Pillsbury Winthrop Shaw Pittman LLP

Global Sourcing

Phillip Rees
Partner | London
+44.20.7847.9562
phillip.rees@pillsburylaw.com

Cynthia Fairweather O'Donoghue
Senior Associate | London
+44.20.7847.9579
cynthia.odonoghue@pillsburylaw.com

John L. Nicholson
Senior Associate | Washington, DC
+1.202.663.8269
john.nicholson@pillsburylaw.com

1540 Broadway | New York, NY 10036
www.pillsburylaw.com

This article first appeared in
The Journal of E-Commerce, Technology and Communications
February 2007, Volume 13, Issue 2, ISSN 1357 3128

Transferring Personal Data Outside the EEA: The Least Worst Solution

Article 8 of the European Convention on Human Rights guarantees the right of an individual to privacy. The European Commission, whose role is to harmonise differing legislation of EU Member States, drafted the EU Data Protection Directive 95/46/EC, in order to ensure that citizens (or data subjects) throughout the EU were guaranteed basic rights as to their personal data. Member States were obliged to implement the Directive into their respective national legislation by 24 October 1998.

The Directive regulates the processing (defined so widely as to encompass any action) of personal data. However, given the multi-national nature of companies and the Internet, the Commission was concerned with what might happen to personal data that was transferred outside the EU. Article 25 of the Directive therefore prohibits the transfer of personal data to a third country outside the EEA unless that third country ensures an adequate level of protection for the data transferred. Articles 25(6) and 26 permit various exceptions to this prohibition, and a number of Commission-approved business solutions have been developed to take advantage of these exceptions. Unfortunately, the adequacy of these solutions has been sorely tested, leaving multi-national data controllers frustrated and industry bodies like the International Chamber of Commerce (ICC) seeking practical ways to improve their efficacy. This article considers the current position with regard to each of the solutions available from the perspective of multi-national organisations.

The Exceptions

The following exceptions permit a data controller (the person who determines the purposes for and means by which personal data is processed) to transfer data to outside the EEA: the Adequacy Club, being a group of countries whose data protection laws have been approved as sufficiently stringent; actual consent to such transfer by the data subject concerned; various other derogations in the Directive, not all of which are terribly useful to multi-national companies; the Safe Harbor programme, permitting data to be transferred to US companies who have enrolled; the Standard Contractual Clauses (SCCs), Commission-approved contracts for use between companies based inside and outside the EEA, and the Binding Corporate Rules (BCRs), for use by companies with subsidiaries based inside and outside the EEA.

Transferring Personal Data Outside the EEA: The Least Worst Solution

The Adequacy Club

Article 25(6) says that the Commission may find that a third country ensures an adequate level of protection. To date, the Commission has found that Argentina, Canada, Guernsey, the Isle of Man, Switzerland and any US-based company subscribing to the Safe Harbor principles afford such a level.

This is not an over-subscribed club. Recital 4 of the Commission Decision 2001/497/EC states that "the Commission is unlikely to adopt adequacy findings under Article 25(6) for more than a limited number of countries in the short or even medium term." Other countries that have adopted comprehensive data protection law are Australia, Chile, Hong Kong, Japan, and New Zealand. Nevertheless, they have not been elected members of the Adequacy Club. Article 25(6) therefore is of limited use to a multi-national company wishing to transfer personal data globally (unless, of course, such a company conducts business exclusively among the members of the Adequacy Club).

'Article 25(6) ... is of limited use to a multi-national company wishing to transfer personal data globally (unless, of course, such a company conducts business exclusively among the members of the Adequacy Club).'

Consent

Article 26(1) says that personal data may be transferred to outside the EEA where the data subject has given his consent unambiguously to the proposed transfer. In November 2005 the Article 29 Working Party, the independent EU advisory body on data protection and privacy, issued a paper on the Article 26 derogations (WP 114) which highlighted that consent must be a clear and unambiguous indication of wishes, given freely, specific and informed.

Thus, although consent seems a stress-free resolution to the Article 25 prohibition, WP 114 spells out that the threshold is high. Clear and unambiguous requires a specific action on the part of the data subject: an implied or retrospective consent does not meet the definition. For example, the Working Party stressed that in their opinion the relationship between an employer and employee would impede any such consent from being defined as "given freely". Moreover, "specific and informed" means specific to each data transfer and informed as to the specific circumstances regarding each transfer. For these reasons consent is unlikely to be of use to any multi-national company seeking to transfer personal data to outside the EEA.

