EU outsourcings: data security and privacy issues

Anthony Nagle, Morrison & Foerster

www.practicallaw.com/7-385-0565

An EU outsourcing transaction often involves the cross-border transfer of personal data to countries outside the EU. In this regard, the relevant EC legislation is the Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) (Directive), and particularly its security and adequacy requirements.

This chapter focuses on current privacy considerations and compliance requirements concerning EU-originated cross-border outsourcing transactions, as well as the key developing privacy issues or trends affecting such transactions. It begins with a brief overview of the nature of outsourcing transactions and the types of personal data typically involved in such transactions. It then examines the three main concerns that arise in any cross-border outsourcing transaction:

- Establishing who the data controller and the data processor are (*Article 2, Directive*).
- Ensuring that the outsourcing contract contains the appropriate security measures and complies with the security requirements of the Directive.
- Complying with the applicable data protection transfer provisions in respect of transfers to countries outside the European Economic Area (EEA).

OUTSOURCING AND PERSONAL DATA

Outsourcing has been described as an arrangement of any form between a customer organisation and a supplier organisation by which the supplier performs a process, service or an activity that would otherwise be undertaken by the customer itself. There are many different reasons why customers decide to outsource, but often the basic commercial proposition is that the customer wants the supplier to do what the customer currently does for a lower price and at the same or better level of service.

There are many types of outsourcing transactions. For example, a typical IT outsourcing transaction (ITO) might involve the sourcing of:

- IT infrastructure, a local area network (LAN) and wide area network (WAN).
- Desktop services.
- Data centre services and application development.
- A help desk.

On the other hand, a business process outsourcing transaction (BPO) involves the contracting of responsibility of specific business functions to a supplier, which might involve the sourcing of:

- Back office functions, such as:
  - logistics;
  - payroll services;
  - benefits administration; and
  - recruitment and staffing services.
- Front office functions, such as:
  - customer services;
  - technical support;
  - marketing and advertising; and
  - HR.

Outsourcing transactions usually involve the transfer from the customer to the supplier of, for instance, budget and financial information, various physical assets (for example, hardware and servers), intellectual property rights and, of course, personal data.

The two main types of personal data in an outsourcing transaction are likely to be:

- **Employee data.** Personal data is transferred to the supplier if the customer's employees transfer to the supplier under Directive 2001/23/EC on safeguarding employees' rights on transfers of undertakings, businesses or parts of business (Acquired Rights Directive). This normally involves the transfer of employees' terms and conditions, service histories, performance and appraisal information and sensitive personal data, such as sickness records, to the supplier.
- **Customer data.** This is personal data relating to the customer's corporate clients and customers. It is probably going to be the most critical and important personal data transferred to the supplier as part of the outsourcing arrangement because it is usually "high volume", valuable and will almost certainly relate to the core business of the customer.

As suppliers' global solutions for their customers in the current outsourcing environment continue to adapt and change to meet

their customers' global business operations and needs, personal data transferred to suppliers is often likely to reside in the suppliers' databases and servers inside and outside of the EU.

Indeed, many EU-based suppliers operate "follow-the-sun" type flexible sourcing models where around-the-clock seamless support is provided to the customer's clients. As a result, the personal data may be transferred or made available to the supplier's other data centres around the world so that as one data centre goes offline another data centre will pick up responsibility for the next shift and continue to service the customer's clients wherever they are in the world. Customers handling EU personal data need to ensure they comply with their legal obligations in respect of transferring such personal data to countries outside the EU.

DATA CONTROLLERS AND PROCESSORS

The Directive has been implemented into local laws by EU member states (for example, the UK implemented the Data Protection Act in 1998 (DPA)). Under the Directive, a customer outsourcing personal data is treated as the "data controller" and the supplier is treated as a "data processor" (but see box, *The SWIFT case*). The data controller is basically the entity or organisations which "alone or jointly with others determines the purposes and means of the processing of personal data", while the data processor is the entity or organisation that processes personal data on behalf of the data controller (*Article 2, Directive*).

