the United States and Europe in regards to data privacy laws, it is necessary to explain the context of data privacy laws in Europe.

In the European Union, as well as in the European Economic Area, data privacy law is based on European Directive 46/95/EC, dated 24 October 1995 (the "Directive"), which deals with the protection of individuals with regard to the processing of personal data and the free transfer of such data. The Directive was implemented by national data privacy laws, such as the German Federal Data Privacy Act (*Bundesdatenschutzgesetz* or BDSG) and the British Data Privacy Act of 1998. Hence, EU Member States' national laws on data privacy are based on the same Directive and, therefore, on the same principles. Nevertheless, they vary in certain aspects.

In practice, the data subject's consent can rarely be used as a valid justification for transfer; the law sets strict requirements for a declaration of consent and the sheer volume of data eventually requested in disclosure proceedings often makes it nearly impossible to procure the written consent of every person whose data might be concerned.

The Directive

Pursuant to the general principles established by the Directive, collecting, processing and using personal data is permitted only if the data subject has consented, or if there is a statutory justification. The same holds true for the transfer of personal data to a third party. Moreover, additional requirements have to be met if personal data is transferred to third parties located outside the European Union or the European Economic Area.

In practice, the data subject's consent can rarely be used as a valid justification for transfer; the law sets strict requirements for a declaration of consent and the sheer volume of data eventually requested in disclosure proceedings often makes it nearly impossible to procure the written consent of every person whose data might be concerned. Hence, parties regularly need to find a statutory provision that justifies the data transfer required for an e-discovery.

When is processing personal data permitted?

Pursuant to Article 7 (c) of the Directive, the data controller may process personal data if processing is required in order to comply with other legal obligations. However, disclosure in e-discovery proceedings is based on US e-discovery rules. Such foreign law statutes, however, do not constitute a legal obligation within the meaning of Article 7 (c) of the Directive. Hence, Article 7 (c) of the Directive does not provide for a justification to process personal data in e-discovery proceedings.

However, Article 7 (f) of the Directive allows for the processing of personal data if such processing serves the legitimate interests of the data controller and if these interests are not outweighed by fundamental rights and freedoms of the data subject. Consequently, Article 7 (f) of the Directive requires a thorough balancing of the legally protected interests of the data controller and those of the data subject.

Disclosure of personal data during litigation would certainly serve the justified interests of the data controller if that individual or entity is involved in litigation. Therefore, the transfer and use of third-party data may generally be possible before European courts.[10] However, that provision does not generally permit the transfer of personal data to US courts, as additional measures are required to ensure an adequate level of protection for a data transfer to parties outside the European Union or the European Economic Area.

May personal data be transferred to the United States?

In the course of pre-trial e-discovery proceedings, Article 26 (1) (d) of the Directive might come into play. This provision permits the transfer of personal data without the requirement to guarantee an adequate protection level if the transfer is necessary "for the establishment, exercise or defense of legal claims."

It is worth noting that, for instance, the English-language version of the Directive does not require the establishment, exercise or defense of legal claims to take place in a specific forum, while other language versions,[11] such as the German version of the Directive, require "court proceedings."

The German-language version of Article 26 (1) (d) of the Directive has been implemented into German law in Section 4c Subsection 1 Sent. 1 No. 4 BDSG. Germany, like several other countries, has chosen to implement a stricter version of the Directive, allowing for a transfer of personal data to a party in a country outside the European Union without any further measures to guarantee an adequate protection level *only if* "the transfer is required … for the establishment, exercise or defense of legal claims before courts." Hence, it is questionable whether Article 26 (1) (d) of the Directive and Section 4c Subsection 1 Sent. 1 No. 4 BDSG also cover pre-trial disclosure proceedings.

A disclosure request by a US court seems to be incompatible with EU and German privacy laws. However, considering the economic importance of requesting or producing documents in e-discovery for European parties, companies are advised not to completely refuse a disclosure request on the grounds of existing national data privacy legislation. Often, a better alternative is to find a privacy-compliant approach to the requested disclosure.

In support of this view, it could be argued that the legal interests of a party subject to e-discovery are exactly the same as if this party actually litigated before a US court. However, Article 26 (1) (d) of the Directive forms an exception to data privacy that has to be interpreted narrowly so as not to circumvent the European data privacy standard.[12]

Discovery in the United States is typically conducted prior to the beginning of the actual trial proceedings. It is aimed at gathering evidence in preparation for the actual trial and does not, typically, take place *before the court*. As the pre-trial gathering of evidence is not a familiar element of the German civil procedure law, it can be assumed that an exception provision is not intended to cover such unknown pre-trial proceedings.

