
Managing Compliance in the Global Space – Transborder Data Flow

by Katherine Sainty, Partner and Andrew Ailwood, Law Graduate

Modern business is increasingly borderless. The communications revolution and the reduction in international trade barriers has allowed business to globalise and for regions to specialise. The call centre answers the phone in India, the product is designed in Europe, made in China and it is all managed from the US. But these business units must share their information; information about employees, customers and suppliers. Transborder data flow is the transfer of data containing personal or sensitive information from an entity in one country to an entity in another jurisdiction and is an area of increasing regulation around the world. Strict European regulation is driving change and setting the international standard for personal privacy protection.

1. What are the transborder restrictions on data flows?

Data protection or protection of personally identifiable information about an individual became a key legal issue once the EU sought to ensure its member states regulated data use and privacy. This is the derivation of Australian laws in the area.

1.1 EU Initiatives

The EU Data Protection Directive¹ (95/46/EC) (the **EU Directive**) was passed in 1995 and sets standards for processing personal data and the transfer of such data within the European Union. The directive is designed to enable the free movement of data while protecting the privacy of European Union citizens and applies to any organisation that processes personal data within the European Union, including both public and private sectors (except law enforcement) and foreign entities. The Directive's standards cover the collection, storage, use and disclosure of personal data, with especially stringent rules for the processing of sensitive data, for example information on health. The Directive's primary purpose was to implement the right of privacy under the European Convention for the Protection of Human Rights and Fundamental Freedoms and to ensure equivalent levels of protection in EU member states for the purpose of facilitating an integrated economy through free movement of information.

Article 25 of the EU Directive requires EU member states to only allow transfer of personal data to third countries which have an **adequate** level of protection for data. That adequacy will be determined with reference to the nature of the data, the purpose and duration of the proposed processing operation, the country of origin, the destination country and the rule of

¹ EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such data (95/46/EC)

law, professional rules and security measures in force in the third country. Article 25 (4) and (6) gives the European Commission (the executive arm of the EU) the power to determine whether a third country provides an inadequate or adequate level of protection.

Article 26 derogates from Article 25 by allowing transfers to third countries with inadequate levels of protection where the transfer takes place on condition that:

- (a) the data subject consents to the transfer;
- (b) the transfer is necessary for performance of a contract with the data subject;
- (c) the transfer is necessary for performance of a contract for the data subject's benefit;
- (d) the transfer is necessary or legally required on important public interest grounds or in exercise or defence of legal claims;
- (e) the transfer is necessary to protect the vital interests of the data subject; or
- (f) the transfer is made from a register which by law is intended to provide information to the public.

The member state's privacy authority (usually an executive government authority) may authorise transfers which do not comply with the above definition of adequacy, but which the authority's opinion have adequate safeguards with respect to the protection of privacy. This discretion on the part of the member state privacy authority is particularly aimed at allowing transfers made under the control of appropriate contractual clauses². The Commission can also approve standard contractual clauses for use when contracting with recipients that ensure adequate levels of protection for information being transferred to a recipient in a third country³.

In January and September 2001, the Working Party issued two decisions outlining issues relevant to consider in formulating standard contractual clauses for the processing of personal data suitable for providing adequate protection for data transferred to non-complying third countries, such as Australia. The decisions provide a benchmark for compliance with the EU Directive⁴.

The EU Directive does not create direct obligations for individuals in the EU, rather it places an obligation on member state to pass implementing legislation at a municipal level. Furthermore, the rights annunciated in the EU Directive are minimum standards. Member states can provide a level of protection which exceeds this minimum in their implementing legislation.

EU member states have all passed their own local legislation implementing the data protection laws. Some countries have exceeded the minimum standards set by the EU and require more stringent privacy protection.

² Article 26(2) of the EU Directive 95/46/EC

³ The model contract clauses can be found at http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm

⁴ All the relevant Working Party material can be found on the EU web page in the section dealing with data protection at: http://europa.eu.int/comm/internal_market/privacy/index_en.htm.