From a customer perspective, the customer must ensure that its outsourcing contract does not somehow give ownership of its personal data to the supplier or it does not set up the contract in such a way that the supplier will be deemed to be a data controller under the definitions of the Directive. Likewise, the supplier needs to be careful in the way it operates the services and the underlying data handling processes it has contracted to carry out under the outsourcing contact. It must ensure it does not take on the role of determining the purposes and means of processing because, if it does, the supplier will be required to comply with the Directive as a data controller.

Given that the Directive makes the data controller (that is, the customer) responsible to the relevant individuals (that is, the data subjects) (*Article 2, Directive*) for any unlawful processing of their personal data (including the acts or omissions of suppliers processing personal data under an outsourcing transaction), the onus is on the customer to ensure that its outsourcing arrangements remain compliant with the Directive. In this regard, it must ensure that any necessary requirements of the Directive flow down to the supplier in the outsourcing contract along with appropriate liability and breach provisions.

The Directive also prohibits an organisation from carrying out any processing of personal data until it has notified the relevant supervisory authority in the relevant member state (*Article 18, Directive*). As a result, notification is a statutory requirement across all the member states. For example, in the UK, a data controller must register with the Information Commissioner's office (ICO) unless it is exempt, and failure to notify is a criminal offence. Once notified, basic information about the type of processing that will be carried out along with other basic details of the data controller are made available for public inspection, including a register of data controllers.

THE SWIFT CASE

For the last decade or more, the traditional assumption in the UK has been that suppliers are always data processors if they operate under the instructions of the data controller via the terms of the outsourcing contract. However, this assumption was turned on its head in the SWIFT case (*Article 29 Working Party Opinion No.10/2006 (Processing of personal data by the Society of Worldwide Interbank Telecommunication (SWIFT)*).

SWIFT was a Belgian company facilitating international money transfers for financial institutions. It transferred financial data to its US operations and the financial information was accessed by the United States Department of Treasury under various subpoenas. Under the Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) (Directive), the US is not deemed to be a country offering adequate protection for personal data. As a result, such data transfers to the US were in breach of Article 25 of the Directive. SWIFT argued that it was merely the data processor, and therefore it could not be in breach of the Directive.

The European data protection authorities initially held that even if they assumed that SWIFT acted as a data processor (as the contractual privacy provisions between SWIFT and the banks and financial institutions was not clear cut), SWIFT had taken on further responsibilities that went beyond the original set of instructions and duties it had as a data processor. Accordingly, it was held to be a joint data controller (that is, with the financial institutions) and liable for compliance with EC data protection laws.

However, by the time the case was finally determined by the Belgian data protection authorities towards the end of 2008, it was concluded that the financial institutions were the data controllers and SWIFT was the de facto delegate and data processor of such financial institutions.

Although SWIFT was eventually deemed to be a data processor, the lesson to be learnt here, and particularly in long-term outsourcing arrangements, is that suppliers need to be alert to changes in the day-to-day processing operations they perform for their customers. Such changes might take them outside their initial contracted role as data processors; if such activities mean they unintentionally become data controllers, they will take on the burden of having to achieve full compliance with the Directive as well as the consequences of failing to comply.

SECURITY OF PROCESSING AND OUTSOURCING TRANSACTIONS

A data controller must put a written contract in place if a data processor is carrying out any processing on the data controller's behalf (*Article 17, Directive*). The contract must require the data processor to act only on the instructions of the data controller. Due to the inherent complex nature of outsourcing transactions, complying with this provision should not be difficult for customers as a contract is always required in an outsourcing arrangement between a customer and a supplier.

SECURITY: GOOD PRACTICE DEVELOPMENTS

ISO 22307:2008: Financial services

In the early part of 2008, the International Organisation for Standardisation (ISO) issued a new privacy standard for financial data. According to the ISO, ISO 22307:2008 will help private and public sector organisations identify and mitigate privacy issues and risks associated with processing financial data of customers or consumers using automated, networked information systems. The privacy impact assessment (PIA) described in the standard should be carried out "at an early stage in the development of a proposed financial system". This is the type of management tool that organisations will use to capture the necessary security protections in their outsourcing contracts with third party suppliers. Undoubtedly, banks and other financial institutions will begin requiring their suppliers to comply with ISO 22307:2008 in future outsourcing transactions.