According to the guiding principles of avoiding data transfer (pursuant to Section 3a BDSG) and limiting the processing of data to a specific purpose, data handling must be avoided if it is not required.[13] Therefore, applying the exception would contradict German data privacy law standards. That leads to the restrictive interpretation of the exception regulation, as it cannot justify any transfer of data to the United States in the course of pre-trial discovery proceedings.[14]

The Exception and Data Privacy Principles

A disclosure request by a US court seems to be incompatible with EU and German privacy laws. However, considering the economic importance of requesting or producing documents in e-discovery for European parties, companies are advised not to completely refuse a disclosure request on the grounds of existing national data privacy legislation. Often, a better alternative is to find a privacy-compliant approach to the requested disclosure. Such a privacy-compliant solution might be found by considering the background and the purpose of the exception provision detailed in Section 4c Subsection 1 Sent. 1 No. 4 BDSG.

What are a data recipient's obligations?

Public accessibility of European documents produced during US e-discovery proceedings is quite problematic from a European privacy law perspective.[15] In a German scenario, the documents produced as evidence in discovery proceedings are only accessible to persons attending the court proceeding itself (*Gerichtsöffentlichkeit*),[16] and decisions are only published in anonymous form.[17] In the United States, however, decisions, writs and protocols in current proceedings can be accessed by anyone worldwide. Documents are even made public over the Internet.

This demonstrates that the recipients who are entitled to receive the documents, including personal data, are not able to protect the personal data against any further transfer or public access. Furthermore, the recipients are generally not able to guarantee that the data is only used during, and for the purpose of, the respective litigation proceedings, or that it is only processed as much as necessary. Therefore, when transferring data, additional measures should be implemented to guarantee that the data is not processed outside the discovery.

Which data can be transferred?

Another important point is that only data that is necessary for the support of the claim may be transferred. Many provisions in the German privacy law permit data processing only if it is required for the specific purpose set out in the respective exception provision, Section 4c Subsection 1 Sent. 1 No. 4 BDSG. Therefore, this principle should be considered as a general restriction relative to data transfer in e-discovery.

"Required"—Overriding Interests

Generally, the exception provision permits a data transfer if such transfer is *required* to support legal claims before German, European or other courts. The provision describes an exception where the data subject's interests are minor and subordinate to the justified interests of the parties involved in litigation.[18] The BDSG grants the effective prosecution of claims that supersede the data subject's interests.[19] Therefore, the word "required" does not require any additional assessment if the party transferring the data has interests that override the interests of the data subject. The principle of proportionality acts as a guideline for the permitted type and scope of data transfer.[20]

Definitions of "Required"

As a guiding principle, the criterion "required" has to be interpreted restrictively. Although the exception provision suggests that there is a general option to transfer personal data to countries outside the European Union for litigation purposes, information required under US law will not automatically be held as required within the meaning of Section 4c Subsection 1 Sent. 1 No. 4 BDSG.

The aim of the discovery process in the United States is to ensure that the parties to litigation proceedings have access to required and relevant information for their cases, given the rules and procedures of the jurisdiction in which the litigation takes place.[21] Discovery is a fundamental part of the litigation process in common law jurisdictions, but the scope of what is required for discovery differs greatly between common law and civil code jurisdictions. The European and German understanding of discovery in trials varies significantly from the understanding of discovery under US law. Accordingly, it must be assumed that US courts would prefer a wide interpretation of "required." From a German law perspective, however, one would have a very restricted understanding of what documents should be disclosed under the US procedures, and the scope of required data would be limited and concentrated.[22] In the German legal context, "required" is interpreted as "mandatory" and does not merely mean "useful."[23]

Predominant Understanding

Some data privacy analysts state that the US perspective should be decisive. They argue that, as the German exception provision generally allows the transfer of data required in litigation, the clause should be interpreted to allow the transfer of required data under the applicable law. Thus, if a company is involved in litigation in the United States, then the general meaning of "required" should be defined by US law.[24] That perspective should not be applied, however, in jurisdictions where fundamental principles of data privacy are not respected or enforced. In such cases, interpretation of the term "required" according to applicable law should be restricted.