The EU uses two key terms when discussing protection in third countries. Article 25(1) requires that the level of protection in a third state must be **adequate**. Adequacy is primarily determined by decisions of the European Commission through the findings of Working Parties. There is also a concept of **equivalent** protection. Preamble (8) to the EU Directive requires that the level of protection be equivalent, that is, substantially the same. In contrast, the concept of adequacy is more subjective and need not be objectively equal to the standard within the EU.

1.2 An example: UK implementation of the EU Directive

The *Data Protection Act 1998* (UK) is the UK's implementing legislation of the minimum standards required by the EU Directive. Section 1 of the UK Act defines personal data as data relating to a living person which can be used to identify the person from that data or from the data in conjunction with other information in the possession (or likely to be able to be in the possession) of an organisation. Schedule 1 contains the basic privacy principles.

In July 2004, the European Commission called upon the UK Government to justify its approach to data protection laws, on the grounds that they may not properly implement the EU Directive. This followed from the definition 'personal data' given in a recent Court of Appeal case that the personal data must relate directly to the relevant subject rather than matters in which the individual was involved⁵. The EU Directive is intended to apply to both direct and indirect information, but the UK implementing legislation has not reflected this breadth. The EU is expected to place pressure on the UK to amend this definition.

1.3 Trans-border data protection in the New EU

On 1 May 2004, the EU expanded to include 10 new member states. These countries primarily coming from Eastern and Southern Europe, many from former Eastern Bloc countries. These countries were quick to ensure they were seen by the EU to have made attempts to implement the strict EU Directive.

In implementing the trans-border controls, the new member states of Cyprus, the Czech Republic, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia require that the trans-border transfer be submitted to the local regulator (member state privacy authority) for approval, even where a model contract is used. In contrast, Estonia does not require regulator approval. Slovenia and Latvia do not discriminate between EU and non-EU countries. This is a direct contradiction to the intent of the Directive to facilitate intra-EU data flow.

This experience in the new EU states illustrates that even where member states derive their legislation from the same source, namely the EU Directive, there can be real differences in application.

⁵ *Durant v Financial Services Authority* [2003] EWCA Civ 1746

1.4 Australian Transborder Restrictions

The *Privacy Act 1988* (Cth) (the **Privacy Act**) regulates handling of personal information in Australia and originating from Australia.

Under Australian Law, specifically National Privacy Principle (**NPP**) 9, if an organisation's overseas activity is required by the law of a foreign country, then it does not interfere with the privacy of an individual under Australian Law.

An organisation may transfer personal information overseas provided that one of the following conditions is satisfied:

- the organisation reasonably believes a law, binding scheme or contract applies at the destination which effectively delivers privacy standards substantially similar to the NPPs;
- the individual consents to the transfer;
- the transfer is for the benefit of the individual and it is impracticable to obtain consent, but it's likely consent would be given;
- the transfer is required by a contract between the individual and the organisation, or a contract between the organisation and a third party in the interests of the individual; or
- the organisation has taken reasonable steps to ensure the information will not be held, used or disclosed by its recipient inconsistently with the NPPs.

The EU Directive has imposed a minimum standard for data handling practices on its members states. It requires data transferred outside the EU, for instance to Australia, to be handled in a manner deemed to be *equivalent* or to at least be deemed *adequate* by EU standards (through European Commission approved methods).

1.5 The EU view of Australian Transborder Protections

In 2001, the EU Data Protection Working Party expressed its concern about the extent of protection Australian privacy law provides for EU data flowing to Australian private sector companies. In particular, the Working Party was concerned because some small businesses and employers, in relation to certain employee data, are exempt from complying with the personal information handling provisions in the Privacy Act. Thus equivalence with EU standards is not possible.

The Working Party took the view that because of these exemptions it is necessary to assume that all data transfers to Australian businesses from the EU could be regarded as adequate only if appropriate safeguards were introduced to meet its concerns. As such, the Working Party recommended EU citizens exercise extra safeguards, for example contractual clauses, when exporting data to Australia. Alternatively the EU suggested that voluntary codes of conduct or approved privacy codes which addressed the concerns expressed in the Working Party Paper would be effective given that these are enforced either by the Privacy Commissioner herself or by an independent adjudicator.

