DechertOnPoint

January 2007 / Issue 1

A legal update from Dechert's Data Protection and Privacy Group

Legitimising Cross-Border Data Flows by the Self-Assessment Method: Different Approaches throughout Europe

The transfer of personal data to outside the E.U. is problematic for international organizations. Article 25(1) of the Directive 95/46/EC[1] (the Directive) prohibits the transfer of personal data to any country or territory outside the E.U. (a third country) unless the third country 'ensures an adequate level of protection' for the rights and freedoms of those individuals whose personal data is being transferred.

There are, of course, a number of well-known methods of legitimising a transfer of personal data and, in broad terms, they fall into two categories. First, the level of protection can be adequate as a result of putting in place one of a number of structural methods (safe harbour for transfers to the U.S., model contracts, binding corporate rules, adequacy findings by the E.U. Commission). Secondly, a transfer to a third country is actually allowed under the Directive where there is no adequate protection by means of certain derogations set out in Article 26(1) (including consent and necessity for the performance of a contract). Conceptually, these two approaches are very different; the former approach assures adequacy, the second approach allows a transfer where there is no adequacy.

Whilst most of the above methods are well-known and frequently discussed (and indeed criticized), there is a further method, not so well-known, which is available in some, if not all, of the member states--namely, for the data controller itself to assess the level of protection and ensure by other means, without putting in place one of the instruments sanctioned by the Commission, that such protection is adequate. This article focuses on this method, which we refer to as adequacy 'self-assessment', and compares it to the other methods, discussing its strengths and weaknesses and how the authorities or regimes in a number of countries including the U.K., France, Germany, Belgium and the Netherlands approach this method.

We commence, however, with a brief summary of other methods of legitimising data transfers out of the E.U., and indeed the European Economic Area, although a full exposition is outside the scope of this article.

Summary of Common Methods of Legitimising Data Transfers

Community Finding

The easiest way of legitimising the transfer is to choose your third party country carefully! Article 25(6) of the Directive allows the European Commission to make a finding (which the member states must adhere to) in relation to the adequacy either of a specific country or in relation to a class of transfers to that country. Transfers to those counties (including Argentina, Switzerland and Canada) would automatically be adequate for the purpose of the Directive. Some member states (for example, France) have additional requirements even if this route is used[2].

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] The French data protection authority (CNIL) requires companies filing declarations or authorizations prior to collecting and processing personal data to expressly specify if they are transferring data outside the E.U. and, if so, to describe the transfer in quite some detail including describing the identity and country of the recipient of the data, the type of data transferred and the purpose for it. This applies even if the country has been adjudged as adequate.

Binding Corporate Rules

Recently, binding corporate rules (BCRs) have been introduced by the European Data Protection Commissioners, with supplementary guidance issued by the U.K. Information Commissioner (the U.K. ICO), which has been welcomed as offering a further method by which personal data may be transferred out of the E.U. BCRs constitute an internal suite of documents within a company setting out how the company intends to provide adequate safeguards to individuals whose personal data is being transferred to a third country, and must contain data protection safeguards no less than those provided for in the Directive.

BCRs are not straightforward to put in place, in that a corporate group must create legally binding internal documents for the benefit of affected individuals, with one delegated company taking responsibility for the compliance of the whole of the group, with the whole of the group being required to undertake comprehensive data protection audits. When all these steps are fulfilled, the BCRs would be submitted to one national data protection supervisory authority (perhaps in the country where the organization has its E.U. headquarters) which will in turn liaise with the other relevant national data protection authorities with the aim of approval by all the authorities concerned. An iterative process then takes place as comments are fed back to the lead authority and the organization.

For all these reasons, BCRs have been criticized as offering a solution which is only really appropriate for the most sophisticated international organizations and, in particular, only for those that wish to share amongst their group and not externally.

Safe Harbour

Another method used to fall within Article 26(2), when the destination country is the U.S., is the safe harbour scheme.