Other Article 26(1) Derogations

There are a number of derogations under Article 26(1), of which two are likely to be of interest to a multi-national company. The first of these applies where the transfer is necessary for the performance of a contract between the data subject and the data controller. The second applies where the transfer is necessary for the performance of a contract concluded in the interest of the data subject.

Like consent, although these derogations seem at first glance a handy way to get out of Article 25, in reality they are of limited use. In the July 1998 Working Paper on the application of Articles 25 and 26 to the transfer of personal data (WP 12) the Working Party emphasised that the "necessity" criterion would be interpreted strictly and so limit both derogations, while in WP 114 the Working Party expressed the view that neither exception would apply to a contract between employer and employee.

Furthermore, in WP 114 the Working Party pointed out that the positioning of Article 26(1) was effectively misleading. Article 26(1) lists various derogations to Article 25. Article 26(2) comments that in certain circumstances

such as appropriate contractual clauses, the transfer of personal data to outside the EEA may be acceptable. The Working Party stated that "they would find it regrettable that a multi-national company would plan to make significant transfers of data without providing an appropriate [contractual] framework… and that the derogations of Article 26(1) should preferably be applied to cases in which it would be genuinely inappropriate, maybe even impossible, for the transfer to take place under Article 26(2)".

The advice is clear: just because Article 26(1) is positioned before Article 26(2) does not mean that it comes before Article 26(2). If a multi-national company wants to transfer personal data to outside the EEA it should be thinking along the lines of Safe Harbor, the SCCs, or the BCRs.

Safe Harbor

In July 2000, the Commission propagated the Safe Harbor decision (2000/520/EC), recognising the US Department of Commerce's Safe Harbor programme as providing adequate protection for transfers of personal data from the EU. Participation in Safe Harbor is generally limited to US organisations that are under the jurisdiction of the US Federal Trade Commission (FTC). Certain organisations (such as telecoms carriers, meat packers, banks, insurance companies, credit unions and not-for-profit organisations) may not be eligible for Safe Harbor.

The Safe Harbor programme is set out in seven privacy principles, 15 FAQs, the Commission's decision and letters between the Departments of Commerce and Transportation, the FTC and the Commission. The seven privacy principles are related to: notice, choice, onward transfer, access, security, data integrity, and enforcement. Participation in Safe Harbor by US organisations is voluntary and is subject to an annual self-certification requirement available online.

Despite being in force since November 2000, as of December 2006, fewer than 1100 companies have signed up for Safe Harbor, of which just under 900 are currently certified as participating. One reason for companies' reluctance is the nature of the dispute resolution and enforcement requirements of the programme. One method of compliance is committing to cooperate with European data protection authorities. Since complying with European data protection authorities is required under the SCCs, the Safe Harbor program adds the potential for additional penalties to the process. For example, a company's failure to abide by the Safe Harbor principles might be considered deceptive and actionable by the FTC, which has the power to seek administrative orders and civil penalties of up to $12,000 per day.

'...a company's failure to abide by the Safe Harbor principles might be considered deceptive and actionable by the FTC, which has the power to seek administrative orders and civil penalties of up to $12,000 per day.'

Another reason for the lack of participation is the annual recertification requirement, which requires participating organisations annually either to submit a new self-certification form or to reaffirm its existing self-certification. An organisation's reaffirmation must include the following four points:

- the information previously submitted to the Department of Commerce for purposes of self-certification is still correct and accurate;
- the officer is authorised to certify the organisation's continued adherence to the Safe Harbor framework;
- the officer understands that misrepresentations in any information provided by the organisation may be actionable under the False Statements Act; and

- as a consequence of this annual self-certification, failure to adhere to the Safe Harbor framework may lead to enforcement action by the relevant enforcement authority.

The recertification process adds effort and risk over and above that necessary to implement and comply with the SCCs. The advantages of the Safe Harbor programme are that enforcement is generally done in the US and it does not include the liability regimes of the SCCs. However, because of the additional effort and risk associated with the Safe Harbor programme, most companies transferring data from the EU to the US have elected other means to comply with the EU's data protection requirements.