Encryption

Encryption can protect data by rendering it unreadable to unauthorised users who do not have the access key. Although the Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) (Directive) does not specifically mention encryption, data protection authorities around Europe are beginning to recommend encryption as a:

- Necessary security measure for transfers involving critical personal data.
- Means of complying with Article 17 of the Directive.

For example, in the UK, in 2008 guidance provided by the Information Commissioner's Office (ICO), it has been recommended that portable and mobile devices (including memory sticks) used to transfer or hold personal data (the loss of which could cause damage or distress to individuals) should be protected using appropriate encryption software. Already, specific provisions are being included in outsourcing contracts requiring, for example, the encryption of suppliers' employee laptops (or consultants and contractors who may also have access to the information) and the encryption of sensitive personal data via e-mail.

Incident response plans

In the UK, in March 2008, the ICO published a note on good practice (*Guidance on Data Security Breach Management*). The note provides guidance on the appropriate course of action that organisations should take once a data security breach occurs. The note specifies four steps:

- A recovery plan should be prepared and put in place, which should include damage limitation measures.
- An assessment of any ongoing risks associated with the breach should be undertaken.
- The organisation needs to decide if the breach should be notified to the ICO.
- An organisation should not only determine the cause of the breach but the effectiveness of the organisation's response to that breach.

The impact of this guidance on outsourcing transactions is that customers will be seeking to incorporate the supplier's good practice in this area as a contractual commitment and obtain appropriate remedies in cases where the supplier fails to comply with such a commitment.

A more difficult requirement for the customer is to identify (and incorporate into the contract) and negotiate with the supplier, the most appropriate security measures required to keep the relevant personal data safe and secure (*Article 17, Directive*). Data controllers "must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing" (*Article 17, Directive*).

This means that the customer, as part of the negotiations and the due diligence phase before contract signature, needs to establish the appropriate security measures that it requires the supplier to put in place.

For example, the corresponding Directive provisions implemented in more detail in the UK (provisions relating to the seventh data protection principle under the DPA), require the data controller to take account of the state of technological development and the cost of implementing any measures to ensure a level of security appropriate to:

- The nature of the personal data that is to be protected.
- The harm that might be caused if the relevant personal data was unlawfully processed or lost, and so on.

To incorporate appropriate security measures into the outsourcing contract, the customer may often be guided by good industry practice in respect of keeping the relevant data secure. For example, it may choose to apply an appropriate International Organisation for Standardisation (ISO) security standard along with other detailed security measures set out in its organisation's security policies and other related compliance documentation (*see box, Security: good practice developments*).

The UK's DPA, in compliance with the Directive, requires that, in addition to building appropriate security measures into the outsourcing contract, the customer must obtain sufficient guarantees about the technical and organisational security measures governing the processing that the supplier will carry out. The best way to do this is to negotiate such guarantees into the outsourcing contract.

The Directive also makes it clear that for the customer to be compliant, it must take reasonable steps to ensure the supplier

remains compliant with those security measures. The best way to be able to demonstrate this is by including into the outsourcing contract, for example:

- Regular security testing and assurance obligations.
- Audit and access rights for the customer.
- Detailed security reporting obligations that the supplier must follow.
- Security and governance meetings.
- Site visits to the supplier's premises.

The DPA also requires customers (as data controllers) to take reasonable steps to ensure the reliability of the supplier's employees who have access to the personal data. This would apply regardless of whether the supplier's employees are in the EU or, for example, operating out of a processing centre in India.

TRANSFER OF DATA OUT OF THE EEA

Another issue that the customer in an outsourcing contract must address is whether a transfer outside the EEA meets the Directive's requirements relating to "adequacy" (*Article 25, Directive*).

The Directive and the local implementing legislation in member states contain strict rules on exporting personal data outside the EEA. These rules also catch intra-group transfers between, for example, an organisation based in the EU that is transferring personal data to its affiliate companies in countries outside the EEA that are processing on its behalf.