This scheme, approved by the E.U. in July 2000, is a voluntary scheme by which U.S. organizations and companies commit themselves to complying with a set of data protection principles backed up by guidance provided by the U.S. Department of Commerce and a number of Frequently Asked Questions. There are seven safe harbour principles which broadly reflect the contents of the Directive. By complying with the safe harbour principles, U.S. companies adopt an adequate level of protection for transfers of personal data to the U.S. from E.U. member states.

The scheme is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the E.U. or facing prosecution by European authorities under European privacy laws. Certifying to the safe harbor scheme will ensure that E.U. organizations know that they provide 'adequate' privacy protection, as defined by the Directive, when transferring data to the U.S.

Model Contracts

A further method which is recognised by Article 26(2) of the Directive is the use of model contracts containing standard contractual clauses.

The European Commission provides model contracts between the data exporter and the data importer intended to provide adequate safeguards for personal data transferred by the data exporter in the E.U. to processors and controllers outside the E.U. The original set of data-controller-to-data-controller clauses (Set I) were not widely used, and an alternative set promulgated by various business organizations, has gained much wider currency (Set II).

The use of one of these contracts would automatically remove any risk of non-compliance so that an exporting controller who uses the model clauses does not need to make a separate assessment of adequacy in relation to the transfer. However, the model contracts have been subject to criticism and may not always be appropriate. Despite Set II removing some of the bigger problems with the earlier Set I, some important down-sides remain.

First, the non-E.U. data importer will have to accept contractual liability as against the data subject for its breach of the provisions set out in the contract. Moreover, there are increased powers for the supervisory authorities to intervene and prohibit or suspend data flows. Lastly, for present purposes, the due diligence requirements contained in Set II may not be attractive where the data importer does not necessarily want its facilities and operations to be reviewed by the data exporter. There are other issues, but detailed criticism is outside the scope of this article.

Derogations

Other methods of transferring personal data to third countries bypass the adequacy requirement of Article 25 and, instead, fall within permitted derogations to Article 25 under Article 26(1) of the Directive. This states that transfers of personal data to a third country which do not ensure an adequate

level of protection may take place if one of a number of conditions is satisfied including (there are others) the data subject giving his consent to the proposed transfer; the transfer being necessary for the performance of certain contracts between the data subject and the controller; or the transfer being necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.

Consent is often discussed, but is not without problems (a full discourse of which, again, is outside the scope of this article). Whilst it is superficially attractive, consent must be given freely, be specific and be informed and, where sensitive personal data is concerned, must also be 'explicit'. Recently, document WP 114 of the Article 29 Working Party[3] suggests that relying on consent may prove to be a 'false good solution', appearing simple at first glance but, in reality, complex and cumbersome. What if one of thousands of data subjects withholds consent? What if one data subject revokes their consent?

The Self-Assessment Approach Under The Directive

The self-assessment approach to legitimising transfers of data from member states to third countries is based on the premise that the data exporter should itself consider and make a judgement as to whether, in the particular circumstances of a transfer, that transfer is made to a country which can ensure an adequate level of protection. It should be made clear at the outset that whilst, arguably, this approach is envisaged in the Directive[4], the Directive left it to member states to decide to allow the approach or not each thought best.

Legal Justification Under The Directive

The legal justification for self-assessment as to adequacy is to be found in paragraph 1 of Article 25 (1) of the Directive:

> *The member states shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if ... the third country in question ensures an adequate level of protection.*

Article 25(2) sets out criteria which factor into an assessment of adequacy as follows:

> *The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.*

These quoted passages do not, in fact, say who should make that assessment. Indeed, although not express, there is a focus on specific transfers which suggests that the assessment could be made by the data controller itself. This issue was considered in the first document published by the Working Party on the transfer issue, back in 1998, 'WP12 – Working Document: Transfers of Personal Data to Third Countries'. This says, at page 26, in the context of decisions as to the adequacy of protection offered in a third country:

> *Such rationalisation is needed irrespective of who is making the decision, whether it be the data controller, the supervisory authority, or some other body established by Member State procedure. (emphasis added)*

WP12 also says, somewhat hidden in footnote 19, that:

> *Member states may set down different administrative procedures to discharge their obligations under Article 25. These may include imposing a direct obligation on data controllers and/or developing systems of prior authorisation or ex post facto verification by the supervisory authority. (emphasis added)*

As we will see, the U.K., Germany, Belgium and the Netherlands took the approach (at least arguably) of allowing a data controller to discharge the obligation of assuring adequacy and doing so without necessarily following one of the instruments promulgated at the European (or indeed national) level. France and some of the other countries surveyed in this article expressly did not.