Perhaps Safe Harbor's primary drawback for multi-nationals is that for them its usefulness is limited to EEA subsidiaries of a US parent company. A multi-national company wishing to transfer data globally may prefer a universal solution and not one that can only be used for the US and leaves the company needing to implement different solutions elsewhere.

'... any multi-national company wishing to use the SCCs should contemplate the possibility of two potential actions against it, in the event of an infringement.'

Standard Contractual Clauses

There have been three Commission-approved versions of these, allowing the transfer of personal data to outside the EEA under Article 26(2). The SCCs are contractual arrangements, offering third party beneficiary rights to affected data subjects, between a data exporter, based inside the EEA, and a data importer, based outside the EEA, whereby both parties undertake not to infringe the Directive. The data controller, who remains at all times liable to the applicable data protection authority for any infringement of the Directive, need not necessarily be the data exporter. Therefore, any multi-national company wishing to use the SCCs should contemplate the possibility of two potential actions against it, in the event of an infringement: (1), an investigation into their activities by the applicable data protection authority (and in the UK infringement of the Data Protection Act is a criminal offence with the possibility of an unlimited fine if tried in the Crown Court), and (2), a civil suit by the data subject against the data exporter and/or data importer, as applicable.

Controller-to-controller, SET I: Commission Decision (2001/497/EC) on standard contractual clauses for the transfer of personal data to third countries.

SET I never proved popular with data exporters, on account of its joint and several liability regime, making the data exporter liable to the data subject for any infringement by the data importer. Given that it is not possible to vary or modify the terms of the SCCs, companies tended to avoid SET I which is nevertheless still in force; however, multi-national companies wishing to transfer personal data to outside the EEA should probably consider SET II, which was drafted in order to circumvent the liability regime drawback in the light of recommendations made in 2004 by the ICC.

Controller-to-controller, SET II: Commission Decision (2004/915/EC) amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.

The liability regime of SET II is fault-based, which marks a considerable business improvement upon SET I. However, there are still some drawbacks to using SCCs SET II.

SET II incorporates a due diligence regime (not in SET I) whereby the data exporter undertakes to use reasonable efforts to ensure that the data importer is able to satisfy its legal obligations. In the event that the data exporter does not use reasonable efforts and the data importer infringes the Directive, the data subject may in those circumstances proceed directly against the data exporter. A multi-national company wishing to use SET II therefore needs to take this due diligence regime seriously, and of course not all data importers will relish the requirement to submit their data protection structures to a data exporter's due diligence investigation.

Furthermore, where there is an alleged infringement by the data importer the data exporter is under an obligation take appropriate action against the data importer within a month. If he does not do so, the data subject may then proceed directly against the data importer. It is not clear whether he can join a suit against the data exporter as well for failing to take appropriate action.

Finally, SET II contains enhanced provisions allowing the data exporter to terminate the contract. SET I envisages solely the circumstance where a data importer informs a data controller that pending legislation may be about to force him to breach the SCCs: in such an eventuality the data exporter may terminate the contract. SET II provides for six scenarios allowing the data exporter to terminate. For this reason SET II may be less attractive to data importers.

Nonetheless, this version, despite drawbacks, is the most up-to-date Commission-approved resolution of the Article 25 prohibition for controllers. However, if the data importer is a processor (as defined in the Directive) the version below should be used.

Controller-to-processor: Commission Decision (2002/16/EC) on standard contractual clauses for the transfer of personal data to processors established in third countries.

The liability regime for the controller-to-processor SCCs makes the data exporter responsible for any infringement unless he has disappeared or become insolvent, in which case the data importer is liable.

In October 2006 the ICC submitted a paper to the Commission proposing amendments to the Standard Contractual Clauses (controller-to-processor). The paper does not modify the liability regime. It does, however, address the issue of onward transfers. The ICC comments that data transfers to a second data processor are very common in practice, an opinion supported by the Commission SCCs review, in which the Commission said that it would like to see clear rules to perform onward transfers to data processors. SCCs SETS I and II do cover onward transfers to data controllers but not to processors. In the event that the ICC's proposed amendments to the SCCs controller-to-processor are approved, the provisions concerning onward transfers to data processors can be re-used if the Commission gets round to adopting a consolidating decision merging all three ICC sets, something the Commission review said it was "considering".

