

Issue: September 2006

European Outsourcing: Growing Demand Highlights Data Protection and Other Key Issues

By MICHAEL FINN, GENERAL DYNAMICS UK
CHRIS HOLDER AND BRIDGET TREACY, BARLOW LYDE & GILBERT
RUTH HARVEY AND RANDALL PARKS, HUNTON & WILLIAMS, LLP

Outsourcing has become a permanent feature of European business. Originally limited to manufacturing, information technology, and a few highly specialized business functions, outsourcing is now used to cut costs in a broad range of functions as well as to provide a competitive business advantage. The trend has become viral, with new deals spreading from department to department at large firms and from competitor to competitor in industries like financial services and energy. Few businesses of any size are immune.

Over the course of the last few years, growth of the European outsourcing market, which includes both information technology (IT) and business process (BPO) transactions, has accelerated. Although there have been fewer megadeals in recent months, many smaller business process deals have been struck. Globally, 2005 was a record year, with more IT and BPO deals signed than ever before.

The European outsourcing market has developed differently from country to country. The UK has mirrored the US trend toward large IT transactions and still leads the way with some global BPO transactions. A recent example is the outsourcing of Unilever's human resources functions to Accenture, a deal reported to be worth over \$1 billion. The Nordic region of Europe has followed closely behind. One of Europe's biggest IT outsourcing deals last year was signed by ABN Amro bank in Holland. Although countries like Germany, France, and Italy have been slow to recognise the potential advantages of outsourcing, these areas now are beginning to show growth, particularly in BPO transactions.

One of the recent factors driving more activity in this market has been the renegotiation and restructuring of existing transactions. The large-scale suppliers (IBM, EDS, CSC, and Accenture) have seen a marked rise in

such renegotiations, which have put strains on existing relationships with customers. However, there has not been an equivalent rise in the number of lawsuits filed, which suggests that all parties prefer to renegotiate deals in private.

Key European Legal Issues

The largest global outsourcing vendors and consultants generally employ the same business and transactional models worldwide. Consequently, from a legal perspective, the big issues that trouble lawyers working in this area are the same from country to country: namely, the interrelationship between price, scope of services, service levels, and terms and conditions.

The major legal differences in European outsourcing are found in the data protection requirements of the European Parliament's Data Protection Directive and the employment-related rules under the Acquired Rights Directive. This briefing does not address industry-specific rules, such as the UK Financial Services Administration's outsourcing guidance, which should also be considered.

As background for readers not familiar with European regulation, 25 separate member states make up the EU. The legislative body for the EU, the European Parliament, has the power to formulate regulation (in the form of Directives) that is nonbinding in each member state until enacted into domestic law. The detailed provisions of the domestic legislation are left to each country. Consequently, even though a European Directive may be implemented in 25 member states, it may well be slightly different in each, resulting in a variation in laws across the EU.

The Data Protection Directive: What Is Protected?

The Data Protection Directive (95/46/EC) (the "Directive") regulates the processing of personal data in EU member states. Since almost every outsourcing involves some processing of personal data, often across national borders, planning for compliance is a key element of every transaction.

According to the Directive, "personal data" is any information which relates to an identified or identifiable natural person. An identifiable person is one who can be identified, directly

a quarterly supplement of ACC Docket

or indirectly, from the information — in particular by reference to an identification number or to one or more factors specific to an individual's physical, physiological, mental, economic, cultural, or social identity. The breadth of this definition means that very few outsourcing transactions will not involve personal data. Further, the Directive applies to the processing of personal data by automatic means (for example, electronically held files) as well as to nonautomated processing, provided the nonautomated files form part of a structured filing system.

In this Issue

European Outsourcing: Growing Demand Highlights Data Protection and Other Key Issues 1

By Michael Finn, General Dynamics UK
Chris Holder and Bridget Treacy, Barlow Lyde & Gilbert
Ruth Harvey and Randall Parks, Hunton & Williams, LLP

Outsourcing in the United Kingdom 4

By Mark Duesenberg, Lenovo Group Limited
Jerry Temko, Astellas Pharma Europe Limited
Nick Perry, Bird & Bird (nick.perry@twobirds.com)
Richard Graham, Bird & Bird (richard.graham@twobirds.com)

Outsourcing 6

By Ian Jones, British Telecommunications plc

Outsourcing – IT Dinosaur or State of the Art? 7

By Bernard E. Lankes, Sun Microsystems Australia

Ad-ding Up Correctly 10

By Carolyn Boyle, International Law Office

There is a further subset of personal data, known as "sensitive personal data," which consists of special categories of data and is subject to additional safeguards. Under the Directive, sensitive personal data may include information relating to a person's racial or ethnic origin, religious beliefs, trade union membership, and health or sex life. Particular care must be taken with such information, because apparently innocuous details can sometimes equate to sensitive personal data. For instance, a person's name can indicate both their racial or ethnic origin and religious beliefs. The generally accepted best practice in most European jurisdictions is that sensitive personal data can only be processed subject to the explicit consent of the individual.

The scope of the Directive is extremely far reaching due to the wide definition of "processing," which includes obtaining, recording, storing, amending, retrieving, disclosing, and destroying the data. Consequently, even calling data up on a computer screen may constitute "processing." It is difficult to envisage any use of personal data by an outsource supplier which would not amount to processing under the Directive.

The Directive imposes obligations on "data controllers," who are the individuals or entities that determine the purposes for and the manner in which personal data will be processed. The role of data controller is distinct from that of a "data processor," who merely processes data in accordance with the instructions of a data controller. The data processor does not have any obligations under the Directive, but will (or should) have contractual obligations imposed on it by the data controller.

Applying the provisions of the Directive to the context of IT outsourcing, a company which outsources its data centre — or any other part of its infrastructure that "processes" data — will remain the data controller as long as it continues to determine what data is recorded, how and for what purpose, and how the data is to be processed. Suppliers who merely provide the IT infrastructure would typically be characterised as "data processors."

The Directive contains a number of data protection principles which effectively form an enforceable code of practice governing the processing of personal data. Businesses which process personal data as data controllers must ensure that all such use or processing is in accordance with these principles. A failure to

do so may result in fines (which in some EU jurisdictions can be significant), an order that the processing cease, or negative publicity, which is increasingly seen by businesses as a serious deterrent.