The Working Party also expressed reservations about Australia's regulation of sensitive information within the Privacy Act and the lack of correction rights which exist for EU

citizens under the Act. Under the Privacy Act, limitations are placed on the collection of sensitive data, but not on the use or disclosure of such data. The EU Working Party was concerned that this provision could not sufficiently protect sensitive personal information.

In addition, section 41(1) of the Privacy Act allows the Privacy Commissioner to investigate an act or practice only if it interferes with the rights of Australian citizens or permanent residents. The Working Party was concerned there was no provision in Australia to ensure EU citizens' privacy rights are also protected by the Commissioner's powers of investigation.

The Federal Attorney-General, issued a media release on 26 March 2001 rejecting the Working Party's findings on the basis that they "display an ignorance about Australia's law and practice". The Attorney-General also argued that the Act is world-leading legislation and that, in many ways, it goes significantly further than the US Safe Harbor Agreement, which the EU judged to be adequate. At this stage there appears to be no proposal for the Working Party to reassess the Australian Privacy Act. Given that the Act is currently under review (as originally foreshadowed when the legislation was passed) it is likely that the Working Party may be invited to reassess the legislation once any amendments are made as a result of that process. Consequently Australian organisations need to look to the recommendations in the Working Party's decisions for practical solutions to these issues in the medium term. Standard contractual clauses approved by the European Commission are one such solution, as are binding corporate rules.

1.6 USA

In contrast to the centrally standardised and monitored EU privacy regime, the United States has adopted a less prescriptive approach to data protection. Following the EU's 1998 implementation of the EU Directive (which prohibited the transfer of personal information out of the EU without adequate privacy protection in the recipient jurisdiction) substantial economic pressure was placed on the US to ensure that multi-nationals could continue to deal with the personal information of EU citizens. In response the US Department of Commerce developed the 'safe harbor' framework which was approved by the EU and came into effect in November 2000.

The Safe Harbor framework provides a regime where individual companies may elect to adhere to seven 'safe harbor principles'. The EU has certified that the seven principles provide adequate protection. This finding of adequacy is binding on all 25 EU member states. The US will have jurisdiction over complaints by EU citizens against US organisations.

US organisations must 'self certify' annually to the US Department of Commerce that they agree to adhere to the safe harbor requirements. The Department then publishes a list of organisations that have self-certified. That list includes Apple Computers, Disney, Eastman Kodak, Ernst and Young, General Motors, Intel, Johnson and Johnson, Monsanto, Proctor and Gamble, Boeing and Pepisco.

By adopting the safe harbor provisions, the US organisation agrees to treat information in accordance with the following seven privacy principles:

- (a) **Notice** – at the time of collection, organisations must indicate:

-
- (i) the purpose for collection and use;
 - (ii) the means by which the individual can contact the organisation;
 - (iii) the types of third parties to which the organisation discloses the information; and
 - (iv) the choices and means the organisation offers for limiting its use and disclosure.
- (b) **Choice** – organisations must give the individual the opportunity to opt out from having their information disclosed to a third party or used for incompatible secondary purposes. For sensitive information, this choice to disclose or use for secondary purposes must be explicit and affirmative (ie an opt-in).
- (c) **Onward Transfer** – before disclosing to a third party, organisations must apply the notice and choice principles. If the organisation is acting as an agent, it may transfer the information if the third party recipient also subscribes to the safe harbor principles or is bound by the Directive or another finding of adequacy. Alternatively, contractual obligations to provide equivalent protection may be sought from the third party recipient.
- (d) **Access** – organisations must provide individuals with access to their information. They must also provide the ability to correct, amend or delete information that is inaccurate.
- (e) **Security** – organisations must take reasonable precautions to protect personal information from loss, misuse and unauthorised access, disclosure, alteration or destruction.
- (f) **Data Integrity** – personal information must be relevant to the purposes for which it is used and an organisation should ensure it is reliable.
- (g) **Enforcement** – the organisation must have:
- (i) recourse mechanisms in place to handle complaints and disputes;
 - (ii) procedures for verifying implementation of the principles;
 - (iii) obligations to remedy problems arising out of failure to comply with the principles.