This view complicates the application of the exception that should allow a data transfer. First, "required" is more a factual criterion than a legal interpretation. In addition, it is difficult to define which principles are to be considered fundamental.

In concert with the principles of data reduction and data economy pursuant to Section 3a BDSG, the principle of proportionality generally serves as a guideline according to which data may be processed. This principle would apply here and would restrict the amount of data that may be transferred.

The provision of Section 4c Subsection 1 Sent. 1 No. 4 BDSG only allows the transfer of data that has already passed the proportionality test. Therefore, the general permission to transfer data for litigation purposes is implicitly restricted by the fundamental data privacy principles expressed in German law.

Such principles include data reduction and data economy pursuant to Section 3a BDSG, which prohibits a transfer that is not required for the intended purpose. As this is a German law provision, German law standards with respect to data transfer must be met for the exception provision to serve as a justifica-

tion.[25] Therefore, when transferring data for discovery proceedings, only required data pursuant to German law standards should be transferred.

Article 29 Data Protection Working Party

Article 29 Data Protection Working Party adopted Working Document 1/2009 on pre-trial discovery for cross-border civil litigation on 11 February 2009.[26] As Article 29 Working Party is the independent EU advisory body on data privacy, it must promote the uniform application of the Directive's general principles among EU Member States.[27]

Article 29 Data Protection Working Party acknowledges that the Directive allows a transfer of personal data for litigation purposes pursuant to Article 26 Subsection 1 (d) of the Directive. This, in turn, permits the transfer of personal data for litigation purposes under the same conditions as Section 4c Subsection 1 No. 4 BDSG. However, Article 29 Data Protection Working Party requires the transfer to be compliant with certain European data privacy requirements. Therefore, although Article 29 Data Protection Working Party acknowledges both the German and the European allowance for such data transfer, it refers to the obligation of the transferring party to adhere to certain European standards, rather than simply relying on the data subject's legal permission, i.e., the data subject's consent.[28]

Moreover, Article 29 Data Protection Working Party strictly interprets the identical European exception provision in order to ensure that "the exception does not become the rule."[29] Where the transfer of personal data for litigation purposes is likely to be a single transfer of all relevant information, there would be possible grounds for processing under Article 26 Subsection 1 (d) of the Directive where it is required for the establishment, exercise or defense of legal claims. Where a significant amount of data is to be transferred, Article 29 Data Protection Working Party recommends using Binding Corporate Rules (BCR) or Safe Harbor to provide an adequate level of data privacy.[30]

Reasons to Apply Restrictive Requirements to Data Transfers

Absent a restrictive approach to data transfer, German and European data privacy principles would be undermined and could no longer be adhered to. Accepting each demand for disclosure as required by US courts would open the door to foreign jurisdictions reaching into the German legal system.[31]

A broad interpretation of data privacy would not be compliant with European and German data privacy law. The exception provision does not allow an extensive transfer of data. Rather, it covers only the transfer of data required for the litigation proceeding. Thus, because it is an exception, the provision needs to be interpreted narrowly.[32]

If it is concluded that the transfer of data is permissible, the transfer would have to comply with the German data privacy principles of binding purpose (*Zweckbindung*), requirement (*Erforderlichkeit*) and data reduction and data economy (*Datensparsamkeit*).[33] Only such an approach can satisfy the need of European and German data privacy laws' enforcement. Further, because this exception is part of German law, German legal measures apply.[34]

Are there blocking statutes in other European countries?

Other European countries provide more specific blocking statutes. For example, in France, there are explicit blocking statutes for international judicial proceedings. The French national Blocking Statute no. 68-678 prohibits the disclosure of information in "foreign judicial and administrative proceedings."

Article 1 of French Law no. 68-678, dated July 26, 1968, as modified by Law no. 80-538, dated July 16, 1980 (the "French Blocking Statute"), prohibits the "disclosure in writing, orally or under any other form, [and] in any place to foreign public authorities, of documents or information of a business, commercial, industrial, financial or technical nature which would interfere with French sovereignty, security and essential economic interests or public order…," as well as the "claiming [or], seeking [by the parties to litigation] or disclosure [by both the parties to the

foreign litigation and third parties], [whether] in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature for the purpose of constituting evidence in view of foreign judicial or administrative proceedings or in relation thereto."