The principles require that personal data be:

- processed fairly and lawfully;
- processed only for the purposes specified by the data controller to the individual;
- adequate, relevant, and not excessive;
- accurate and up-to-date;
- not retained unnecessarily;
- processed in accordance with the individual's rights, including the right of subject access;
- processed securely; and
- only transferred outside the European Economic Area (EEA) if adequate protections exist.

These principles may appear straightforward, but care should be exercised in assessing compliance, as the domestic legislation of individual member states expands on many of the principles, which in fact require more compliance activity than their basic description might suggest. From the perspective of an outsourcing agreement, these obligations should be contractually imposed upon the outsource supplier so that the outsource supplier is contractually obliged to process the data in accordance with the principles. A failure to deal adequately with this issue can mean that the customer, who remains responsible for the data under the Directive, may be in breach of its obligations.

Processing v. Data Protection Obligations

In the context of an outsourcing transaction, data processing (i.e., the transfer of the data) may take place at several stages: during due diligence, contract negotiation, and the transition or implementation stage. At each of these stages, the customer will need to ensure that any transfer of personal data is undertaken on a fair and lawful basis. In practical terms, satisfying the "fair and lawful" requirement means that the customer will need to fulfill one, or in the case of sensitive personal data, two, of the criteria specified in the Directive — usually, a "legitimate interest" in processing the data and/or consent of the data subject.

It is also essential that the customer establish the capacity in which the outsource supplier

will process the data. If the supplier is a mere processor, it will have no obligation to comply with the Directive. The customer should therefore, seek to flow into the outsource contract certain of its obligations under the Directive. In addition, the security principle requires the customer, as controller, to evidence the processing arrangements by a written contract, require the supplier to process data only in accordance with the customer's instructions, and ensure that the processor has in place adequate technical and organisational security measures to protect the data.



In practice, the majority of outsource suppliers seek to characterise their role as that of processor, rather than controller. This effectively limits their data protection compliance obligations to those specified in the contract. It is still common, particularly in outsource deals involving smaller businesses, to see contract terms simply requiring the parties to comply with their obligations under the Directive and relevant local laws. Counsel should be careful about this approach, as the Directive does not impose any obligations on a mere processor. An outsource customer could thus become unnecessarily exposed to risk as a result of

their outsource supplier's noncompliant processing of personal data. Consequently, the better-advised companies detail in the contract exactly what is required of the processor.

Alternatively, it may be the case that the outsource supplier is actually a controller, regardless of the provisions of the contract. This determination will be a question of fact and requires careful analysis of the data processing activities in the context of the specific services to be outsourced.

It is common for customers to impose detailed security obligations on outsource suppliers covering such things as security measures relating to the systems over which data may be transferred, accessed,

selecting a supplier. Customers should make sure that audit rights are a part of the contract and exercise those rights during the contract term.

Personal Data Cross-border Transfers

A further layer of complexity is added where the personal data is to be transferred abroad as part of the outsourcing transaction, given that Article 25 of the Directive prohibits transfers of data outside the EEA unless the importing jurisdiction has "adequate" data protection. This "adequacy" may be established in various ways: individual countries may be designated under the Directive as having an adequate data protection law; US companies (for example) may voluntarily submit to EU-style data principles through a safe-harbor scheme; or the parties may execute a set of model clauses, approved by the European

Commission as a contractual basis for ensuring adequacy when data are transferred outside the EEA.

so far only three corporations have had their schemes approved by the data protection regulators. Despite this relatively slow start, this concept is widely considered to be the likely future structure for cross-border transfers.

The Acquired Rights Directive and TUPE

One important issue that must be considered for European outsourcings is the broad impact of the local regulations (generally similar in nature) implementing the EU Acquired Rights Directive. As an example, the UK has adopted the Transfer of Undertaking (Protection of Employment) Regulations 2006 ("TUPE," pronounced "two-pea"). In brief:

- TUPE protects employees on "transfers" of "undertakings," including the transfers of business functions that occur in outsourcings. Employees who are associated with the transferred functions automatically move their employment contracts to the outsourcing supplier. Therefore, the customer's employees who provide the outsourced function will become employees of the company providing the outsourced services.
- The supplier takes the employment contracts on the same terms and conditions and with full length of service intact, as well as inheriting various liabilities of the former employer, including discrimination liability, personal injury liability, restrictive covenants, collective issues, consultation liability, and possibly the obligation to provide a similar pension.
- No changes can be made to the terms and conditions of employment unless there is (a) an unrelated nontransfer reason for the change; or (b) an economic, technical, or organizational reason involving changes to the workforce numbers or function.
- An employee can choose to object to being transferred, but will usually lose all TUPE and other employment rights.
- Special rules exist protecting employees from dismissal from either the old or new employer; such dismissals will be deemed automatically unfair.
- There are notification obligations that must be met to the employees who are transferring and to the new employer.

How Does TUPE Affect Outsourcings?

The implications of TUPE for outsourcing transactions are significant:

- Headcount reductions — and related



manipulated, and stored; organisational security measures governing access to premises; and prohibition on staff bringing data storage devices on the premises (e.g., mobile phones and memory sticks).


In addition to imposing detailed security measures, customers should undertake due diligence on aspects of data security before

While the model contract clauses are sometimes used in the context of intragroup transfers, data protection regulators recognize that between subsidiaries within a corporate group, a system of internal contracts would provide a more practical solution to cross-border data flows. Although there is a degree of enthusiasm for these so-called "binding corporate rules for international data transfers,"

savings — can be difficult to achieve without careful planning. Even well-planned terminations may be challenged, and the parties should anticipate this possibility in the outsourcing agreement.

- Similarly, suppliers may find it difficult or impossible to harmonize the terms of employment of the transferred workforce with those of their existing workforce. Inevitably, any resulting costs find their way into the price of the supplier's services.
- Accommodating the required notices and advance consultations with employees also requires planning to avoid delays.
- Terminating an outsourcing agreement can trigger an ironic result: The customer must assume obligations to the very employees of the supplier who is responsible for failure. Contracts must address not only the initial transfer, but also the possibility of later transfers.
- Suppliers may require extensive due diligence of employment records to evaluate their exposure to transferred claims.
- TUPE may force the parties to construct contractual representations and indemnities to redistribute commercially unsatisfactory allocations of liability.
- The variation of local implementations of the Acquired Rights Directive, may require several different compliance solutions in multicountry outsourcing.