The basic principle of Article 25 of the Directive, as implemented by local legislation in the member states, is that personal data must not be transferred to a country or territory outside the EEA unless that country or territory provides an adequate level of protection for the rights and freedoms of the individuals whose personal data is being transferred. The data controller, of course, must always remember that it still needs to have a legal basis for processing in the first place (that is, the personal data must be processed fairly and lawfully), which is one of the basic tenets of the Directive and which has been implemented into the local implementing legislation across the member states.

The obvious upside from a European perspective is that Article 25 does not have an impact on data transfers within the EEA and, therefore, there is a free-flow of personal data in outsourcing transactions within the "four walls" of the EEA.

At first glance, Article 25 is potentially highly problematic. However, there are a number of established approaches to legitimising a transfer of personal data to countries outside the EEA, some of which are more preferable and suitable for outsourcing arrangements than others. These options are:

- Adequacy.
- Model contracts and ad hoc contracts.
- Binding corporate rules (BCRs).
- The "Safe Harbor" scheme.
- Derogations.

Adequacy

The European Commission can make a finding that a particular country does, or does not, ensure adequacy in terms of protecting personal data (*Article 25(6), Directive*). If an outsourcing data transfer from the EU is to one of the approved countries, the customer does not need to worry about compliance with Article 25 of the Directive but it will still need to ensure that it complies with all the other data protection principles, in particular the security requirements under Article 17 of the Directive. To date, the following countries have been approved by the Commission: Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Jersey and Switzerland.

The more countries that are added to the approved list in the years ahead, the easier it will be for customers and suppliers alike because, for those approved countries, they will no longer have to worry about the prohibition on transfers under Article 25.

The Directive allows data controllers to self assess the adequacy position of a country to which it wishes to transfer personal data (*Article 25(1), para 1, Directive*). In effect, this is no different an approach than the data controller assessing that it has put the most appropriate security provisions in place to meet the requirements of Article 17. However, not all member states (for instance, France and Spain) have allowed data controllers in their jurisdiction to take such an approach and have directed them to use one of the other means available in terms of complying with the adequacy requirements of Article 25.

The Directive describes the criteria that need to be factored into an assessment of adequacy for a third country outside the EEA, such as (*Article 25(2)*):

- The nature of the personal data.
- The purpose and duration of the proposed processing operations.
- The country of origin and the third country of final destination.
- The rules of law in force in the third country of final destination.
- The professional rules and security measures that are complied with in that third country.

Within those member states in which self assessment is acceptable, there are many different approaches taken. As a result, not only would it be difficult for a customer to determine categorically (after having carried out the self assessment in good faith) that adequacy exists in a complex long-term outsourcing arrangement involving transfers to one or more third countries, but there would be no legal certainty in the approach across member states. If more than one third country is involved in the outsourcing arrangement, then self assessment is not feasible.

In practice, due to the value of outsourcing contracts, the risk to client and customer data and the resulting reputational damage for the customer if data is lost or damaged, as a matter of good practice, customers want to rely on a safer method of achieving adequacy.

Accordingly, self-assessment is rarely raised as an option for debate during the negotiation phase of outsourcing transactions.

The other practical consideration due to the risks involved, of course, is that it would be difficult to obtain internal corporate sign-off within the customer organisation or sign-off from the consultants and other advisers (working on the transaction) if self assessment is the only proposed method of complying with the Directive's adequacy requirements.

Model and other ad hoc contracts

Another method of legitimising the transfer of personal data outside the EEA is the Commission approved "model contracts" (an approved means of compliance under Article 26(2) of the Directive). These are standard contracts that cannot be amended should the customer wish to rely on them. Although there are certain drawbacks with these contracts for both customers and suppliers, use of the model contracts is one of the more common ways customer organisations tend to achieve compliance with Article 25 of the Directive.

To date, the Commission has approved the following types of model contracts governing the transfer of personal data from a data controller within the EEA:

- To a data controller outside the EEA, the model contract approved by Commission Decision 2001/497/EC15, dated 15 June 2001, and an alternative version of the model contract approved by Commission Decision 2004/915/EC17, dated 27 December 2004.