In addition, under Article 2 of the French Blocking Statute, the requested party must inform the French Minister of Foreign Affairs immediately upon receipt of the request. Article 3 of the French Blocking Statute provides that "without prejudice to any more serious sanctions permitted by law, any violation of the provisions of Articles 1 and 1b of this law shall be punished by a sentence up to 6 months of imprisonment and a fine up to EUR 18,000 or only one of these two sentences."

The French Blocking Statute is applicable, for instance, in the case of deposition requests, even if the deposition is taken outside of France. The statute applies, too, if the victim of the offense is a French national or if an act made in preparation of the deposition has been made on French soil (such as gathering documents to be produced before a US court).

German data privacy regulatory authorities have provided a two-tiered plan pursuant to which German companies can react to US court disclosure requirements and still remain compliant with the BDSG.

In order to avoid any risks, it is generally recommended that a foreign court should resort to the 1970 Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters (the "Hague Convention"). This is because the French Blocking Statute is not applicable if the taking of evidence abroad is conducted via the Hague Convention (and, more generally, in compliance with French law or treaties and international conventions).

Suggestions for Practical Implementation

The conflict between US disclosure requirements and European data privacy law is not yet resolved, and there are no provisions guiding this conflict. As a result, parties to relevant international litigation should obey certain principles in order to ensure compliance with the European and respective national data privacy laws. This will help avoid negative consequences if the laws are violated.

What Do German Authorities Recommend?

German data privacy regulatory authorities have provided a two-tiered plan pursuant to which German companies can react to US court disclosure requirements and still remain compliant with the BDSG. As a first step, the data shall be rendered anonymous before it is sent to the US court. If identity-specific information is required, the data shall be sent to the US courts in non-anonymous form.[35] US courts have accepted such procedures in the past.[36]

To comply with the need to transfer only such data as is "required" for litigation purposes, German authorities suggest the following procedure. First, the data should be filtered in Germany or in any other country covered by the EU Data Privacy Directive. Then, the data can be transferred. This procedure, however, applies only if filtering would not be disproportionate.[37] Another approach is to base every transfer of data to US courts on prior consent of the data subjects (if practicable),[38] or to involve a data trustee.[39]

What should companies operating in Europe do?

European companies involved in a US trial or e-discovery will often be challenged to comply with national privacy laws such as the German Federal Data Privacy Act and the European Directive 46/95/EC. They must be mindful of the relevant requirements for a permissible transfer of personal data from Europe, and especially from Germany, to US courts. Therefore, companies may wish to pursue several actions when transferring information to the United States, such as:

- Attempt to convince the US court not to demand access to personal data in the European Union that would not be compliant with EU data privacy laws. In practice, US courts do not generally refuse to obey European data privacy laws.[40] As the US Supreme Court stressed in the *Aérospatiale* case: "American courts, in supervising pre-trial proceedings should exercise special vigilance to protect foreign litigants from the danger that unrequired or unduly burdensome discovery may place them in a disadvantageous position."[41]

  However, in a decision dated January 2010, the US District Court of Utah did not accept the German Data Privacy Act as a justification to not disclose information.[42] Nevertheless, raising the problem

before a US court might lead to a compromise.

- Argue the conflict with the US court and demonstrate that the company is trying to fulfill the discovery requirement but is hindered by German law. It is essential for German parties to substantiate the German legal requirements.[43] By suggesting ways to obey the court orders while remaining compliant with German data privacy laws, the court may agree that the party is using its best endeavors to cooperate with the court. That may lead the court to abstain from sanctioning the company. This holds true even if the company does not disclose the required information if this was discussed with the opposing party in a discovery conference.[44]
- Render personal data anonymous or pseudonymous and then transfer the depersonalized information. This can be done by simply redacting information in the respective documents.
- Limit the information to the personal data that is required as proof in the proceedings, and filter the respective data in Germany.
- Restrict use of the delivered personal data to the litigation only; i.e., the purpose for which the data was transferred.[45] The data must not be revealed to the public, to the media or to competing enterprises.[46]
- Strive to convince the US court to protect the personal data against access by third parties by issuing protective orders or filing under seal.[47]
- Seek to enter into a litigation agreement pursuant to which the opposing party's lawyers have access to the documents but the parties themselves do not.[48]
- Delete personal data after it is used, and request deletion by other parties.
- Safeguard the legal findings with technical and organizational measures.[49]

If conflicts between the two legal systems cannot be resolved prior to trial, it is recommended that European companies consult and cooperate with the responsible data privacy regulatory authorities to get approval for each situation.