Lawyers Can Help Avoid Delays

As the trend toward outsourcing continues to develop, more businesses with European operations will contend with the unique challenges posed by the market and its legal peculiarities. Assembling an experienced team that understands the outsourcing industry, its players, and the local rules is at least half the battle. Including the lawyers on that team from the inception of an outsourcing project can avoid surprise and delay later on. 

This article does not provide a complete statement of the law. It is intended merely to highlight issues which may be of general interest and does not constitute legal advice.

Outsourcing in the United Kingdom

By MARK DUESENBERG, LENOVO GROUP LIMITED
JERRY TEMKO, ASTELLAS PHARMA EUROPE LIMITED
NICK PERRY, BIRD & BIRD (NICK.PERRY@TWOBIRDS.COM)
RICHARD GRAHAM, BIRD & BIRD (RICHARD.GRAHAM@TWOBIRDS.COM)

Outsourcing has been a major strategic solution for a number of businesses in recent years. English law and commercial practices relating to outsourcing are similar in many regards to those found in the United States. When considering an outsourcing, you should weigh each risk carefully, whether it is operational, financial, regulatory, or reputational, and balance the risk against each proposed benefit of the outsourcing.

The main driver behind an outsourcing is usually to reduce the cost of the delivery of services currently being provided in-house. However, there are other drivers, including access to skills, a desire to focus on core business, or to allow the service provider to invest in a noncore business area. Important risks to consider include employment and pension liabilities, which can significantly affect the cost of the project, and the risk allocation for changes in law and third-party licence fees.

The Framework: Governed by English Law

Many organisations with a presence in several European jurisdictions contemplate a “pan-European” outsourcing, in which services in a number of jurisdictions are simultaneously outsourced to a service provider located in several or all of those jurisdictions. A common approach for these pan-European outsourcings is to have the holding entities enter into a framework agreement allowing local entities to draw-down services under local implementation agreements. The framework agreement is often entered into under English law, and covers both the “framework” terms and most of the service terms, which will be common to all jurisdictions. There are then “subsidiary” local contracts entered into under local law that accommodate the variations in local law. This approach is the best way of resolving local legal, regulatory, and tax issues and allows for a more uniform approach to service delivery in all the jurisdictions.

Employment and Pensions Risks for Your Existing Workforce

One of the most important factors to consider in any European outsourcing is the risk

associated with statutory employment and pension liabilities. Under English law, if you outsource part of your business to a third-party service provider, your employment contracts will usually automatically transfer to the service provider. This significantly affects the cost of the project and often requires contractual allocation of risk between you (the outsourcing customer) and the service provider dealing with pre- and post-transfer employment liabilities. Employment contracts will also transfer back to you at the end of the outsourcing, or onward to a new service provider should a new service provider be appointed. Since this is governed by protective employee legislation, you and the service provider cannot agree to contract out of it.

When transferring employees, you must have sufficient staff who can manage the service provider during the outsourcing and/or are able to bring the service back in-house after the outsourcing ceases. Also, if you terminate an individual's employment contract as a result of your outsourcing, the termination is likely to be deemed an unfair dismissal, which you will be obliged to compensate accordingly. Finally, like most EU Member-States, the United Kingdom has statutory procedures requiring consultation with employee representatives. These procedures vary throughout Europe, where consultations tend to be with works councils and can often delay the implementation of an outsourcing, making pan-European simultaneous “go-live” very difficult to achieve.

Recent legislation has imposed a minimum obligation on service providers to provide pension benefits for transferring employees who satisfy certain conditions. This obligation can have a significant impact on the service provider's costs and thus on the costs of and risk allocations for outsourcing. You should therefore carefully consider the pension position of any employees being transferred to a service provider. The pension position will ultimately depend upon whether the existing employees benefit from an occupational, stakeholder, personal, or group scheme. As a result, the existing pension arrangements will determine whether the service provider has an obligation to contribute toward the pensions of transferring employees and whether the service provider will have any flexibility to offer alternative pension arrangements.

Data Protection and Security Risk

Under English law, data protection

legislation imposes strict requirements on any organisations that process data which relates to the identity of individuals. Although there are likely to be commercial solutions to the various legislative requirements, the regulatory, reputational, and financial risks are significant if the requirements are not met. This risk is even more significant if the business sees customer data as a critical business asset. You therefore need to consider this issue at the outset; although it sounds innocuous, data protection can fundamentally affect the structure of a deal or the question of which services can be outsourced.

Eight data protection principles need to be followed by any organisation that transfers or processes personal data. These include the obligation to process personal data fairly and lawfully and in accordance with the individual's rights. Your business will be considered a data controller for the purposes of data protection legislation, as it ultimately determines the purposes for which, and the manner in which, personal data is to be processed. As a data controller, your business will not be able to delegate its statutory duties to the service provider acting as a data processor. Any wrongful disclosure of data or unlawful processing may attract criminal and civil liability.

The overriding principle of the data protection legislation is that the data must remain secure. This obligation will often require both the customer and the service provider to seek to achieve the requirements of both international and British standards (i.e. ISO/BS17799).

Processing and Overseas Transfers

The service provider will generally be seen as a data processor. It will be your obligation, as data controller, to make sure that the contract with the service provider meets the requirements of the data protection legislation.

Any transfer of data from within the United Kingdom to outside the European Economic Area will also attract further regulatory protection. English law requires that "adequate protection" be afforded to such data, a requirement that your business should consider. The solutions to

this requirement include ensuring that the exporting and importing entity enter into EU Model Contractual Clauses that cannot be amended, or, if the data is being transferred to the US, that the recipient of the information participate in the US Department of Commerce's Safe Harbor programme.

Limiting Your Contractual Risk

From a legal point of view, the most important part of the project is negotiating the contract so that your business is contractually protected from the key risks. Many of the core risks identified in this briefing can be addressed in the contractual documents.

English law restricts how parties can limit their liability by contract. These restrictions tend



to be greater than those imposed under US law. As an example, under English law, certain categories of loss cannot be excluded or restricted such as liability for death or personal injury. English law and US law also differ on the treatment of gross negligence, wilful default, and liability for loss of profit. Although these issues may appear technical, they can alter the financial risk profile of the deal for both parties and often prove contentious in negotiations.