The safe harbor principles are enforced indirectly, via a self regulatory approach. The US policy is to encourage private sector enforcement of the principles, primarily through internal dispute resolution systems in adopting organisations. The US does not have a government authority specifically empowered to deal with privacy complaints, such as in EU countries or Australia. Instead, Federal and state laws concerning unfair and deceptive acts will apply where an organisation has purported to adhere to the safe harbor principles but has failed to in implementation⁶. The Federal Trade Commission (*FTC*) is empowered to enforce the *False Statements Act* (18 U.S.C. §1001) which would apply where a company has falsely stated that it adheres to the principles. The *FTC*'s can also ensure

⁶ www.export.gov/safeharbor/sh_overview.html

companies adhere to their stated privacy policies as a promise under section 5 of the *Federal Trade Commission Act*. The FTC has issued penalties of up to US\$100,000 and its investigations have led to Amazon.com settling a class action for US\$1.9million⁷. Even an FTC investigation that does not find an organisation in breach can be costly in terms of management time, legal expenses and negative publicity.

Apart from the Safe Harbor principles and their indirect enforcement, data protection at a Federal level is fragmented and focuses on areas such as spam, children's information, health information and financial information. For example, the FTC administers the *Gramm-Leach Bliley Financial Modernization Act of 1999* which concerns privacy obligations of financial institutions to their customers.

The US also has the *Children's Online Privacy Protection Act Rule* which is enforced by the FTC and applies to the collection of personal information from children under 13 over the internet. Primarily it ensures consent to use and disclosure and general control of information is in the hands of parents and guardians.

1.7 India

Given the importance of out sourcing to the Indian economy, data protection has become a hot political issue. While the lack of data protection laws does not generally affect India's ability to handle personal information from the United States, the growing market of out sourcing from EU countries is placing greater pressure for India to comply.

Naturally, the EU standard contractual clauses can be used to bind an Indian outsourcing provider, but a local regime deemed to be 'adequate' will increase India's ability to compete with emerging out sourcing economies such as new EU member states in Eastern Europe.

The existing Indian privacy law focuses on an implicit right of privacy in the Indian Constitution, but the *Information Technology Act 2000* (India) skirts around this issue.

There has been much discussion of resolving the issue in India. It was initially proposed that legislation modelled on the EU Directive would be implemented. However, the Indian Government's position was revised so as to favour a model more like the US Safe Harbor Agreement that would give Indian organisations flexibility and an appearance of regulatory simplicity⁸.

This issue will continue to be topical as in early November 2004, the Indian Government announced that data protection measures would be on the agenda for 2005⁹.

1.8 China

China does not have wide ranging data protection laws. The planned economy was generally inconsistent with broad privacy rights. As China moves to a more capitalist economic model, its citizens have a greater interest in privacy rights. That said, as yet

⁷ Bender, D and Raskopf, R, 'Cross Border Data' *The New York Law Journal* (29 July 2003)

⁸ Bender, D 'Data Protection Law in India: A Change In Direction' *Privacy and Security Law Report* (12 January 2004)

⁹ Govt to introduce data protection laws, *Business Standard*, India 3 November 2004

there are no specific privacy laws applicable to data protection in the People's Republic of China as a whole.

Hong Kong, however, does have the *Personal Data (Privacy) Ordinance* (Cap. 486) which came into force on 20 December 1996, but is only binding in the Special Administrative Region of Hong Kong. The Ordinance broadly provides rights for informed consent at the time of collection, an obligation of accuracy, openness and security, limitations on the purpose of use and a right of access and correction. The Ordinance also has an employee record exemption.

1.9 Spam

Australian companies must be aware that in a borderless world electronic communications expose companies to significant legal risk. The regulation of spam or junk electronic communications has become a major initiative internationally in the last two years. The Australian legislation is similar to that in the UK and some US states. A multinational that sends emails on behalf of its Australian subsidiary will fall within the ambit of the legislation, as will a foreign company that emails an account accessed by a person present in Australia.

The Australian initiative, the *Spam Act 2003* regulates spam by prohibiting all commercial electronic messages (**CEMs**) with an Australian link (a sender or recipient in Australia will be sufficient). These are messages sent via any media (SMS, MMS, email etc) that offer or advertise a product or assist to defraud. Thus the spam legislation has theoretical transborder restrictions, although the enforcement of these will depend in practice on cooperation between the various jurisdictions with similar legislation. The intention is to have intersecting legislation world wide, with international cooperation in enforcement. These legislative measures are in addition to technological reforms being driven by large internet players such as Amazon.com, eBay, Cisco Systems and Microsoft¹⁰.