- To a data processor outside the EEA, the model contract approved by Commission Decision 2002/16/EC16, dated 27 December 2001.

In an outsourcing arrangement, the customer is the data controller and the supplier is the data processor and, therefore, the latter type of model contract is relevant. This is commonly known as the "Controller to Processor Model Contract".

As the Controller to Processor Model Contract is uniform across all the member states, this can be beneficial for a multinational company outsourcing elements of its businesses within Europe to a supplier outside the EEA. From a contract management, uniformity and security perspective, this model contract represents a relatively straightforward way of managing and remaining compliant with the transfer requirements of Article 25 of the Directive.

However, there are a number of drawbacks with the Controller to Processor Model Contract, which have been criticised by not only the outsourcing community but by businesses at large. The main broad criticisms made against the Controller to Processor Model Contract are that it is non-negotiable and its provisions are too onerous on both the customer and the supplier.

Significant drawbacks of the Controller to Processor Model Contract are that its terms:

- Provide that data subjects will be deemed "third party beneficiaries" who will have rights to obtain compensation and enforce specific terms of the model contract. This is something that is not appealing to customers who are outsourcing large client or customer databases.

- Create cross-indemnification provisions in respect of breaches of the terms. This is something that customers and suppliers may wish to deal with differently in line with their standard indemnity positions.

- Contain restrictions on onward transfers to further sub-data processors. This means that separate Controller to Processor Model Contracts would need to be put in place between the customer and each of the sub-data processors. In complex multi-country, multi-sourcing outsourcing arrangements involving lead suppliers, consortiums, contractors, consultants and other third parties, this could require significant time, effort and costs to be incurred not only during the negotiation phase but throughout the life of the outsourcing on the contract management side.

Some member states have additional registration requirements (that is, in addition to requiring the use of the model contracts) for transfers outside the EEA. As a result, customers and suppliers should seek advice on the local law position in the relevant member state.

In outsourcing transactions in practice, some customers do not automatically seek to use the model contracts to comply with Article 25 of the Directive. If anything, due to the drawbacks outlined above, the common practice for both customers and suppliers is to test and consider the implications of using the model contracts on a transaction-by-transaction basis.

Ad hoc agreements. It is possible to use other contractual clauses (that is, other than the model contracts approved by the Commission) in certain member states for the purposes of complying with Article 25 of the Directive. However, as some of the member states' supervising authorities could require individual approval for such clauses, this option is not widely used for outsourcing purposes across the EU.

In the UK, the ICO has provided guidance stating that data controllers can use their own contracts to plug gaps to achieve adequacy (*Data Protection Guidelines - International transfer of personal information; General advice on how to comply with the 8th data protection principle*). The ICO has explained that the reason they can use their own contracts is that such contracts cannot prevent the UK-based data controller from being held responsible for the acts of the non-UK-based data processor, and data subjects would still be able to enforce their rights against the UK-based data controller. The ICO could still also enforce against the UK data controller.

The ICO's guidance requires such contracts to be comprehensive to ensure adequacy exists, including meeting the security requirements of Article 17 of the Directive. In outsourcing guidance to small and medium business, the ICO has said that in such cases it is likely that there will be adequate protection for the transferring data (*Data Protection Good Practice Note Outsourcing - a guide for small and medium sized businesses*). This is because the use of "appropriate security measures, the selection of a reputable organisation and restrictions on use help ensure an appropriate level of protection for personal data. However, you need to be sure that the contract with the other organisation and its terms are enforceable in that country".

Binding corporate rules (BCRs)

The Article 29 Working Party (an advisory group made up of representatives from each of the EU data protection authorities) considers that

BCRs are an appropriate way for multinational companies and other such groups to ensure adequate protection for personal data transfers to countries outside the EEA. In other words, BCRs facilitate compliance under Article 25 of the Directive.