With most major transactions, indemnities will allow you to specifically address any significant risks you consider likely to arise as a result of the outsourcing. In the United Kingdom, market practice generally dictates that service providers usually accept certain indemnities, such as for breach of intellectual property, confidentiality, and data protection, or for liabilities arising from employment.

Financial Services: A Regulatory Risk

For organisations working in the financial services sector, compliance with financial services legislation is fundamental. In the United Kingdom, the Financial Services Authority is the regulatory body responsible for implementing a whole host of rules and guidance and has extensive enforcement powers. Failure to comply with their regulatory requirements can lead to significant fines and, in some cases, a withdrawal of the right to continue providing financial services. It is worth noting that unless your business operates within the financial services industry, the rules and regulations are unlikely to apply to your business.

Drafting Tips

Many of the risks identified can be mitigated by careful drafting of the agreement's terms and conditions. We highlighted the two areas where the drafting plays a fundamental role in risk allocation: limitation of liability and indemnity protection. Another area is that of agreed remedies for breach of contract, commonly referred to as "service credits." Generally speaking, service credits are agreed sums to be deducted from the charges for the relevant services where there has been a failure to reach the agreed service levels.

Service credits can act as an incentive for the service provider to meet the agreed performance levels. They also make the recovery of damages easier and avoid the common problems of proving actual loss.


When drafting the appropriate service credit mechanism, it is important to consider whether the service credits are supposed to be an alternative to damages or merely act as a relatively minor price reduction should the service levels not be met.

Where the service credits are intended to be an alternative to damages, it is important that any deduction from the charges be no more than a genuine pre-estimate of the loss suffered. Under English law, any agreed sums payable on breach must be a genuine pre-estimate of the anticipated loss, rather than a penalty — a charge intended to apply undue force on the party to perform its obligations. If a court

determines that the agreed sums are not a genuine pre-estimate, it will hold the sums to be an unenforceable penalty.

Where the service credits are not intended to be an alternative to damages, then you should consider whether the agreement also permits the customer to recover any damages on top of the service credits received. Service providers and customers tend to have opposing views on this — for obvious reasons — and so the issue needs to be considered carefully.

Balancing the Pros and Cons

When considering outsourcing, it will be necessary to balance the proposed benefits against the risks of the outsourcing. Each risk should be identified from the outset and a practical solution agreed to. And of course, in addition to the risks identified above, you should also consider both the political and the reputation risks that might arise when outsourcing. 

Outsourcing

By IAN JONES
BRITISH TELECOMMUNICATIONS PLC

Outsourcing is as old as the hills. Man has always looked at ways of achieving his objectives through the endeavours of others. In the commercial world, outsourcing has developed over the years into a sophisticated, multibillion-dollar business model. Yet achieving a good outsourcing solution is time consuming and legally complex.

Good outsourcing should release an organisation to concentrate on its core business. If the activity to be outsourced is not a core activity for that business, then it is likely that someone dedicated to that activity will be able to run it more efficiently, lowering the costs to your organisation.

Organisations also look to outsourcing to transfer risk to a service provider. After all, risk is a commodity that is bought and sold. Risks that the outsourcer might transfer would include risks related to technology and development, people, and the balance sheet.

Finally, business expertise could be a reason to outsource. A service provider may well be better placed to understand developments in thinking and technology which will allow greater efficiency.

Risks

Of course, the benefits of outsourcing will not be captured unless we, as lawyers, draft agreements that deliver the financial benefits, share the potential efficiencies, and properly transfer the risk. In particular, there are three categories of structural risks attached to outsourcing that should be carefully considered:

Control. Loss of control is a major issue for outsourcers, who need to strike a balance between moving the activity to a service provider and retaining sufficient control to ensure business continuity. Good performance management regimes, as well as “step-in” and termination rights, can help to offset the concern that an organisation has ceded its destiny to its service provider.

Financial. These risks are myriad, but all return to the same two points. First, is the proposed service provider financially viable and capable of providing the services over the life of the contract? You may want to consider requiring guarantees and performance bonds. Second, if your company outsources an activity to a service provider, can your company tell whether it is achieving a proper return on its investment? Any outsourcing arrangement must provide your company with sufficient information for its financial return to be adequately transparent, without putting the service provider under unnecessarily onerous duties to provide fiscal information. Proportionality is vital.

Reputation. Some companies like to outsource the management of their customer relationships. But be wary: A failure in this area can have a big impact on your brand and reputation. A good example of how the disruption of even a noncore activity can affect a company is the Gate Gourmet industrial action. In the summer of 2005, British Airways not only took a hit to immediate revenue of over 35 million pounds, but also suffered negative publicity when Gate Gourmet, the outsourced manager of its in-flight catering, became involved in a dispute with its workers. This underlines the need to ensure that agreements give the outsourcer suitable rights to be warned of and get involved in issues that may affect its reputation. Reputation is an especially important consideration when outsourcing activities that ensure your company's legal or regulatory compliance.

Stages

There are three key stages in a successful outsourcing:

Transfer of the activity. For a lawyer, the initial stages of the transaction are similar to selling a business. The process to be outsourced will inevitably involve tangible assets, such as property and equipment; people (with their rights, which could be different in various jurisdictions across the world); and intangible property, such as intellectual property and business exploitation rights. Any agreement should define these assets and specify what assets and rights will be transferred to a service provider. Thus considerable due diligence will be necessary, coupled with the usual network of representations, warranties, and indemnities.

Unlike a sale of a business, outsourcing will have two further aspects. First, the outsourcer should carry out some due diligence — possibly extensive — on the service provider. Second, there is the outsourcing agreement itself. These documents are often complex, consisting of a framework agreement and a raft of subagreements which govern major areas of the proposed relationship (for example: service-level agreements, performance management agreements, and governance arrangements).


To successfully transfer an activity, the lawyers involved will need good project management skills. The lawyers and the commercial team should also have excellent and regular communication, and of course adequate time is always a key factor.

In-life management. Good in-life contract management is essential to successful outsourcing. A relationship can quickly deteriorate and the objectives of the outsourcing can become lost, if there is inadequate contract management. The lawyers involved must recognise that although they will perhaps be focusing on the drafting and negotiation of the agreements, the outsourcing relationship itself is generally long-term and organic.

During the contract life, there will inevitably be formal contract variations as well as agreements over changes in custom and practice. The tendency is, unfortunately, for the parties to avoid formal change control

procedures, especially for minor changes. Fight this tendency: Record evidence of all changes in case of a formal dispute. Be particularly careful to track service-level breaches that could lead to compensation arrangements (e.g., service credits) and, ultimately, contract termination.