---

3 The Working Party is body set up by Article 29 of the Directive to give guidance on the Directive generally and consists of representatives from the supervisory authorities of each member state.

4 As we will see below, the European Commission disagrees that this is the case.

The view of The European Commission

In 2003, the European Commission published its first report on the implementation of the Directive[5]. Amongst other issues, it commented on the wide divergences in implementation approaches to Article 25 and said at paragraph 4.4.5:

> *The approach adopted by some member states, where the assessment of the adequacy of protection provided for by the recipient is supposed to be made by the data controller, with very limited control of the data flows by the state or the national supervisory authority, does not seem to meet the requirement placed on member states by the first paragraph of Article 25(1).*

This view is not, however, justified in the report, except by a quotation of the very same Article 25(1) that is also used to justify the opposite position by certain member states.

It should also be added that where the European Commission was also critical of the approach taken in other member states that do not allow this approach but take what might be considered as the other extreme--namely, to require some form of prior authorisation from the relevant supervisory authority for each and all transfers to third countries.

The Position in The U.K.

In the U.K., Article 25(1) is enshrined as one of the eight fundamental 'data protection principles', set out in the U.K. Data Protection Act (the U.K. Act). The eighth principle states that the level of protection in relation to the cross border transfer of personal data must be 'adequate in all the circumstances of the case'.

The U.K. took up the option allowed in the Directive of imposing a direct obligation upon data controllers to ensure adequacy, and also leaves them to assess adequacy. In short, the data controller is directed to approach this data protection principle in the same manner as it is directed to approach the other 'data protection principles'[6]. Just as it makes its own assessment as to whether or not there is a legitimisation for the processing (Article 6(a), or the first data protection principle in the U.K.) or as to security measures to take (Article 17, or the seventh principle in the U.K.), it too has to make its own assessment as to whether there is an adequate level of protection.

ICO Guidance

The U.K. ICO has recently published guidance comprising two separate documents: a legal analysis of the eighth principle 'The Eighth Data Protection Principle and International Data Transfers' (the U.K. Legal Analysis) and also a more business orientated paper containing general compliance advice for companies transferring personal data overseas (the "U.K. General Compliance Advice"). In the U.K. Legal Analysis the U.K. ICO states that if he is required to investigate a particular transfer, he *'will expect to see evidence that the data controller making the transfer has followed the approach and the various criteria set out in this guidance'*.

The U.K. Legal Analysis then goes on to discuss the process which a data controller should go through after determining that there is a proposed transfer of data. Most importantly for the purposes of this article, the U.K. Legal Analysis states that the controller should decide whether there is an adequate level of protection for the transfer. This might be on the basis of a community finding of adequacy in relation to a particular country (discussed above) or a particular type of transfer to a U.S. safe-harboured organization (also discussed above). However, it might be on the basis of the data controller *itself* assessing adequacy.

It will be recalled that Article 25(2) of the Directive sets out the factors which must be taken into account in assessing whether there is adequacy and this has been implemented in the U.K. in Schedule 1, part II paragraph 13 of the U.K. Act. The U.K. Legal Analysis usefully categorises the factors to be taken into account into two categories, the 'general adequacy criteria' and the 'legal adequacy criteria'.

The general adequacy criteria are factors which the exporting data controller will be able to identify easily and include the nature of the personal data, the country or territory of origin of the information contained in the data, the country or territory of final destination of that information, the purposes for which, and period during which, the data are intended to be processed, and any security measures taken in respect of the data in that country or territory.

---

5 COM(2003) 265 of 15.5.2003.

6 The other seven 'data protection principles' are transpositions of the requirements in Article 6 of the Directive (as to data quality) and Article 17 (as to security).