In summary, BCRs are a type of privacy policy that:

- Apply across companies in the same group.
- Are internally binding within the group and externally binding in terms of the data subjects.
- Enforceable against those companies in relation to the processing and exporting of personal data.

BCRs offer large multinationals with complex corporate structures a means of complying with Article 25 of the Directive by using a combination of binding and enforceable group privacy policies, codes of conduct and audit procedures. BCRs are seen as the best long term solution for group companies for personal data transfers within the same corporate group (as opposed to putting in place layers of model contracts between their numerous legal entities).

In practice, BCRs are the much talked about but little used option of ensuring adequacy. They have certain drawbacks including:

- They are complex.
- There is confusion over what exactly needs to be put in place.
- They involve lengthy implementation timeframes (and associated costs).
- Until recently, each member state would have to approve the relevant proposed BCR (*see box, Binding corporate rules: recent developments*).

As a result, so far, no multinationals have obtained approval for a set of BCRs that apply across the member states of the EU. Indeed, there have been very few outsourcing arrangements put in place that have used BCRs as a mechanism for ensuring compliant personal data transfers outside the EEA for the purposes of Article 25 of the Directive.

Guidance and procedures issued by the Article 29 Working Party in the "BCR toolkit" issued in the middle of 2008 finally seem to be making BCRs a more user-friendly and realistic option for small and large companies (*WP 153, WP 154 and WP 155; adopted by the Article 29 Working Party on 24 June 2008*).

Despite this development, BCRs are unlikely to be used extensively in the outsourcing field. This is because BCRs apply intra-group, but most outsourcings consist of data transfers to third party suppliers outside the group. As a result, model contracts or other relevant adequacy option(s) still need to be put in place between customers and suppliers (with BCRs only playing a role where the supplier then goes on to use some of its group members as its sub-data processors).

Safe Harbor

If a supplier to an EU organisation in an outsourcing transaction is based in the US, then the "Safe Harbor" scheme may be an option that can be used to legitimise the transfer out of the EEA. The Safe Harbor scheme has been in place since 1 November 2000 and, in addition to the adequacy findings in respect of particular countries under Article 25(6) of the Directive (*see above, Adequacy*), the Commission has deemed that the Safe Harbor scheme meets the required level of adequacy.

Safe Harbor is a voluntary scheme containing data protection principles similar to those under the Directive. The scheme is operated by the US Department of Commerce with whom organisations can voluntarily register if they adhere to the principles.

Unfortunately, the scheme does not cover all companies: telecommunication companies and financial institutions are not covered. Another drawback is that not all suppliers in the US have registered with the scheme, and as a result, it may not be an option in every outsourcing transaction.

Derogations

Certain derogations from the data transfer requirements of Article 25 of the Directive regarding personal data to countries with-

BINDING CORPORATE RULES: RECENT DEVELOPMENTS

Single binding corporate rule document

The Article 29 Working Party has amended its existing frequently asked questions' guidance on binding corporate rules (BCRs) (*WP 155 (Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules), adopted 24 June 2008*). The new version encourages (that is, it does not require) companies to collate all of their BCR material in a single document: "…it is strongly recommended that multinational groups using BCRs have a single set of global policies or rules in place to protect all the personal data that they process. Having a single set of rules will create a simpler and more effective system which will be easier for staff to implement and for data subjects to understand".

In January 2009, the Article 29 Working Party released an amended version of WP155, which specified what terminology applicant companies can use when creating their BCRs, the purpose being to avoid any misinterpretation of BCRs across member states and to ensure they remain consistent with the Directive.

Mutual recognition

One of the biggest drawbacks with BCRs is that they have to be approved by each member state in which the group is located. However, in June 2008, the Article 29 Working Party managed to put a co-operation procedure in place. Data protection authorities in nine member states (that is, France, Germany, Ireland, Italy, Latvia, Luxembourg, The Netherlands, Spain and the UK) have agreed to mutually recognise BCRs approved by one of the other nine data protection authorities (one of which will take the lead in approving the initial application) without any further amendment. The Article 29 Working Party is hoping to convince more member states to join this framework during the early part of 2009.