Termination. Termination can occur in two ways: The contract comes to an end or the contract fails. In either case, the outsourcer must be able to take control of any vital assets so that it can start running the outsourced process again itself or, alternatively, re-let the contract — possibly to an alternative service provider. The outsourcing agreement should therefore provide for the retransfer of assets and rights to the outsourcer (or its nominee). Full transition planning should be built in, as splitting mixed systems and processes can be time consuming. If you do not adequately plan for termination and allow sufficient time for any retransfer process, your company could find itself in a weak commercial position when trying to use its rights on termination.

As the commercial world changes, outsourcing will remain a key business tool. Although outsourcing is becoming increasingly complex, the basic tenets outlined can help you make a success of outsourcing. 

Outsourcing – IT Dinosaur or State of the Art?

By BERNARD E. LANKES, SUN MICROSYSTEMS AUSTRALIA

The true cost savings delivered by outsourcing are far from reaching widespread claims of over 60 percent. In reality, the net savings range only between 10 and 39 percent. Nevertheless, the first quarter of 2006 was the strongest quarter ever for outsourcing contracts in Europe, according to The Shared Services and Business Process Outsourcing Association (SBPOA) (*TPI News*, 26-May-2006).

According to SBPOA, in the first quarter of 2006, 83 contracts were signed with a collective value of more than €18 billion compared to 76 deals with a collective value of €13 billion at this time last year. Even if you don't take the 19 restructuring contracts into account, the remaining 64 contracts are valued at €12.1 billion.

Long gone are times when only manufacturers transferred responsibilities for an internal business function to an outside service provider. These days, even law firms sign outsourcing deals. For example, Allen and Overy, which has 4,800 employees in 25 countries (one of the world's largest law firms), signed a

"Bit Pound" 5.5 million British Pounds deal with service provider SAVVIS in January of this year. Under this five-year contract, Allen and Overy outsourced networks and IT infrastructure — including document management, data transfers, accounting, and email — in order to move its data centre away from risk and to gain a high-availability network. SAVVIS also runs much of Wall Street's networking.

Defining Outsourcing Trends

To provide a "one size fits all" definition is a mission impossible, as the term "outsourcing" is controversial and has been used to describe many types of business activities. Related terms include "large-scale outsourcing," "outtasking," and ASP. ASP, meaning Application Service Providing, is also known as Software Outsourcing: Software is delivered via VPN (Virtual Private Network) and paid per hour of the use instead per license. ASP will not be considered in more detail in this article.

Generally speaking, "outsourcing" is when a company transfers responsibilities for an internal business function to an outside service provider. Providers often purchase assets, license software, or hire people that perform the company's function. The transfer of the responsibilities can happen as a whole ("total outsourcing"); or it can happen in parts and sometimes even to various providers ("partial outsourcing or outtasking"), which seems to be the latest trend. In partial outsourcing, it's the company's obligation to manage the relationship between the various providers as to desktop services, call center, host service, and so forth.

The areas subject to outsourcing are getting more complex. A couple of years ago everyone started with outsourcing of IT infrastructure: e.g., the data centre, telecommunication, WAN/LAN. Then people began to transfer IT processes to the provider, a step also known as Information Technology Outsourcing (ITO). Examples of areas suitable for ITO are problem management, desktop management, and release management. I'm positive that many of you have had significant experience in calling the "resolution centre" around the globe for help on laptops or other IT troubles — with varying results! Finally there



is Business Process Outsourcing (BPO). In BPO, a company outsources non-IT business functions, e.g., call centre, payroll or other HR functions, or training.

There is a growing trend of offshore outsourcing. Offshore outsourcing (or "offshoring") is when a company in a high-wage country outsources to a provider that will perform most of the services in a low-wage country. The downsides of offshoring include added telecommunication costs, management challenges, and legal risks. Offshoring to India is extremely popular due to the skilled employee pool, the infrastructure to support outsourcing, and favorable tax regimes. Less well known is offshoring to China, which offers challenges such as employee issues and IP registration. Recently, a number of offshoring deals in Russia have been announced.

Risks and Benefits

Would I recommend entering into an outsourcing deal? It depends. Outsourcing offers three critical benefits to your company: It allows the company to focus on its core function; benefit from enhanced performance from the provider's specialization; and take advantage of improvements in technology. Be cautious about claims that outsourcing will reduce your overhead costs, as your company might have to face added costs associated with managing the provider, such as telecommunication expenses.

Outsourcing's downsides include the loss of day-to-day management control of outsourced services, the dependence on the provider's performance, the loss of skilled employees and assets transferred to the provider, and finally, having to reassume responsibility for the outsourced services upon termination of the contract.

You can group outsourcing's legal aspects into three areas:

- the outsourcing agreement (e.g., warranty, indemnity, IP ownership);
- special regulatory questions (e.g., labour law, tax law, data privacy); and finally,
- problems peculiar to outsourcing services (e.g., whether work is within the contract's scope, crafting service-level agreements (SLA), monitoring and controlling the contract performance).

According to my own experience, outsourcing can work if there is a real partnering mentality on both sides and not just an emphasis on short-term cost reductions.

Outsourcing Project Phases

An outsourcing project can be divided into at least four phases: the decision-making process, planning, implementation, and finally the provision of the services (including termination procedures). Every phase has its essential contract clauses, highlighted in "Steer Clear of Traps," below.

In a very early stage, the decision maker has to develop a vision of the potential outsourcing project and define its strategy.

The next phase is by far the most critical for the outsourced project's success. It consists of: the assessment of the situation; the make or buy decision; the definition of the project; the selection of the provider; the conclusion of an NDA (nondisclosure agreement) and Lol (Letter of Intent); and the analyses of the business and current IT processes.

The provider selection process will focus especially on workforce quality issues, such as the education, language skills, culture, and work ethic of the provider's employees. If offshoring, infrastructure issues will also be important. Infrastructure may cover such matters as political stability, currency, and fluctuations. The company may consider placing a Request for Information (RFI) to receive the provider's information, qualifications, references, and so forth. In a further step, the company may create a Request for Proposal (RFP) to benchmark outsourcing objectives, services to be provided, and pricing.

The third phase — implementation — also offers challenging legal problems, including the transfer of employees and software, hardware transfer financing queries, and the legal construction of SLAs.