The legal adequacy criteria may be more difficult for the controller to assess as they are factors relating to the legal system in force in the third country. They include the law in force in the country or territory in question, the international obligations of that country or territory, and any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases). As the legal adequacy criteria are matters outside the control of both the data exporter and the data importer, the U.K. ICO recognises that it would be inappropriate for exporting controllers to consider such legal adequacy criteria exhaustively in the case of every transfer to a third country. However, exporting controllers are expected to be able to recognize countries where there would be a real danger of prejudice or where it is clear that the country in question does not provide any legal protection in relation to the exported data and the U.K. ICO has made it clear that he expects the data controller to take a more cautious approach in relation to any such transfer.

Guidance on Model Contracts and Derogations

If this prior assessment leads to a conclusion that there is no adequate protection, then the U.K. Legal Analysis says that *at that stage* the use of model contracts or other adequacy assurance safeguards should be implemented; such as safe-harbour where the importer is in the U.S. or one of the exceptions in Schedule 4 to the Act [which are the equivalent to the derogations provided for by Article 26(1)].

Practical Applications and Examples

Given that what is contemplated seems, on the face of it, to be a somewhat detailed analysis and, given that fairly straightforward solutions such as model contracts or signing up to safe harbour (if U.S. is the destination) are available, one might wonder why bother with self-assessment? The U.K. ICO does make clear, however, that the detailed analysis might often be appropriate but will not, in fact, be necessary in some fairly standard scenarios where there is little risk. The two main examples of this are when the transfer is between group companies and where there is a transfer of data to a data processor outside the E.E.A.

Intra-Group Transfers

As an initial point, it is worth noting that if there is only one legal entity (or an international partnership) which shares data across borders it is, as a matter of English law, not possible to put into place a model contract between the different 'branches' of that entity.

In earlier guidance on this issue dating from 1999, now superseded, the U.K. ICO had indicated that where transfers of personal data take place within an international or multinational company and there is in place an internal contract, policy or code regarding the transfer of personal data within such an organization, a strong *presumption* of adequacy can be made. This earlier advice predated the advent of Binding Corporate Rules and so, perhaps for this reason, is not emphasised as much in the new guidance. However, it is still possible to undertake this more informal approach and the U.K. General Guidance note states just that--the data controller can still set up an internal code of conduct in relation to personal data shared throughout the group, and that code may well be sufficient to adduce adequacy. The U.K. General Guidance does warn, however, that a data controller does take the risk that there could be a future challenge as to whether the codes do in fact provide adequacy.

This is indeed one of the main advantages of taking a self-assessment approach. The introduction of formally authorised BCRs is likely to be costly and time-consuming, with the possibility of having to amend the rules following comments from all member states. An informal code of conduct does not have that danger (but, of course, is not necessarily capable of being adopted in other member states).

Outsourcings

A transfer by a data controller to a data processor in a third country outside of the E.E.A. will, of course, be caught by the eighth principle. The U.K. Legal Analysis makes it clear that this type of arrangement will not normally present a problem from an adequacy standpoint, and that the parties do not, in fact, ordinarily have to put in place one of the instruments or (if the processor is U.S.-based) have it join the safe-harbour.

The reason for this is that, where such a transfer is made, the U.K. data controller exporting the data remains the controller and, as such, remains subject to the Commissioner's powers of enforcement. In effect, it remains responsible for protecting individuals' rights under the U.K. Act in relation to the overseas processing of the personal data by the data processor.

Of course, where there is a transfer to a data processor, wherever that processor is located, a

data controller must still comply with the seventh data protection principle (the equivalent of Article 17) which states that *'appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'.*

The U.K. Act goes on to say that the data controller must choose a data processor providing sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out, and take reasonable steps to ensure compliance with those measures (such as conducting regular audits and reviews)[7]. In addition, a data controller will not be regarded as complying with these security requirements unless the processing is carried out under a contract 'made or evidenced in writing', stipulating that the processor is to act only on instructions from the data controller, and which, in turn, contains an obligation on the part of the data processor to comply with provisions equivalent to those imposed on a data controller by the seventh principle.