However, Designated Commercial Electronic Messages (**DCEMs**), which are messages which are purely factual (with no direct or indirect marketing function) or which come from approved non-commercial entities, are not prohibited.

CEMs can only be sent with express 'opt-in' consent from the recipient. The legislation requires that all CEMs contain information indicating the message sender and containing a functional unsubscribe facility. Liability is accumulated on a per-day-of-contravention basis and can amount to millions of dollars per day.

2. Avoiding Your Data Protection Obligations – Data Havens

2.1 Data Havens – what are they?

In the data protection context, a data haven is a similar concept to a tax haven. Data havens are countries that offer the "freedom" to store and move data without answering to anybody, including regulators, competitors and the individuals who's data it is. Data haven

¹⁰ 'Can the Spam' *The Sydney Morning Herald*, 19 November 2004

services are readily available on the internet. One such example is run by HavenCo Ltd¹¹ from self-declared principality on a former World War II anti-military fortress in the North Sea which has not enacted any data protection laws (the Principality of Sealand claims independence from the UK based on its position in international waters off Essex, UK in the North Sea).

2.2 Data Havens – how might they work?

Data havens offer the opportunity for organisations to transfer information out of a country with adequate protection (a **protected country**) and then process and use the information unscrupulously while in the data haven. For example, analyse the data to identify individuals based on their sensitive information that have a certain health problem and then use that information to direct market a treatment for that problem to the consumer. As an example, countries that have been allegedly facilitating data havens include Anguilla and Bermuda.

This is readily believable, given the volume of spam and computer viruses initiated in unregulated jurisdictions.

Transborder data flow restrictions are in place to counter this territoriality problem. Such restrictions are drafted so as to prohibit the **sending** of the information out of the protected country, not as a prohibition on the receipt of the information in the data haven. Such sending is clearly within the territorial powers to regulate of the protected country.

However, the obligation on an organisation in the protected country does not necessarily control that information once it has left the protected country if sent on the basis of consent of the individuals concerned. The recipient in the third country or data haven may transfer the data to an unscrupulous operator and the original sending organisation may have no actual knowledge of that transfer. However without the exceptions such as consent or necessity of transfer, under NPP 9 (as under the EU provisions) transfer out of Australia is only allowed where protection similar to the NPPs is afforded in the recipient country.

Measures such as standard contractual clauses are designed to ensure that the data exporter remains liable for the recipients behaviour as a means to counter this lack of territorial control.

¹¹ www.havenco.com, www.sealandgov.org

3. Compliance

3.1 Obligations on Australian Companies

Essentially, with respect to international data transfer, Australian entities must:

- seek consent from the individual concerned; OR
- ensure the receiving entity is subject to a law, binding scheme or contract which requires information to be held to a standard that is substantially similar to that in Australia; OR
- show that the transfer is necessary for a performance of a contract with the individual concerned, or for performance of a contract for the benefit of the individual; OR
- show that consent is impractical, that if practical such consent would be likely and that the transfer is for the benefit of the individual; OR
- take reasonable steps to ensure that the information will not be treated inconsistently with the Australian National Privacy Principles.

Additionally, when receiving information, Australian entities must:

- comply with any restrictions on the foreign entity sending the information, particularly if that entity is from the EU and is subject to more stringent protection; AND
- only use the personal information in ways to which the individual consented when it was collected; AND
- ensure consent was given to the transfer, and if not, take steps to ensure that the individual is made aware of:
 - the recipient entity's identity;
 - the recipient entity's contact details;
 - the individual's access right;
 - the purpose of collection;
 - the organisations to which the recipient entity would disclose such information;
 - any legal requirement to collect the information; and
 - the main consequences for the individual if the information is not collected.

3.2 Consent at the Time of Collection

The simplest and most prudent measure that a multinational can take is to ensure that when information is collected that the individual is made aware and agrees to any contemplated transfer to related international entities or to any other foreign entities to

which the collecting entity reasonably foresees that it may want to share the information. However, seeking such consent may not always be practical.