'The liability regime for the controller-to-processor SCCs makes the data exporter responsible for any infringement unless he has disappeared or become insolvent, in which case the data importer is liable.'

Binding Corporate Rules

The Working Party's paper on Binding Corporate Rules (WP 74) published in June 2003 set out a framework for a multi-national company to implement a legally binding company policy ensuring data protection compliance for data transfers throughout a company group, in accordance with Article 26(2). The BCRs were intended as an alternative to the SCCs, because of ongoing business criticism of their efficacy. Unfortunately, owing to time and cost drawbacks inherent to the approval procedure for BCRs, very few companies have actively engaged with the BCR process: in the UK only General Electric has had a BCR application approved. Given that we are four years down the line from the original Working Party paper, this does not count as a resounding success.

'... the BCRs are free of the SCCs controller-to-controller SET II due diligence regime.'

Advantages

Although the SCCs may not be varied or modified, the BCRs may be written to a company's specifications, and even based on existing data handling policies they may already have. Furthermore, the BCRs create a safe haven for data transfer: once they have been approved a company is free to transfer data globally within its affiliates, without having to use the SCCs each time there is a data transfer. Finally, the BCRs are free of the SCCs controller-to-controller SET II due diligence regime.

Disadvantages

There are various ongoing disadvantages: the BCRs must be binding within the group, in all locations of the group, so the company must examine the structure of the group and the applicable law to each member of the group; data subjects must be given third party beneficiary rights no less generous than those granted in SCCs controller-to-controller SET I (which was a joint and several regime); data subjects have the right to choose jurisdiction of the member of the group at the origin of the transfer or the EU headquarters of the group; there is an annual audit requirement; and the safe haven works only within the group so that any onward transfers will probably mean going back to the SCCs and the whole point of the BCRs was to act as an alternative to the SCCs. However, the two main disadvantages are time and cost.

Time and Cost

Despite the publication in 2005 of a Working Party paper setting out a model checklist for any BCR application (WP 108) in the UK only General Electric has had a BCR application approved and then only for employee data. General Electric's application was not speedily processed and has taken five months in Scandinavia alone: a BCR application has to be approved separately by each applicable data protection authority. There are considerable legal costs associated with this sort of timeframe. The BCR application is therefore a complex document to draft, with a lengthy timeframe to implement.

The good news is that in July 2006 the ICC has submitted for Working Party approval a Standard Application BCR form for use by any company wishing to apply for BCRs and recognized by all Member States. If the form is approved, more companies could come round to BCRs.

Conclusion

The Directive, although short in length (only 34 articles), imposed substantial requirements upon any data controllers processing personal data inside the EEA, and in particular on those wishing to transfer such data to outside the EEA. Such data controllers were potentially subject to a double liability regime. Not only were they liable at all times for any infringement of the Directive, they were also directly liable to the data subject if they took it upon themselves to be the data exporter. Not surprisingly therefore, any method of compliance with the Article 25 prohibition was always going to be onerous: there is no easy answer to a difficult question.

Recognising this, the Commission and Working Party have laboured hard to provide practical business-like solutions, acceptable to companies operating in a global environment, basing these solutions on Article 26(2) of the Directive which says that appropriate contractual clauses are an acceptable method of compliance with the prohibition. The Commission has helped to draft the principles of Safe Harbor, and published variants of SCCs, two for controller-to-controller, and one for controller-to-processor. The Working Party has commented on Safe Harbor and SCCs in order to help the Commission in its drafting, has advised on the Article 26(1) derogations, and has published another solution—BCRs.

However, there remain disadvantages inherent to all these solutions. The Adequacy Club has an inadequate membership, the Article 26(1) derogations are limited in application, the Safe Harbor applies solely to the US, the SCCs cannot be modified or varied so are not always applicable in a changing global business environment, and the BCRs are unattractive as regards the time and money they cost both to implement and maintain. Nevertheless, these solutions are currently the only viable solutions for transferring personal data to outside the EEA. Any company wishing to transfer personal data to outside the EEA is going to need to consider them, and to come to the least worst solution.

'... any method of compliance with the Article 25 prohibition was always going to be onerous: there is no easy answer to a difficult question.'