Summary

The conflict between US disclosure requirements and European—especially German—data privacy law is ongoing and has not yet been resolved. International regulations are still absent and are urgently needed. Nevertheless, the practical solutions discussed above can help German companies involved in US litigation proceedings to adequately react to disclosure requirements and still remain compliant with German data privacy law. ◆

Endnotes

1 For a recent instructive overview regarding this conflict of companies see Geercken, Holden, Rath, Surguy and Stretton, CRi 2010, 65, 70.

2 Brisch and Laue, RDV 2010, 1, 3.

3 Newman and Zaslowsky speak of a "seemingly irresolvable conflict between broad US-based discovery rules and EU Member States' privacy and data protection directives," Newman and Zaslowsky, see above, p. 1.

4 Brisch and Laue, RDV 2010, 1, 3; Spies and Schröder, MMR 2008, 275, 278.

5 Berlin Data Protection Officer, under: http://www.datenschutz-berlin.de/content/themen-a-z/internationaler-datenverkehr/datenuebermittlungen-an-us-behoerden-sowie-us-unternehmen.

Regarding the general conflict between the US and German systems, see Hilgard in: "Electronic Discovery Deskbook," Chapter "International Issues," *Practicing Law Institute*, 2009; Hilgard and Kraayvanger, "Urkundenvorlegung im Zivilprozess—Annäherung an das amerikanische "Discovery"—Verfahren?" ("Submission of Documents in Civil Proceedings—Approximation to the American Discovery Procedures?"), Die Justiz 2003, 572 et seq.; Kraayvanger, book review: Abbo Junker "Electronic Discovery *gegen deutsche Unternehmen*" (Electronic Discovery Against German Business Entities), DAJV Newsletter 3/2008, p. 136 et seq.; Kraayvanger, "Discovery *im deutschen Zivilprozess—über den Umweg der US-amerikanischen Beweishilfe*" (Discovery in the German Civil Procedure Through US Discovery Aid), RIW 7/2007, p. 496 et seq.

6 Lux and Glienke, RIW 2010, 603, 605; Carsten Domke, International E-Discovery—E-Discovery vs. German Data Protection, Paper for the American Bar Association (ABA) Tech Committee, available under: http://www.abanet.org/labor/techcomm/mw/Papers/2010/pdf/domke.pdf, p. 4.

7 Art.29 Data Protection Working Party, WP 158, p. 6. In the EU, the protection of personal data is considered a fundamental human right that is protected by the laws, Newman and Zaslowsky, The Conflict in Production of Documents From Abroad, New York Law Journal, p. 1, available under: http://www.law.com/jsp/nylj/PubArticleFriendlyNY.jsp?id=1202463762347, p. 2.

8 Art.29 Data Protection Working Party, WP 158, p. 6.; see the decisions *Accessdata Corp. v. Alste Technologies GmbH*, Decision of 21 January 2010, Case No. 2:08cv569, LEXIS 4566, MMR 2010, 275 et seq.; *Richmark Corp.*, 959 F.2d 1468, 1478 (1992); *Weiss v. Natl. Westminster Bank*, 242 F.R.D. 333, 45 ff. (E.D.N.Y. 2007); see Spies/Schröder, MMR 2010, 276 et seq.; see Knöfel, RIW 2010, 403 et seq.

9 See the decisions *Reinsurance Co. of America, Inc. v. Administratia Asigurarilor de Stat*, 902 F.2d 1275, 1281

(7th Cir. 1990); *Volkswagen v. Valdez*, 909 S.W.2d 900,902 f. (Tex. 1995); *Minpeco, S.A. v. ContiCommodity Servs., Inc*, 116 F.R.D. 517, 530 (S.D.N.Y. 1987).

10 Domke, see above, p. 4; controversial: Newman and Zaslowsky, p.1, Lux and Glienke, RIW 2010, 603, 604.

11 Namely the Czech, Dutch, German, Greek, Italian, Latvian, Portuguese, Romanian and Spanish versions.

12 Gabel, in: Taeger and Gabel, BDSG, § 4c no. 11 holds that this provision only applies to proceedings that are covered by the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters. Pursuant to Brühann, in: Grabitz and Hilf, Das Recht der Europäischen Union, Art. 30 no. 9, the provision covers only state court proceedings, as only such proceedings guarantee adequate protection of personal data.