SECURITY: RECENT REGULATORY INITIATIVES

Breach notification

Breach notification is one of the privacy "hot topics" in many EU member states at the moment. EC regulators continue to debate the introduction of an EU-wide requirement to notify regulators of a data security breach, the related notification triggers and thresholds and the steps that will be taken depending on the seriousness of the breach notified. At the same time, specific EU member states have begun reviewing whether they will put their own breach notification measures in place. At the time of writing, the topic is a controversial one, as delegations and lobbyists campaign for further changes to the proposed breach notification proposals.

The likely overall impact on outsourcing transactions following the introduction of breach notifications laws is that:

- Customers will require suppliers to immediately report any actual or suspected data breaches.
- More detailed provisions will need to be incorporated into outsourcing contracts to cover the breach notification assistance activities that suppliers will need to carry out along with any related risk and liability provisions.

ePrivacy Directive

In September 2008, the European Parliament gave "first-reading" approval to a report amending the ePrivacy Directive (2002/58/EC). The draft will need further approval from the Council, which comprises the EU telecommunications ministers. The expectation is that the Council will seek a more lenient regime than currently recommended in the report. It is expected that the ePrivacy Directive is likely to be approved in early 2009.

The stricter provisions approved in the report by the European Parliament:

- Expand the scope of the ePrivacy Directive to expressly cover not only telecommunications providers and internet service providers, but also "private networks" such as corporate networks, universities, hotels and so on.
- Include detailed additional obligations, which are imposed on all providers with respect to security standards, including access controls, a security policy and incident response plan.
- Mean that any security breach leading to "accidental or unlawful destruction, loss, alteration in, authorised disclosure of or access to personal data" would need to be notified to the national regulators. The regulators would decide if notification to individuals is required depending on the seriousness of the breach.

  (Note that in the final months of 2008, there were further proposals about whether the trigger for the notification should only apply if "an imminent and direct danger" is present. In early January 2009, the European Data Protection Supervisor (EDPS) published his second Opinion on the ePrivacy Directive. The EDPS' position is that notifications should be triggered based on whether a breach is "reasonably likely to harm" affected individuals, with "harm" being emphasised as a sufficiently wide concept. Therefore, it is a case of "watch this space" as EU regulators continue to debate this issue.)
- State that annual reports should include all security breaches.

At an EU member state level, other breach notification initiatives include:

- **UK.** In March 2008, the UK Information Commissioner's Office (ICO) published guidance on the reporting of data security breaches (Notification of Data Security Breaches to the Information Commissioner's Office). It provides guidance on when the ICO expects to be notified of a breach of data security and the information that should be provided to the ICO, along with the steps that should be taken on receipt of such notification.
- **Germany.** The German government has recently adopted a draft law amending the German Federal Data Protection Act (*Bundesdatenschutzgesetz*) (BDSG). Once approved by the Parliament, the amendments should enter into effect on 1 July 2009.

  Some of these amendments relate to the introduction of US-style breach notification requirements where there is a data loss relating to sensitive data, criminal records, bank account or credit card data, or personal data subject to legal privilege (for example, data held by lawyers, doctors or journalists). Notification will only be required in cases where the data loss is likely to lead to "serious impediments for the privacy and other individual interests". The legislative commentary states that when assessing whether there are "serious impediments", the types of data, as well as the possible results of the breach, such as damages or identity theft, must be taken into account.

  Both the data protection authorities, as well as all individuals concerned, must be notified "immediately" (as soon as reasonably possible) after containment and as soon as such notification no longer impedes law enforcement. The notice to the authorities should also include an assessment of the measures taken by the organisation to mitigate damages. Interestingly, public authorities are exempt from breach notification.
- **Ireland.** The Minister for Justice, Equality and Law Reform has set up a reform group that will discuss the introduction of mandatory breach notification in Ireland. The reform group, which began its work towards the end of 2008, will examine whether the introduction of mandatory data breach notification is necessary, as well as any related penalties.

out adequate protections are allowed unless otherwise stated by member states (*Article 26(1), Directive*). The derogations are:

- The data subject has given his consent to the transfer.
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party.
- The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.
- The transfer is necessary to protect the vital interests of the data subject.
- The transfer is made from a register which, according to laws or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law "for consultation" are fulfilled in the particular case.