3.3 Standard Contractual Clauses

Another option for an Australian organisation is to use an agreement which contains standard contractual clauses that meet the EU requirements.

The Commission of the European Union made a decision on 27 December 2001 to suggest standard clauses which provide an adequate level of protection when transferring that data to an entity outside the EU¹².

The standard clauses obligate the data exporter to:

- (a) warrant the data being transferred was treated in compliance with the member states' laws;
- (b) notify the affected individual of the export of sensitive data to a country not providing adequate protection;
- (c) make a copy of the standard contractual clauses available upon request to the data subject;
- (d) respond to inquiries from the data subject and privacy authority about processing by recipient; and
- (e) deposit a copy of the standard clauses with the privacy authority on request.

The importer or recipient is, in summary, obligated to abide by the nine standard privacy principles and the decisions of the European Commissions concerning the standard of protection in the relevant third party country. The privacy principles form part of the terms.

Both parties are also obliged to complete an appendix to the standard clauses that sets out the uses, purpose and nature of the information being transferred, as well as how long it will be stored.

The main effect of the standard clauses is to ensure compliance by the recipient with the standard privacy principles. However, the ancillary obligations to deal with inquiries and to make notifications may create unnecessary obligations on the parties concerned.

3.4 Binding Corporate Rules

The EU has recognised the problems that transborder obligations pose to multi-national organisations and has suggested the integration of data protection principles into the corporate governance structure of international groups.

The EU Data Protection Working Party ("Working Party") is the independent European Union Advisory Body on Data Protection and Privacy. In 2003, the Working Party released a Working Document addressing international data transfers - the *Working Document on Binding Corporate Rules for International Data Transfers*. This document suggests that procedures could be simplified to enable more efficient international data transfers within

¹² Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (2002/16/EC)

multinational corporate groups. The paper proposes that in addition to the ability to transfer personal data internationally from an EU member state because of:

- (a) a Safe Harbor agreement with the recipient country;
- (b) an exception, such as consent of the individual about whom the transfer is being made; or
- (c) an alternate safeguard, such as a binding contract with the recipient,

it would be beneficial to allow the data transfers to take place between separate parts of a corporate group where certain binding and enforceable corporate rules are in place. These corporate rules (or codes of conduct) would include general data protection principles as well as procedures for audits and complaints, and would generally allow more flexibility than contractual clauses alone. The Working Party recommended that the use of standard contractual clauses would remain vital to ensuring the effectiveness of a corporate rules requirement for international data transfers. The contractual clauses referred to are from the 2001 Commission Decision discussed above in section 3.3.

The EU has received contributions from a number of organisations which have indicated that it will be necessary to clarify and resolve some issues before binding corporate rules can be effectively used. While discussions were planned for January 2004, they have been postponed in order to gather additional information.

3.5 Highest Minimum Standard

In general, multinational organisations should attempt to adopt privacy policies, procedures and guidelines that satisfy a 'minimum highest standard' approach. This involves identifying, across the jurisdictions that the organisation operates in (or intends to operate in), the highest standard of data protection on each issue. The relevant issues could be the 9 principles in the Safe Harbor agreement or the 10 NPPs under the Australian Privacy Act.

Once a highest standard for each area of protection has been identified, policies and procedures should be implemented that ensure that all companies within the multinational group comply with the highest standard identified, so as to offer a consistent approach across all countries.

Pending EU discussions on the binding corporate rules, an alternative approach would be to implement a transborder data transfer deed between entities in all countries in the corporate structure. By concluding such an arrangement the multi-national can ensure that all companies are contractually bound to follow these 'highest minimum standards' and hence be able to transfer data across borders without consent.

4. Conclusion

Overall the pace and standard of international data protection is being set by the European Union through its emerging status as an economic power. Other countries are having to follow suit with programs or legislation to avoid being left behind. Even the US, to a limited extent, is starting to tow the privacy line. To ensure that multi-national businesses can use the personal information they collect, both efficiently and commercially no matter where they collect it, it is essential that the legal implications of transborder data transfers be assessed. This assessment must include a thorough analysis of the available options for compliance and the relative flexibility provided by each method.

Allens Arthur Robinson

30 November 2004