13 Burainski and Reinl, SchiedsVZ 2010, 187, 191.

14 Lux and Glienke, RIW 2010, 603, 605; Spies and Schröder, MMR 2008, 375, 279; Geercken, Holden, Rath, Surguy and Stretton, CRi 2010, 65,71; Taeger and Gabel, BDSG, Sec. 4c no. 11; Newman and Zaslowsky, see above, p. 3

15 See *American Tel. Tel. Co v. Grady*, 594 F.2d 594 (7th Cir. 1978).

16 Pursuant to Section 169 1. Sentence German Judicature Act (*Gerichtsverfassungsgesetz* or GVG).

17 Lux and Glienke, RIW 2010, 603, 606.

18 Däubler, Klebe, Wedde and Weichert, BDSG, Sec. 4c no. 4; Gola and Schomerus, BDSG, Sec. 4c no. 4. Gola and Schomerus, BDSG, Sec. 4c no. 7; Brisch and Laue, RDV 2010, 1, 7.

19 Taeger and Gabel, BDSG, Sec. 4c no. 9.

20 Id.

21 Art.29 Data Protection Working Party, WP 158, p. 3.

22 Domke, see above, p. 6; Spies, MMR 2007, V, VII.

23 For that strict interpretation of the wording "required" (*erforderlich*) see Taeger and Gabel, BDSG, Sec. 4c no. 11; Simitis, BDSG, Sec. 4c no. 21; Art.29 Data Protection Working Party, WP 114, p. 18.

24 Domke, see above, p. 6. See also Knöfel, RIW 2010, 403, 405, who assumes that data protection law does not play any role in a litigation procedure.

25 See also Newman and Zaslowsky, p. 2: They point out that the foreign court—which in this respect would be the German court—is the one to determine whether the discovery request is reasonable.

26 Document can be downloaded from: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm. See also Hilgard in: "Electronic Discovery Deskbook," Chapter "International Issues," *Practicing Law Institute*, 2009.

27 See the objectives of the Directive under: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/tasks-art-29_en.pdf.

28 So Art.29 Data Protection Working Party, see WP 117, p. 8; WP 114, p. 15; WP 158, p. 15.

29 Art. 29 Data Protection Working Party, WP 114, p. 7. However, there is little guidance on the interpretation of "required" in this context in the Working Paper.

30 WP 158, p. 13. Thereby, Art. 29 Data Protection Working Party reiterates its earlier opinion that Art. 26 (1)(d) cannot be used to justify the transfer of all employee files to a group's parent company on the grounds of the possibility that legal proceedings may be brought in US courts one day, see WP 114, p. 15.

31 Art. 29 Data Protection Working Party, WP 117, p. 8; Spies and Schröder, MMR 2010, 275, 279.

32 Burianski/Reindl, SchiedsVZ 2010, 187, 194; Däubler/Klebe/Wedde/Weichert, BDSG, Sec. 4c no. 4.

33 Brisch and Laue, RDV 2010, 1, 7.

34 It should also be noted that it is not possible to circumvent the prohibition to supply documents or data by examining a witness on the contents of the documents or data. See Hilgard in: "Electronic Discovery Deskbook," Chapter "International Issues," *Practicing Law Institute*, 2009.

35 Annual report of the Berlin Data Protection Officer, 2006, p. 170.

36 See annual report of the Berlin Data Protection Officer, 2006, p. 171.

37 Brisch and Laue, RDV 2010, 1, 5.

38 Art.29 Data Protection Working Party, WP 158, p. 10.

39 See annual report of the Berlin Data Protection Officer, 2006, p. 171.

40 Spies and Schröder, MMR 2010, 275f; Geercken, Holden, Rath, Surguy and Stretton, CRi 2010, 65, 70. For an individual solution that has to be used by the US court in each individual case: Kristen A. Knapp, "Enforcement of US Electronic Discovery Law Against Foreign Companies: Should US Courts Give Effect to the EU Data Protection Directive?" available at SSNR.

41 *Societe Nationale Industrielle Aerospatiale v. US Dist. Court for the S. Dist. of Iowa*, 482 US 522, 546 (1987)

42 *Accessdata Corp. v. Alste Technologies GmbH*, Decision of 21 January 2010, Case No. 2:08cv569, LEXIS 4566.