However, the U.K. ICO would still expect the data controller to undergo a proper 'self-assessment' on the types of matters referred to above, as well as making some due diligence checks in relation to the data processor. If such due diligence and analysis did not reveal any particular risks in relation to the transfer, then the controller-processor relationship and the security measures implemented to comply with the Seventh Principle would be likely to ensure adequacy and, therefore, the transfer would be able to proceed in compliance with the eighth principle.

Other Examples Where Self-Assessment is Appropriate

In practice, self-assessment is likely to be used by U.K. companies when one of the other methods is inappropriate, inapplicable or simply thought to be too cumbersome in the particular circumstances. Examples given by the U.K. ICO in the General Advice include:

- an employee travelling outside the E.E.A. on a business trip with a laptop containing personal information. The employer in the U.K. remains the data controller. A contract cannot be put in place and, if the trip is not to the U.S., the U.K. employer cannot safe-harbour. No other solutions are, in fact, possible and, as long as proper password protection is included on the laptop and sensible precautions are taken, it is reasonable for a data controller to decide there is adequate protection for that personal data

- a U.K. university wishes to transfer biographies of its academics to potential students outside the E.E.A. – it is simply not possible to put in place contracts directly with each potential student. Nothing of a private nature is included, and the information is generally publicly available anyway. It is difficult, according to the U.K. ICO, to see a problem with adequacy here

- the sending of a mailing list to a non-E.E.A. mailing house where the product or business is not particularly sensitive, and where there is a proper contract in place governing how the information is to be used

- as mentioned above, if there is only one legal entity (or partnership) which shares data across borders, as a matter of law, it is not possible to put into place a model contract between the different 'branches' of that entity

The Position in Belgium

In Belgium, the issue of self-assessment is rather vague and ambiguous, with some divergence between theory and practice.

In Belgium, the Directive has been implemented through the Belgian law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data (the Belgian Law). Article 21 § 1(2) of the Belgian Law contains exactly the same provision as Article 25 (2) of the Directive. Consequently, the Belgian Law does not explicitly state who is responsible for the assessment of the adequacy of the level of protection offered by the third country. However, unlike the Directive, Article 21 § 2 of the Belgian Law goes on to provide that:

> *The King shall lay down after advice of [the Privacy Commission] and in accordance with [the Directive] for which categories of processing operations of personal data and under which circumstances the transfer of personal data to countries outside the European Community is not authorized.* (emphasis added)

[7] Paragraph 11 of Part II of Schedule 1 to the Data Protection Act 1998

The law would appear to point towards a case-by-case self-assessment except where the King has blacklisted a country or a specific transfer or set of transfers to a specific country.

This interpretation of the Law is confirmed by several documents. First, by the parliamentary preparatory documents, the initial draft of the Project of Law provided that the King shall lay down a list of *'countries outside the European Community that do not ensure an adequate level of protection'*. This was eventually modified as a result of a 1998 amendment following an argument that it would be preferable to blacklist specific transactions to specific countries rather than countries in general. Secondly, by the Belgian Privacy Commission itself, in its advice on the initial draft of the Project of Law[8], it stated (unofficial translation):

> *The Privacy Commission is of the opinion that, in case of a transfer of personal data to a country outside the European Community, it pertains in the first place to the data controller to determine whether the concerned third country ensures an adequate level of protection, taking into account the criteria mentioned in Article 21,§1(2) of the Project of Law [Article 25(2) of the Directive]. The European Directive does not require that every transfer of data to a country outside the European Community should be submitted to a prior determination by the King that the concerned country ensures an adequate level of protection.*

The advice of the Belgian Privacy Commission also contains some interesting justifications of a case-by-case self-assessment method. It suggests that a general system of prior adequacy determination by an authority would threaten to block the circulation of data and stresses that it is easier for the concerned data controller to assess, for a specific kind of data transfer, whether or not the country or countries to which the data is to be transferred ensures an adequate level of protection. The Belgian Privacy Commission's website also states that data controllers have to assess whether the third country to which the data is to be transferred ensures an adequate level of protection and that, in case of doubt, an opinion can be requested from the Privacy Commission.