Finally, the last phase — the provision of services (the operation phase), including termination procedures — requires a number of conditions on data privacy, IP property rights, change management, benchmarking, and service disruption and termination.

Steer Clear of Traps in Your Outsourcing Agreement

It is best to have a head agreement with various contracts underneath, such as service performance contracts and transfer contracts. Due to the complexity and the sheer size of any outsourcing project, one document that tries to cover all terms at once won't work. The head agreement should cover all terms that apply generally, whether to service performance contracts or to transfer contracts. (Service performance contracts deal with topics such as maintenance and LAN/WAN. Transfer contracts cover the transfer of employees, software, and hardware.) And finally, there will be a group of contracts that cover infrastructure, data privacy, and so forth. In case of contradiction between the various documents, I recommend installing a hierarchy of documents according to which the specialized contracts prevail with regard to the head agreement.



The head agreement will typically cover the classic terms and conditions, such as definitions, warranty, limitation of liability, and change management. Especially important for offshoring are defining the parties and verifying that the party representing the provider does in fact have the power to do so. In an international agreement, determining the applicable law is key.

As the customer, the company may choose the law with which it is most familiar. Having said that, any outsourcing agreement implemented in a foreign legal system must consider the provider's local law in areas such as copyright, software protection, export control, customs, currency, and tax. Equally important are the provisions relating to the enforceability of the agreement. It's essential

to choose a competent court. Make sure that there is a bilateral treaty on the enforcement of judgments of state courts between the company's home country and the country where most of the services will be provided. Even language may be the subject of a clause. If the contract is bilingual, the contract should define one language as preemptive. As a rule, the prevailing language should be an official language of the competent court.

Examples of service performance contracts under the head contract include maintenance contracts, procurement contracts, user help desk contracts, and operation of ERP applications (enterprise resource planning software, such as SAP, Siebel). Service performance contracts should divide the risk between the parties. The first part of a service performance contract typically defines the scope of the provider's services, e.g., second-level PC support, typically including the determination of the risk transfer and the prerequisites and the obligations of the company. The remainder of the contract sets out the SLAs, i.e., the quantifiable and qualitative determination of the services. The services need to be described in detail, including how their performance is to be measured. For example, a quantifiable target could be the resolution of 90 percent of the cases per month within 4 hours. A qualitative target could be 90 percent customer satisfaction per month. The contract should also cover evaluation of the measurements and the consequences such as penalties and/or bonus. Defined service levels and performance requirements are key for the success of any outsourcing project. Transfer contracts cover the acquisition of hardware and software by the provider as well as the transfer of employees.

According to European law, e.g., Para 613a BGB (German Civil Code), some countries are automatic transfer jurisdictions. Would-be providers should be wary: In an automatic employee transfer jurisdiction, no offer and acceptance is required between the employee and the provider before the provider can "inherit" quantities of new employees from the outsourcing company! In addition, the company might be required to notify employees in advance on the timing of the transfer, its reason and legal and economic consequences.

In some countries such as Germany, the approval of the workers' council is essential. We have seen a number of outsourcing plans

fall apart at the very last minute because the workers' council was either involved too late or not at all. According to law in many EU countries, the provider has to guarantee the same terms and conditions for at least one year, including the same benefits levels for the transferred employees. Furthermore, the provider is unable to terminate their employment contracts for 12 months. As an alternative, the provider might like to reach agreement with the employees being transferred to terminate their existing employment contracts in favor of new ones. This is the only way the provider can get rid of the benefits level of the current employer, i.e., the outsourcing company.

Equally demanding is the transfer of software from the company to the provider. If the company is transferring its proprietary software so that the provider can create an update or documentation, then the company must impose conditions to ensure that the IP is safe from third-party theft or infringement. These conditions would include the assignment of inventions, the transfer of ownership, and the enforcement of such agreements not only between the provider and the customer, but also between the customer and provider's employees. But if the company wishes to transfer its right to use third-party software, often it will first have to obtain prior written consent.

The transfer of hardware often raises financing questions. Alternatives might be to purchase, rent, or lease. There are at least two leasing models available: operating leasing and technology leasing. In a technology lease, the company sells its IT assets to the provider. The provider then sells those assets, as well as new hardware, to a leasing company. The leasing company in turn leases the new hardware and the company's IT assets back to the provider. This enables the provider to deliver hardware and services as "full-service leasing" to the company.

Of course, a thorough review under tax and balance-sheet aspects is essential to evaluate the overall tax impact of the outsourcing project on the company. This review is particularly important with respect to transfer contracts, though of course it is significant for the project as a whole.


The last group of agreements under the head outsourcing contract includes the infrastructure and data privacy contracts. With the infrastructure contract, the

company allows the provider to use the company's premises and to use its LAN, telecommunications, and other equipment in order to deliver the services for the company. In this contract, the company's deliverables should be described as thoroughly as those of the provider. The amount paid by the provider for use of the infrastructure should be relatively low, as this use will be mirrored in the provider's business case and therefore be paid by the company at the end of the day.

Data privacy is a serious matter, especially when it comes to offshoring. Various European laws might require a company to protect the privacy of its customers' data. Consider any of the relevant data protection law that might be triggered by the outsourcing; for example, some countries regulate data transfer to an "unsafe jurisdiction." In addition, according to (for example) German law, the provider has to guarantee that its employees and contractors are obliged according to Para 5 BDSG, the German data privacy law, and furthermore that the provider has taken all necessary technical and organisational steps to ensure conformity with the BDSG, Para 9 BDSG.

Finally, when you prepare your outsourcing agreement, be sure to prepare a plan to disengage and transition the service in the event of the provider's insolvency, failure to perform, or changed business conditions. Your plan should include provisions for disaster recovery, force majeure, exit planning, termination procedures, termination fees, dispute resolution (including escalation management), and transition to a successor. It is much easier to agree on these clauses during the contract negotiations than to do so later, when the relationship is in danger.

Look Before You Leap

Outsourcing can be a great benefit to the company and the provider. But you should not jump into outsourcing without doing a complete business, financial, and legal analysis. Benchmarking competitors might be helpful in order to understand their experience, especially when it comes to offshore outsourcing. Keep in mind that outsourcing is not risk-free. Consider the total cost of ownership of outsourcing, not just any reduction on labour costs. Both parties have to approach outsourcing as a kind of partnership, not as a one-sided deal with a vendor. 

