

commerce&technology

In this issue

- **International transfers of data – where are we now?**
- **E-Marketing – good practice**
- **RFID technology – looking ahead**
- **.EU – time is running out**

promoting enterprise

February 2006

International transfers of data – where are we now?

International travel has never been cheaper, the world smaller or global communications quicker, yet transferring personal data out of the European Economic Area (EEA), particularly to the US, is still problematic for those businesses that operate internationally.

Following recent developments in data protection law specifically in the field of cross border data flows, we look at where we are and whether transferring data outside the EEA has become easier?

The problem

Essentially, information about people (personal data) cannot be transferred to a country outside the EEA unless that country ensures an adequate level of protection for the individuals concerned.

“Compliance with EU data protection laws can be achieved in a number of ways. The key is selecting the most appropriate solution for a particular organisation.”

Presently, according to the EU Commission, the US does not offer “an adequate level of protection”. This causes a major headache for US businesses that have a footprint in the UK and EU. US businesses that have UK subsidiaries, branches, agencies, distributors and those US companies that sell

directly to customers in the UK and EU (for example, via the Internet) are all affected by this restriction.

It means that, for example, a UK subsidiary cannot transfer to its US parent customer data or HR data such as performance and health records, contact details and salary and bonus levels.

The solution

The prohibition on transfer of personal data outside the EEA is not absolute. We describe below the principle options that are available to US businesses where they want to transfer personal data from the EU to the US.

Model contracts

The EU Commission has the power to authorise certain standard contractual clauses pursuant to which personal data can be transferred outside the EEA. These are commonly referred to as model contracts. In 2001, the Commission authorised a model contract for use by data exporters but this was criticised for being cumbersome and impractical. Following consultation and lobbying by the International Chamber of Commerce (ICC) and other the business groups, the Commission and the UK Information Commissioner recently approved a new model contract.

The new ICC model contract does not supersede the 2001 contract. Both sets of contracts can be used depending on which is more suitable. Given that the ICC model contract has been negotiated by business groups, it is designed to be more business friendly. So what are the key differences?

Under the 2001 model contract the data exporter and importer were jointly and severally liable for each others actions. This meant that if an individual suffered loss as a result of the data importer's actions the individual could pursue either the data importer or exporter for compensation. Not surprisingly, this proved unpopular with businesses particularly where the exporter and importer were not associated.

Joint and several liability has been replaced by a concept of "due diligence by the data exporter". Due diligence by the data exporter means that it has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under the contract. Unless the data exporter fails to use reasonable efforts, it would not be liable for the actions of the data importer.

The ICC model contract also alters the position on third party beneficiary rights for individuals. Under the 2001 model contract, individuals could sue under the contract either the data importer or the data exporter. Under the new regime, the individual cannot sue a data importer unless the data exporter has failed to take action.

In comparing the two model contracts, the ICC contract is more likely to appeal to data exporters and data importers who are acting at arm's length. Unconnected parties are unlikely to want to be liable for the other party's actions. On the other hand, this may not be so much of a concern where the exporting occurs intra-group and the UK subsidiary may not want to conduct the due diligence on its US parent that is required by the ICC contract. In any event, consideration should always be given as to which model contract is the most appropriate for the particular circumstances.

Binding corporate rules

The EU introduced the possibility for companies within large multinational groups to implement their own worldwide internal data protection compliance and enforcement regime known as Binding Corporate Rules (BCR).

The underlying idea is that a group develops its own rules, policies and procedures for ensuring data protection compliance. These rules are then submitted for approval to the data protection authority of the EU country in which the ultimate parent or operational headquarters of the group is based and that authority then obtains consent to the scheme from all the other EU data protection authorities.

The BCRs scheme is a relatively recent development and is still in its infancy. In 2005, the Commission approved an updated model checklist which describes the required contents of an application to a data protection authority for approval of BCRs.

The BCRs regime is likely to be suitable for the truly multinational group with companies in a number of EEA countries and around the world. It is unlikely to be suitable for one off or infrequent transfers between a small group or unconnected parties.

In December 2005, General Electric was the first corporation to be authorised by the UK Information Commissioner to transfer employees' information outside the EEA using binding corporate rules. General Electric is now able to share personal information such as employee data within the multinational.

"The BCRs regime is likely to be suitable for the truly multinational group with companies in a number of EEA countries and around the world."

Safe Harbor

The Safe Harbor regime was designed – by the US Department of Commerce in consultation with the European Commission - specifically for US companies who have a presence in the EU as a means of complying with EU data protection laws. Initially, the take up of Safe Harbor proved slow but, five years on, Safe Harbor is becoming increasingly popular. Over 800 US companies have signed up to Safe Harbor.

The decision by US organisations to enter the Safe Harbor is entirely voluntary. In order to benefit from Safe Harbor, a corporation must:

- Unambiguously and publicly disclose its commitment to comply with the seven Safe Harbor principles. This needs to be done annually as part of a self certification process.
- Subject itself to the authority of the Federal Trade Commission (FTC) or in the case of US airlines or transportation entities, the US Department of Transportation.

The seven Safe Harbor principles are based on the principles and fundamental rights contained in the EU Data Protection Directive. For example, individuals should be told how data about them is collected and used and should have access to this data. Policies and procedures need to be developed to comply with these principles.