However, the position in Belgium is confused by, in part, some parliamentary preparatory documents which seem to exclude self-assessment as a method of ensuring adequate protection e.g. the explanatory statement to the 20 May 1998 session on the project of law which states that *'the adequacy must be appreciated by the Members States or by the European Commission'.*

Furthermore, the Belgian Privacy Commission, in an explanatory note of 27 October 2006 (regarding data transfer notifications), states that, in case of a transfer to a third country, the declaration must specify whether or not the concerned country ensures an adequate level of protection and, for this purpose, the data controller has to check the Privacy Commission's 'ISO list' which specifies for each country its level of protection[9]. It is interesting to observe that the only countries that are considered to offer an adequate level of protection are the member states and the countries white-listed by the European Commission. Although the Belgian Privacy Commission is only an advisory body which seems to support the self-assessment method, it is difficult to simply ignore the Privacy Commission's list of countries that do not ensure an adequate level of protection.

The Position in France

French law simply does not recognise the concept of self-assessment.

Given this, it is interesting to discuss how France would treat those situations described above which the U.K. would consider appropriate for a self-assessment approach (and in some cases indeed impossible to legitimise in any other way):

- if an employee of a French company were travelling outside the E.E.A. on a business trip with a laptop containing personal information, according to a French law analysis this would not necessarily mean that there would be transfer of personal data to a third country (especially if there is proper password protection included in the laptop). If a data controller remained concerned or knew that personal data was going to be transferred by its employee to an entity outside the E.E.A. (e.g., as a result of the visit of the employee or entering into a contract with the non-E.E.A. entity) it should put in place a contract based on the E.U. Commission model clauses (controller-controller contract or controller-subcontractor depending on the relationship)

8 Nr. 30/96 of 13 November 1996

9 'level of protection 1' being adequate and 'level of protection 2' not being adequate

- if a French university wishes to transfer biographies of its academics to potential students outside the E.E.A., the French university should obtain the academics' express consent to such transfer (with the inherent problems in that approach as described above)

- if a company sends data to one of its branch offices located outside the E.U., then the French data protection authorities would most likely consider that the company should still put into place a model contract with its branches. The contract would be entered into between the company and its branch in the relevant jurisdiction. In practice, the company would be undertaking to comply with E.U. data protection principles in a jurisdiction outside the E.U.

The Position in Germany

The Directive has been implemented into German law by the Bundesdatenschutzgesetz (BDSG). Germany has taken the view that it is impossible for the state itself to control each and every data exchange and has therefore promoted self-regulation and self-assessment in the BDSG.

According to sections 4b(3) and (5) of the BDSG, it is the data controller who is solely responsible for the legality of the data transfer and, therefore, it is the data controller who has to assess the adequacy of data protection in the third country that the data is sent to. The assessment of adequacy in the third country is to be judged objectively but (unlike in the U.K. where the ICO has given detailed guidance) in Germany there is no additional guidance from that contained in the Directive on how such assessment should be made.

However, there is one particular issue of note in the BDSG. Whereas under Article 25(2) of the Directive, the assessment has to be made with respect to the adequacy of the level of protection afforded by a third country, under section 4b(2) of the BDSG, such assessment has to be made with respect to the data recipient. In practice this would mean that it is up to the data controller to assess whether the data recipient provides an adequate level of data protection. This type of assessment would be much easier to perform than assessing the level of protection in general in a specific third country.

Whilst the wording of the BDSG is clear, there is a body of opinion that Germany did not correctly implement the Directive[10]. As a consequence, this view would hold that section 4b(2) of the BDSG should be construed in a manner which conforms with the Directive and that the assessment has to be made in respect of the third country. However, so far there have been no court rulings and, despite criticism by the Commission[11] of Germany's (and other countries') system of self-assessment, there have been no amendments to the BDSG. Accordingly, and from a practical point of view, the data controller can and should rely on the current wording of section 4b(2) of the BDSG.

