October 1998

Avoiding the clash of the Titans: Contractual compliance with EU privacy protection requirements

Jay Forder
Bond University, jay_forder@bond.edu.au

Follow this and additional works at: http://epublications.bond.edu.au/law_pubs

Recommended Citation

This Journal Article is brought to you by the Faculty of Law at ePublications@bond. It has been accepted for inclusion in Law Faculty Publications by an authorized administrator of ePublications@bond. For more information, please contact Bond University's Repository Coordinator.
Avoiding the clash of the Titans

Contractual compliance with EU privacy protection requirements

by Jay Forder, Consultant Editor

The EU Privacy Directive

We have mentioned the EU Privacy Directive in previous issues. It takes a strong stand in prohibiting the transfer of electronic data from EU member countries to countries that do not have "adequate" privacy protection for personal data. The provisions come into effect this month (October 1998).

Since the Directive was adopted in July 1995, commentators have speculated that it could disrupt the transfer of electronic data between the EU and countries such as the USA, Australia, Japan, and Canada. The Directive certainly reflects a major difference in approach between the European Union and other countries.

The International Chamber of Commerce (ICC) recently publicised an attempt to alleviate the concerns of individual businesses affected by this clash. This report outlines the context and summarises the ICC’s proposals.

Much of the EU Directive sets out the standards expected of member countries in their protection of privacy of personal data. This report does not examine these provisions except to comment that they are similar to the OECD guidelines. The privacy principles underlying the Australian Privacy Act 1988 (Cth) are also based on the OECD guidelines. The crucial difference (and the main reason why Australian law is unlikely to be "adequate") is that the Australian Privacy Act applies to the public sector. Apart from some provisions applying to the credit industry, there is no equivalent protection in the private sector.

The "contractual clauses" exception

The EU Directive provides for some situations in which data can still be exported from a member country despite the lack of adequate privacy protection in the target country. The most important of these contemplates contractual provisions providing sufficient protection:

... a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection ... where the controller adduces sufficient guarantees with respect to protection of privacy ...; such guarantees may in particular result from appropriate contractual clauses.

The "controller" here refers to the person who is in control of the personal data. In the situation we contemplate, this would be the person exporting the data from the EU country (referred to as the "data exporter"). The person in the non-EU country to whom data is transferred is referred to as the "data importer".

The ICC’s model clauses

On 24 September the ICC released a set of model contractual clauses. They suggest the provisions be included in any transborder data flow contract if it is uncertain whether the importing country has adequate privacy protection.

The ICC has also urged the European Commission to publicly approve the
clauses as offering adequate protection. The Commission has the power to do this under Article 26(4). Traders adopting the provisions would then know in advance that they comply with the Directive.

The model clauses are designed to be generic. Their main import is that they require the data importer to observe the laws applicable in the data exporter’s jurisdiction. The content of those laws does not need to be identified. This avoids the need to specify particular aspects of the privacy principles, such as requirements that the data be accurate and up to date. Thus, with minor modifications, the clauses can be used for transfers of personal data from any country (even a non-EU country) to a country that does not provide similar protection.

Summary of exporter’s main undertakings (clauses 1 and 2)
The data exporter warrants that it has complied, and will continue to comply, with the laws of its jurisdiction in collecting and processing the data. It undertakes to supply a copy of such laws to the data importer.

Amongst other things, the exporter also undertakes:
- to respond promptly to enquiries from the data subject or authorities in the member state; and
- to disclose details about the data importer if requested; and
- to notify the data importer of the enquiry.

Summary of importer’s main undertakings (clauses 3 and 4)
The data importer warrants that it has full legal authority to use the data for the agreed purpose. It also warrants that it has suitable measures in place regarding unauthorised alteration, loss or destruction of the data.

The importer also undertakes:
- to process the data in accordance with the laws of the country of the data exporter;
- to provide the data subject with the same rights of access and correction as provided for in the country of the exporter;
- not to use the data for any unauthorised purpose;
- not to disclose or transfer the data to a third party or country without the prior consent of the exporter (who is to be satisfied with the terms of the transfer);
- to identify an individual within its organisation who will respond to enquiries promptly; and
- to submit to an audit of its processing and information handling practices.

Summary of other provisions (clauses 5 to 9)
The data importer and exporter indemnify each other against the consequences of breach. A termination clause provides for termination if the data importer is in breach, and includes a right to the return or deletion of the personal data.

A dispute resolution clause applies the rules of arbitration of the ICC. The law governing the contract is specified as the law of the exporter’s country.

Conclusion
One of the strongest concerns with the “contractual provisions” exception to the EU Directive is that it is unlikely to be able to fully protect the interests of the data subject. Data subjects are not privy to the contract between exporter and importer. They might have considerable difficulty obtaining remedies against the importer in a foreign jurisdiction.

These provisions appear to go some way towards addressing this concern in most instances. Initially, responsibility for responding to citizens’ concerns will rest with the data exporter under the laws of the EU member state. The model clauses in turn give exporters and data subjects the same rights against importers in foreign jurisdictions as they would have in their own jurisdictions. It goes without saying that an Australian (or other) importer who uses these clauses ought to make quite sure they are familiar with the laws applicable in the country of the exporter!

The clauses are relatively straightforward. They might assist parties who are concerned about the clash between the EU Directive and local privacy laws, particularly if the European Commission approves the clauses.

2 Article 25(1).
3 The full text of the proposals can be obtained at <http://www.iccwbo.org/Commissions/Telecom_1T/Mode I_clauses.htm>.
5 Article 26(2).