(For more information on outsourcing, see [inter alia](http://www.e-oa.net) the website of the European Outsourcing Association, www.e-oa.net.)

Ad-ding Up Correctly

CAROLYN BOYLE, INTERNATIONAL LAW OFFICE

In today's crowded marketplace, companies must go to ever-greater lengths to protect their brands, outplay the competition and win the hearts and minds of the purchasing public. Refereeing the melee in the advertising sector are the competition authorities and courts, which have recently blown the whistle on unfair marketing practices to ensure that consumers are not misled, competitors do not resort to dirty tricks and the playing-field is kept level for all participants.

In Latvia, the Competition Council is charged with monitoring advertisements to ensure compliance with the Advertising Law. Where the law is breached, the council can order the advertiser to rectify the situation - for example, by removing certain elements from the offending ad, or by retracting or ceasing to distribute it. The council also has the power to impose administrative fines on infringers; but while this remedy has been available since the law's enactment in 2000, the council failed to avail of it until relatively recently.

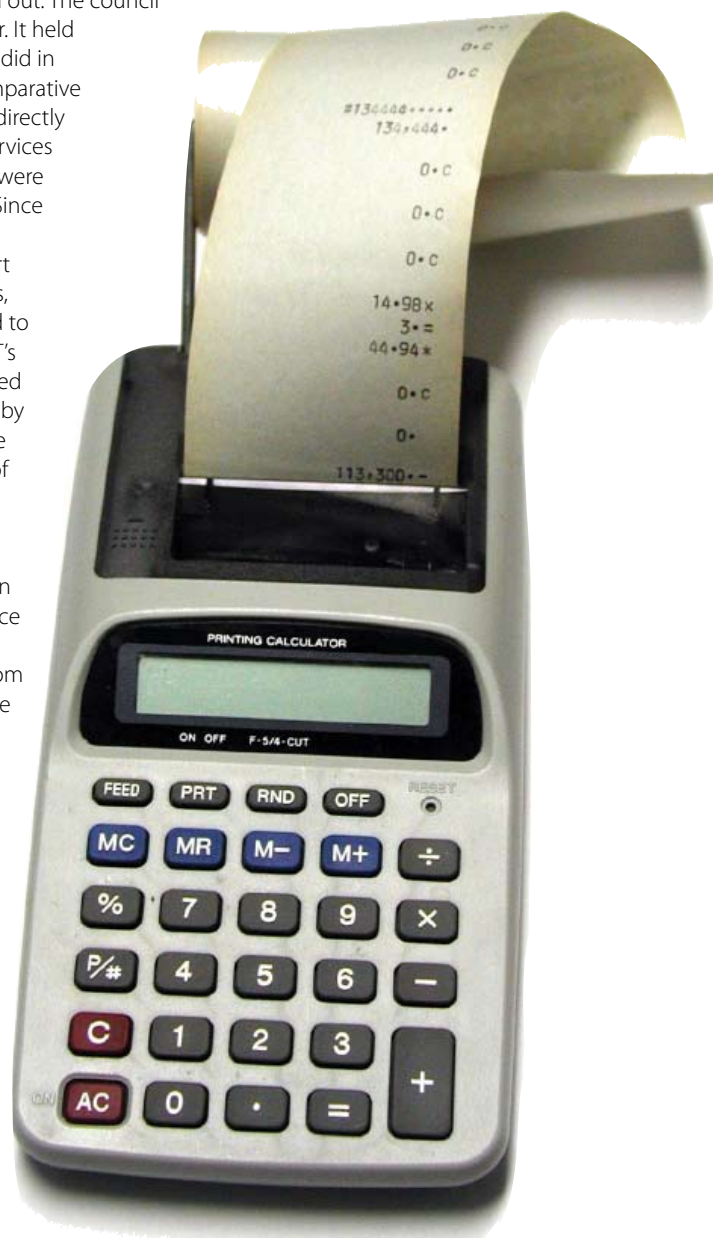
The first indication that the council was adopting a tougher stance toward unfair advertising came last year, when crisp manufacturer Lay's was fined for a slogan which asserted that "Six out of 10 people choose Lay's". The council ruled that the limited research on which Lay's based its slogan was insufficient grounds for such a sweeping claim, and that product testing and verification results presented in the ad were confusing and could be misinterpreted. The council therefore held that the slogan was without objective justification and took the unprecedented decision to fine Lay's for the breach. (Ref 11372)

Lawyers at Loze, Grunte & Cers note that the **Lay's** ruling marked the opening salvo in a new crusade against misleading advertising. Telecommunications companies have fast become some of the most persistent petitioners to the council in this respect, as the intense competition generated by liberalization and the advent of number portability has forced rival operators to dream up increasingly innovative ways of capturing public attention. The latest skirmish involved a high-profile advertising campaign launched by mobile operator LMT, which claimed its services were the most reliable and secure available, using emotive slogans such as "Why choose insecure communications?".

Disgruntled competitor Tele2 brought the matter to the attention of the council, complaining that the ads were misleading and disparaged the services of other providers. LMT counter-argued that the ads merely extolled its own merits rather than denigrating competitors, and were not comparative because no particular operator or competing service was singled out. The council disagreed, however. It held that the campaign did in fact constitute comparative advertising, as it indirectly implied that the services of other operators were somehow unsafe. Since LMT could offer no evidence in support of these allegations, the ads were found to be misleading. LMT's claims further preyed on consumer fears by suggesting that the health or security of those who signed up for competing services might be compromised — an unfounded inference which could drive customers away from other operators. The council thus found that the campaign was in breach of the Advertising Law, and ordered LMT to cease distribution of the ads and issue retractions across the media. In keeping with its new hard-line approach to advertising offences, the council additionally imposed an administrative fine. (Ref 12422)