43 Lux and Glienke, RIW 2010, 603, 607.

44 Spies and Schröder, MMR 2008, 275, 280.

45 Simitis, BDSG, Sec. 4c no. 21.

46 Däubler, Klebe, Wedde and Weichert, BDSG, Sec. 4c no. 8.

47 Spies and Schröder, MMR 2008. 275, 280 with regards to FCPR Rule 26(c).

48 Id. at 275, 280.

49 See Brisch and Laue, RDV 2010, 1, 7. With respect to these measures, companies may rely on the technical and organizational measures as set out in Sec. 9 Sentence 1 BDSG.

MARINA G. ARONCHIK
Associate

Marina Aronchik is an associate in the Chicago office of Mayer Brown's Corporate & Securities practice. Ms. Aronchik's practice includes information technology and outsourcing transactions, mergers and acquisitions and corporate governance. Before joining Mayer Brown, Ms. Aronchik worked in the information technology industry helping clients implement a variety of web-based applications and data management systems, including SAP.

KRISTY L. BALSANEK
Associate

Kristy Balsanek is an associate in Mayer Brown's Government and Global Trade group. Kristy's practice focuses on international corporate compliance and international business transactions where she counsels clients on commodity jurisdiction questions, classifications, export licensing, customer screening, anti-corruption, compliance program design and implementation, audits, voluntary disclosures and internal and US government investigations.

CAROL J. BILZI
Counsel

Carol Bilzi has counseled clients on the regulatory and policy aspects of international business and financial transactions for over twenty years. Her export control work encompasses compliance with the Export Administration Regulations (EAR) governing dual-use exports, including the export of encryption software and technology, and the International Traffic in Arms Regulations (ITAR) governing the export of defense articles and services. Carol's practice includes counseling on transactional compliance, export licensing, voluntary disclosures, and enforcement actions, with particular emphasis on the development and implementation of corporate compliance programs.

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.

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.

MARK C. HILGARD
Partner

Mark C. Hilgard leads the litigation and arbitration practice of Mayer Brown in Germany. He has an extensive multinational practice in which he focuses on a wide range of commercial litigation and arbitration, as well as on merger and acquisition transactions. Litigious and arbitral matters in which Mark has represented clients or in which he acted as arbitrator include post-M&A disputes, contractual disputes, complex liability cases, cartel law disputes, and plant engineering and construction controversies. In corporate and commercial matters Mark has a special emphasis on mergers and acquisitions.

ROBERT J. KRISS
Partner

Robert Kriss has represented some of the world's largest Internet and technology companies in commercial and class action litigation. He began representing Internet-based companies in the late 1990s when he successfully defended America Online in over 60 class actions arising from consumers' alleged difficulties connecting to AOL. Since then, Bob has successfully defended numerous consumer class actions involving a wide variety of Internet-based marketing and billing practices and has represented clients such as Accenture, Acxiom, AT&T, Oracle, Mead Johnson and others in commercial and securities litigation involving information technology outsourcing and new system implementation. He also has assisted companies in investigating and remediating data breaches and in establishing privacy policies.

D. MICHAEL MURRAY
Partner

Michael Murray focuses his practice on mergers and acquisitions, corporate governance and general corporate counseling. He represents buyers, sellers and financial advisors in connection with public and private M&A transactions, joint ventures and similar transactions.

ANDREA PATZAK
Former Associate

Andrea Patzak's 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. Andrea now is employed by SCHULTE RIESENKAMPFF Rechtsanwaltsgesellschaft mbH.

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.

LINDA L. RHODES
Partner

Linda Rhodes is a member of our Business & Technology Sourcing Practice and our Corporate & Securities Group. Her practice includes representing clients in a diverse array of information technology outsourcing, business process outsourcing and business sourcing transactions. Linda also focuses her practice on other complex commercial transactions, including mergers, acquisitions and divestitures, joint ventures and financing transactions. She has represented a wide spectrum of clients, from emerging companies to large multinational corporations, in a variety of industries. Linda has substantial experience in leading contract negotiations, bringing complex transactions to successful closure and effectively managing the international aspects of global transactions.

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, since 2008 he has been leading a team of attorneys that 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.

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

TAUIL & CHEQUER ADVOGADOS
in association with Mayer Brown LLP
- São Paulo
- Rio de Janeiro

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.