In general, enforcement of the Safe Harbor will take place in the US in accordance with US law and will be carried out primarily by the private sector. Private sector self regulation is backed up as needed by government enforcement. The lack of a proactive enforcement approach from the FTC and other similar governmental bodies has led to concerns which have been voiced by the EU Commission that the Safe Harbor regime is not being enforced adequately. In general, there is a concern that personal data is not being safeguarded as was intended when the regime was set up.

Safe Harbor has become a realistic method for compliance with EU data protection laws. However, given the lingering doubts about the adequacy of Safe Harbor in protecting the data of EU citizens it is possible that we could see some changes in the future.

Consent

Transfers outside the EU of personal data can be made with the individual's consent. Such consent to be valid must be freely given, specific and informed. This may be a solution for the transfer of (for example) customer data but is problematic in the case of HR data even if the employees consent. The UK data protection regulator has expressed doubt as to whether consent given by an employee can ever be "freely given" given the unequal relationship between employee and employer.

Consent is unlikely to be valid if the individual has no real choice but to give his consent or where the individual has no real understanding of what he is agreeing to. The reasons for the transfer, the countries involved should be specified and any potential risks involved in the transfer should be brought to the individual's attention.

Which solution?

Compliance with EU data protection laws can be achieved in a number of ways so as to permit US organisations to transfer data from the EU and UK. The key is selecting the most appropriate solution for a particular organisation.

E-Marketing – good practice

Following the UK Information Commissioner's recently published guidance on electronic marketing, we take a quick look at what is involved.

Data Protection Act

The first thing to think about is the Data Protection Act (DPA). This says that using someone's details for marketing is unlawful unless it is carried out "fairly and lawfully".

To comply with the DPA, consumers must be told how information about them may be used and have consented to that use. This consent may be implied by an opt-out approach (the user must request not to be included on a list, for example by de-selecting a checkbox).

E-Commerce Regulations

If an email/SMS is unsolicited, then it must be clearly and unambiguously identifiable as unsolicited. For example, in relation to SMS, the first few characters of the SMS must be used to say that it is an unsolicited text for marketing.

Privacy and Electronic Communications Regulations

These Regulations create a more onerous requirement

than under the DPA. The opt-out approach cannot be used. Instead, there is a 'soft opt-in' requirement. Consumers must specifically agree to receive email/SMS, for example by selecting a checkbox. An exception is where there is an "existing commercial relationship".

Existing Commercial Relationship

You can send an unsolicited email/SMS:

- if the sender obtained the contact details in the course of the sale or negotiations for the sale of a product or service;
- the sender is marketing its own similar products and services;
- the addressee is always able to opt out of future marketing free of charge.

This exemption is not always straightforward to apply.

Good practice points

- Go for permission-based marketing as much as possible.
- Provide a privacy policy when you collect details.
- Do not have consent boxes pre-ticked.
- Provide a simple and quick method for customers to opt out at no cost, other than that of sending the message.

RFID technology – looking ahead

During 2005, the somewhat oddly named but influential “Article 29” EU Data Protection Working Party began a public consultation on data protection issues relating to RFID technology. The Working Party recognised the benefits of RFID technology. In particular, it can help businesses manage their inventory, streamline the supply chain, engage in more targeted marketing and enhance consumers’ shopping experience. However, the Working Party also highlighted the privacy concerns that come with the widespread deployment of RFID technology.

The Working Party warned that the RFID technology may surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores), monitor consumer behaviour in stores, or read the details of clothes and accessories worn. All represent a potential invasion of the privacy of an individual. The developments in technology and reductions in costs which are fuelling global implementation of RFID can only exacerbate the potential problem.

The results of the consultation were inconclusive. Opinion is divided between the need for additional legislation specifically covering RFID technology and the belief that existing data protection legislation adequately covers RFID technology. Looking ahead, we expect more discussion on this issue, further comment from the Working Party and, possibly, proposals for specific regulation.

.EU – time is running out

Time is running out for trade mark holders that wish to beat the rush and obtain a .EU top level domain name. To qualify for a domain name during the first sunrise period (which runs to 7 February 2006), applicants must hold a registered trade mark identical to the domain name being applied for. During the second sunrise period, which runs from 7 February 2006 to 7 April 2006, the eligibility criteria are relaxed to include (for example) company names and trade names identical to the domain name being applied for. Documentary evidence will be required (such as a certified copy of the trade mark certificate).

Once the sunrise period finishes on 7 April 2006, anyone can apply for a .EU domain.

Technology group contact details

Nigel Miller

Tel: +44 (0)20 7614 2504
nmiller@foxwilliams.com

Paul Osborne

Tel: +44 (0)20 7614 2503
plosborne@foxwilliams.com

Mark Tasker

Tel: +44 (0)20 7614 2568
mtasker@foxwilliams.com

Gavin Foggo

Tel: +44 (0)20 7614 2543
gfoggo@foxwilliams.com

Kolvin Stone

Tel: +44 (0)20 7614 2596
kstone@foxwilliams.com

Steve Barnett

Tel: +44 (0)20 7614 2626
sbarnett@foxwilliams.com

This briefing paper is for general information and is not a substitute for legal advice.

Fox Williams
Ten Dominion Street
London
EC2M 2EE

Tel: + 44 (0)20 7628 2000
Fax: + 44 (0)20 7628 2100

www.foxwilliams.com