India's Monopolies and Restrictive Trade Practices Commission is also keeping a close eye on the national media to ensure that competitors do not hit below the belt in their advertisements. Manisha Singh of Lex Orbis reports that pen manufacturer Cello was recently in the dock for a television ad that

depicted its Maxriter model beating another pen in an endurance race: while the challenger broke down after 2,000 metres, the Maxriter continued writing for 4,000 metres and was crowned the winner. Rival company GM Pens insisted that the design of the losing pen was not mere coincidence: with its distinctive white body and transparent blue tip, it closely



resembled a well-known GM Pens model. GM Pens further questioned Cello's contention that the Maxriter could write for 4,000 metres as claimed. The commission duly issued a temporary injunction prohibiting Cello from screening the ad or disparaging the products of GM Pens, and recently confirmed the injunction. In its final ruling, the commission held that although the name


of the losing pen was not indicated in the ad, the pen depicted was clearly the GM Pens model. Moreover, after analyzing the results of tests conducted by both manufacturers, the commission concluded that there was insufficient proof of the alleged durability of the Maxriter. The ad thus not only denigrated GM Pens' products, but also made a false claim. Cello was thus ordered to pull the ad and to refrain from making any further allusions to the products of GM Pens in its advertising materials. (Ref 12399)

Equally, however, competitors that unfairly cry foul in an attempt to stifle successful marketing strategies will be given short shrift, as a recent decision of the Venezuelan competition authority reported by lawyers at Travieso Evans Aria Rengel & Paz demonstrates. Once again, the dispute involved participants in the hotly contested mobile telephony sector. Corporación Digitel, the third-ranking player on the market, accused industry leader Movistar of ripping off a longstanding campaign through which various Digitel services were advertised using slogans ending in the word 'me' (eg, "Call Me", "Take Me", "Transfer Me"). When Movistar revamped its image through a pervasive media campaign incorporating similar expressions, Digitel claimed this unfairly took advantage of the reputation and loyalty it had cultivated through its own ads. In its defence, Movistar explained that its campaign had been rolled out simultaneously across 13 Spanish-speaking jurisdictions and did not deliberately target Digitel. It further observed that the Digitel campaign had dropped off the public radar in the last couple of years, as Digitel was spending less on promoting it. Finally, Movistar highlighted the incongruities in Digitel's allegation: a well-established market leader simply would not waste valuable resources in devising a campaign to exploit the reputation of a relative minnow with fewer customers and a narrower geographic reach. The competition authority found these arguments persuasive and dismissed Digitel's complaint. (Ref 12008)

Of course, it is not only competitors to which crafty advertisers often allude — whether directly or covertly, positively or negatively — in order to boost their own appeal. Back in Europe, a string of glittering events in the international sporting calendar has triggered a crackdown on 'ambush marketing', through which brand owners associate themselves unofficially with prestigious sporting events in a bid to capitalise on the consumer and media

interest they generate. Such strategies are detrimental not only to the companies that shell out millions for the privilege of official affiliation, but also to event organizers, which struggle to attract future funding when the voices of sponsors are drowned out by the clamour from ambush marketeers. Italy led the field by introducing legislation to frustrate opportunistic advertisers ahead of the 2006 Winter Olympic Games, held in Turin this January. According to the IP team at Trevisan & Cuonzo Avvocati, the law reserved the right to use the world-renowned Olympic symbols strictly to the official committees and agencies that organized the games, as well as to third parties granted written authorization by the International Olympic Committee. The use of distinctive signs which could mislead consumers into assuming a correlation between the relevant goods or services and the games was prohibited, and ambush marketing was expressly forbidden. Breach of the law was made punishable by administrative fines of up to €100,000, on top of the usual remedies available for trademark infringement. (Ref 12068)

Although there are some years to go before the 2012 Olympics kick off in London with the usual lavish opening ceremony, the UK government has wasted no time in putting in place a legal framework to deal with ambush marketing. Under the Olympic Symbol (Protection) Act 1995, the use of Olympic symbols and mottos is already the exclusive preserve of official Olympic bodies and duly authorized third parties. This protection has now been consolidated by the London Olympics Act, which establishes a new 'London Olympic association right' to protect signs relating specifically to the 2012 games. Any unauthorized party that uses in the course of trade images, words or combinations of words which might create some association with the games in the minds of the public will be held in breach of the act and subject to administrative penalties. The enactment of further regulations on advertising and street trading is also anticipated as the games draw near, in order to reflect potential policy shifts or changes in Olympic venues. (Ref 11307) Again, however, overzealous attempts to protect event brands will not be tolerated. FIFA's 2003 registration of the marks FUSSBALL WM 2006 and WM 2006 invited three separate challenges on the grounds that the marks were descriptive and lacked distinctive character; Maiwald Patentanwalts' Stephan Schneller and Andrea Lasar explain that 'fussball' means 'football', while 'WM' stands

for 'Weltmeisterschaft', translated as 'world championship'. The Patent and Trademark Office concurred with the opponents that the marks were mere references to the 2006 World Cup and duly cancelled the registrations. On appeal to the Federal Patent Court, FIFA pointed to its monopoly as the World Cup organizer and contended that the marks had achieved distinctiveness through use in connection with the event. In the court's view, however, the marks should remain publicly available to describe the tournament. Finding that the marks had only been used together with the FIFA name, and that a clear majority of the public did not connect them with FIFA, it cancelled the marks in relation to all goods and services except merchandising. Even this lifeline was snatched from FIFA's hands upon further appeal to the Federal Supreme Court, which cancelled the FUSSBALL WM 2006 outright and sent the WM 2006 back to the Federal Patent Court for further examination of distinctiveness in relation to merchandising. By ambitiously seeking to over-extend its influence over the World Cup brand, FIFA appears to have scored something of an own goal. (Re f 12475) 

A full discussion of any of these topics can be accessed at the International Law Office website by inputting the four-digit reference number at www.internationallawoffice.com/archive.cfm

Save the Date

Don't miss these important ACC Europe Chapter Events.

15 Sep 2006 European Law Update 2006
– Frankfurt

21 Sep 2006 Arbitration – Brussels

28 Sep 2006 Conducting Internal
Investigations – Practical Guidance
– Munich

1 Oct 2006 Electronic Disclosure – London

1 Oct 2006 Whistleblowing – Paris

Visit www.acca.com for complete details

Looking Ahead: Topics Covered in Forthcoming Issues of European Briefings

December 2006 – Insolvency/Chapter 11

March 2007 – EU Labor Law

June 2007 – Whistleblowing

September 2007 – Non Disclosure Agreements

European Briefings Key Contacts

We welcome your comments about European Briefings and are always interested in finding out what topics you would like to see addressed in future issues. Please send your comments, ideas, and indication of your interest in writing for European Briefings to: Ken Lawrence, Director of Publishing, Association of Corporate Counsel, Lawrence@acca.com