The Position in The Netherlands

Articles 25 and 26 of the Directive have been implemented in the Netherlands through articles 75 to 78 of the Dutch Data Protection Act of 6 July 2000 (the Dutch Law). The position in the Netherlands, unlike in some other countries, is clear on the issue of self-assessment of the adequacy of the level of protection ensured by a third country. An analysis of the Dutch Law, its explanatory memorandum, the statements of the Dutch Minister of Justice and the statements of the Dutch College for Personal Data Protection (CBP) shows that the assessment of the adequacy of a specific personal data transfer is, in the first instance, the responsibility of the data controller. However, in cases of doubt, the data controller may request information from the CBP. There is no obligation on a data controller to request advice from the CBP and the CBP has no obligation to analyse the issue specifically.[12]

This position has been confirmed by the Dutch Minister of Justice when answering questions during parliamentary discussions. The Minister of Justice has stressed that because self-assessment decisions remain subject to an ex-post review by the courts, it may be advisable in some situations to request a prior opinion from the CBP or the Ministry of Justice.

The CBP makes some interesting observations in its policy paper on transfers of personal data to third countries. The policy paper explains that the CBP's policy on the provision of information in response to requests from data controllers will mainly be focused on the provision of general information. It

10 Rittweger/Weisse, Computer und Recht, 2003, p142.

11 Para 4.4.5 of the Commission's First Report referred to above in note 5.

12 Page 193 of the explanatory memorandum to the Dutch Law

states that *'the evaluation of the actual level of protection in a specific case will in principle have to be carried out by the controller, legally bearing the responsibility for such a decision'*. The CBP will only evaluate a specific case if there is a sufficient interest justifying such an evaluation, for example if there is great risk involved in the transfer, an important interest at stake, or if complaints have been filed by concerned data subjects.

The CBP also comments that the data controller should not make an adequacy decision in cases where it has any doubt, stressing that there is no legal obligation on a data controller to self-assess as there are other alternatives:

> *It is advisable for the controllers not to take the decision to let a transfer go ahead unless the circumstances surrounding the case make it very clear that the level of protection in the third country is adequate. In case of doubt, a transfer should not take place on the basis of such a decision but could still be legally allowed on the basis of one of the exceptions of Article 77, paragraph 1, or a permit of the Minister of Justice under Article 77, paragraph 2*[13].

In other words, in cases of doubt or where the controller does not want to take any risk, the mechanisms of Article 26 of the Directive are available to the data controller.

Other Countries

Some other European countries expressly exclude self-assessment as a method of ensuring the adequacy of protection offered by third countries.

Greece: Greece has implemented the Directive through Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data. This law is very clear and straightforward on the issue of self-assessment, expressly stating in Article 9.1 that transfers of data to third countries will only be permitted if a permit has been granted by the Greek data protection authority[14]. There is therefore no scope for self-assessment by the data controller.

Spain: The Spanish Law 15/1999 on Personal Data Protection is also straightforward on the issue. Article 33 states that the Spanish Data Protection Agency is responsible for determining whether or not there is adequate protection in a third country.

Portugal: The Portuguese law n°67/98 of 26 October 1998 on the Protection of Personal Data (implementing the Directive), expressly states in article 19.3 that *'it pertains to the National Commission for the Protection of Personal Data (the CNPD) to determine whether a country outside the European Union ensures an adequate level of protection'*. The CNPD has confirmed that data transfers to third countries must receive prior authorization from the CNPD. Transfers of personal data to third countries white-listed by the Commission must still be notified to the CNPD.

Slovenia: The Personal Data Protection Act of the Republic of Slovenia, under the heading 'Transfer of personal data to third countries', provides that personal data can only be transferred to third countries when the National Supervisory Body has issued a decision that the country to which the data is to be transferred ensures an adequate level of protection of personal data. The Act also contemplates a list of countries recognized as ensuring an adequate level of protection and a list of countries which have been found in part to ensure an adequate level of protection.

Malta: Malta's Data Protection Act 26/2001 provides that the adequacy of the level of protection ensured by a third country is to be determined by the Data Protection Commissioner.