These derogations represent a different approach to the other adequacy options whose roles are to ensure adequacy is or will be in place before the data transfer occurs.

In the UK, the ICO has provided guidance:

- Implying that the derogations should only be relied on as a last resort.
- Specifically stating that in instances where adequacy is not in place, then the interpretation of the derogations should be narrowly construed.

The guidance also reminds data controllers that they still need to comply with the other data protection principles, in particular the security requirements (*sections 4.1.2 and 4.1.3 of the ICO's guidance note entitled Data Protection Act 1998 - The Eighth Data Protection Principle and international data transfers*).

Similar to the self-assessment option (*see above, Adequacy*), it is rare for a customer to proceed with an outsourcing arrangement on the basis of one of the derogations. Use of the derogations would not be seen as a practical long-term strategy for multinational companies outsourcing from many locations across the EU.

FUTURE DEVELOPMENTS

As the trend towards cross-border outsourcing continues to rise (in particular, BPOs, which tend to involve more personal data than traditional ITOs) and more countries around the world put their own legislation in place to protect and control the cross-border flows of personal data, customers and suppliers will need to be more vigilant to ensure that they comply with both:

- EC privacy regulatory requirements.
- All the relevant local law privacy measures that may need to be put in place depending on the countries involved.

Gone are the days when all that was required was for lawyers (often without the customer or supplier present) to negotiate the basic data protection clauses to be incorporated in an outsourcing contract. Gone too are the days when the customer relied on generic contract clauses requiring the supplier to "comply with all applicable local laws". From a privacy perspective, such local laws need to be clearly identified in the outsourcing contract, with a clear understanding of what the supplier is required to do on a country-by-country basis.

Current good practice dictates that an entirely separate privacy work stream be put in place for the negotiation phase of an outsourcing transaction. This involves lawyers, risk managers, security experts and privacy officers of both organisations. In recent times, this has often required the final output from the work stream to be signed-off by management at the highest levels of both organisations.

The dedicated work stream should:

- Negotiate the standard privacy clauses for the outsourcing contract.
- Ensure that the necessary and relevant security policies and standards and related obligations and responsibilities are incorporated into the outsourcing contract and fully understood by the supplier.
- Ensure that these related obligations and responsibilities are included within the pricing in the outsourcing financial model.

The work stream should also focus on building assurance mechanisms into the outsourcing contract that apply for the duration of the contractual term.

Breach notification looms heavily on the EU horizon in 2009 (*see box, Security: recent regulatory initiatives*), and future work streams will need to get to grips with building in new risk or liability contract provisions for data loss or damage breaches and assurance mechanisms. Such mechanisms could include, for example, requiring the supplier to have incident response plans in place and requiring mandatory attendance by the customer or supplier at monthly data protection forums to review data breaches during the contract term. These should be as transparent as possible and give the customer confidence that the personal data transferred is being processed securely and in accordance with the relevant legislative framework(s).

CONTRIBUTOR DETAILS

Anthony Nagle
Morrison & Foerster
T +44 20 7920 4029
F +44 20 7496 8529
E *anagle@mofo.com*
W *www.mofo.com*

SEAMLESS SOLUTIONS. TIMELESS TEAM VALUES.

We are Morrison & Foerster – a global law firm with world-class credentials in all aspects of Sourcing across all industry sectors.

The diversified talents of our 60 top-tier lawyers operating on three continents, allows us to integrate seamlessly commercial, regulatory, technical and economic issues into one comprehensive sourcing solution.

Perhaps our most impressive quality is our team approach. Clients value our collaborative style and inclusive perspective no matter how complex the issue or far-reaching the project. As an integral member of your team, we are uniquely prepared to deliver outstanding results with maximum efficiency.

From legal advice and project management to deep expertise in financial services, HR, data privacy/security, tax and other relevant disciplines, our outsourcing resources go beyond the expected.

MORRISON | FOERSTER