Problems with Self-Assessment

Although this is suitable for some data controllers (in particular, those where their presence in Europe is limited to those countries which recognise the method), there are some problems with the self-

---

13 Dutch College for Personal Data Protection: 'Policy Paper on transfers of personal data to third countries in the framework of the new Dutch Data Protection Law').

14 'the transfer of data is permitted to a non-member state of the European Union following a permit granted by the Authority if the latter deems that the country in question guarantees an adequate level of protection. For this purpose the Authority shall particularly take into account the nature of the data, the purpose and the duration of the processing, the relevant general and particular rules of law, the codes of conduct, the security measures for the protection of personal data, as well as the protection level in the countries of origin, transit and final destination of data. A permit by the Authority is not required if the European Commission has decided, on the basis of the process of Article 31, paragraph 2 of Directive 95/46/EC of the Parliament and the Council of 24 October 1995, that the country in question guarantees an adequate level of protection, in the sense of Article 25 of the aforementioned Directive' (unofficial translation)

assessment approach. The main problem, as can be seen from the above, is that not all member states have adopted the Directive in such a way as to allow self-assessment. The Directive is a minimum standard and some member states have in place more restrictive regimes which perhaps even require prior authorisation. Even if the legislation was adopted in such a way so as to allow this type of approach, the enforcement bodies may simply not agree that this is the correct approach. Not all member states have the detailed guidance on the issue available as, say, in the U.K.

Secondly, there remains the possibility that the data controller has wrongly assessed the adequacy issue. This would then be a breach of the Directive or of the implementing legislation. Thus an advantage of binding corporate rules, model contracts, and safe harbour are that they are *guaranteed* to be adequate. Having said that, certainly in the member states (such as the U.K. and Belgium) where there is official guidance as to the use of this approach, it must be considered unlikely that there will be official enforcement action when a data controller has, in good faith, gone through the steps set out by that guidance, although private actions may always be a danger.

It is for the second reason that even lawyers in the U.K. (where there is the clearest of guidance from the supervisory authority) do not often point their clients in this direction, but if a data controller were willing to live with some risk, it may be an approach worth exploring in a jurisdiction which allowed for a data controller assessment.

Conclusion

Self-assessment is available in many of the countries surveyed in this report. There are some differences in approach even amongst those countries, with, for example, the U.K. almost directing the use of self-assessment in the first instance with fall-back on the other structural methods when not available or in the case of doubt, and with the Netherlands taking the completely opposite stance.

The main criticism of it, however, remains that there is no legal certainty in using this approach. Even when it is available as a method, it is possible that the data controller, having carried out the exercise in good faith (and following any official guidance), will have got the assessment wrong, and that may for some organizations always be a worry. Nonetheless, it may well in the instance of simple, perhaps ad hoc, transfers be a method which is practical for easy use, especially when there is a reluctance in a recipient organization to accept what they might (however unjustly) consider onerous contractual obligations to data subjects and associations under, for example, the model contracts.

A version of this Note will appear in the January 2007 issue of World Data Protection Report. The authors are Renzo Marchini, Sarah Delon-Bouquet, Olaf Fasshauer, Jean-Yves Steyt and Benedikte Verdegem.

Practice group contacts

For more information, please contact one of the lawyers listed, or the Dechert lawyer with whom you regularly work. Visit us at www.dechert.com.

Sarah Delon-Bouquet
Paris
+33 1 53 65 05 12
sarah.delon@dechert.com

Olaf Fasshauer
Munich
+49 89 21 21 63 21
olaf.fasshauer@dechert.com

Renzo Marchini
London
+44 20 7184 7563
renzo.marchini@dechert.com

Jean-Yves Steyt
Brussels
+32 25 35 54 25
jean-yves.steyt@dechert.com

Benedikte Verdegem
Brussels
+32 2 535 5440
benedikte.verdegem@dechert.com

Dechert LLP

www.dechert.com

UK/Europe

Brussels
London
Luxembourg
Munich
Paris

US

Austin
Boston
Charlotte
Harrisburg
Hartford
New York
Newport Beach
Palo Alto
Philadelphia
Princeton
San Francisco
Washington, D.C.