

CHAPTER 7: CROSS-BORDER INFORMATION TRANSFERS

7.1 As was indicated in Issue Paper 24, the ease with which electronic data flows across borders leads to a concern that information protection laws could be circumvented by simply transferring personal information to other countries, where the national law of the country of origin does not apply. This information could then be processed in those countries, frequently called “information havens,” without any limitations.

7.2 It is for this reason that Article 25 of the European Directive imposes an obligation on member states to ensure that any personal information relating to European citizens is protected by law when it is exported to, and processed in, countries outside Europe.¹

¹ See Bygrave *Data Protection* at 81; Broadly similar, but less complicated, principles on transborder data flows are set down in paras 17-18 of the OECD Guidelines and in Principle 9 of the UN Guidelines. The latter differ in some respects from the other instruments in their terminology - employing the (undefined) criteria of “comparable” and “reciprocal” protection - though they probably seek to apply essentially the same standards as the criteria of “equivalency” and “adequacy”. At the same time, while the Convention and OECD Guidelines have been primarily concerned with regulating flow of personal data between the Member States of the CoE and OECD respectively, the UN Guidelines seek to regulate data flows between a broader range of countries

7.3 The European Union and all its trading partners have been required to have adequate information protection regimes, conforming to the European Data Protection Directives, with effect from 24 October 1998.² This means that transfer of information from the EU to both private and governmental bodies will normally only be permissible with countries which have acceptable information protection legislation or selfregulation covering the information protection principles outlined in Chapter 4 of the Discussion Paper.³

7.4 The following points should be noted:⁴

- a) Article 25 requires an “adequate level” of protection, not “comparable level” or similar level”.
- b) Under Article 25, the determination of “adequate level” can be made by the transmitting country, by another EU member nation, or by the EU staff in Brussels.
- c) Article 25(2) provides that an adequate level of privacy protection is assessed in light of all circumstances surrounding the information transfer operation, including:
 - the nature of the information;

²

The following clauses from the Directive govern the transfer of information:
CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES
Article 25
Principles

1. 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, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. 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.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision.

³

See also DMA Submission on Open Democracy Bill.

⁴

Fisher R Excerpt from *Privacy of Personal Information and the National Information Infrastructure* as referred to in a fax received from ITC Consumer Liaison(hereafter referred to as “Fisher excerpt”).

- the purpose and duration of the information processing and transmission operation;
- the rules of law in force; and
- the professional rules and security measures established for the information.

7.5 Information sharing now takes place on an international scale and involves a tremendous amount of personal information. Information regarding credit transactions, for example, flows routinely from the country where charges are incurred to the country where the bill is ultimately settled. A broad ban on the transfer of information to third countries would therefore be disruptive and expensive. In light of these economic realities, the Directive provides certain exemptions to this provision of Article 25 in Article 26. In terms of these exemptions adequacy is determined in each individual case or with regard to individual bodies.

7.6 Article 26⁵ identifies the circumstances under which an EU member nation can authorise transfer in the absence of an adequate level of information protection, including:

- a) the data subject has unambiguously given consent to the transfer (it is not clear whether assent is required, or if notice with the opportunity to opt out is sufficient).

5

Art 26 provides as follows:

Article 26 Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

- (a) the data subject has given his consent unambiguously to the proposed transfer; or
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or(e) the transfer is necessary in order to protect the vital interests of the data subject; or(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation" are fulfilled in the particular case.

2. Without prejudice to paragraph 1, 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 within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2. If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2). Member States shall take the necessary to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

b) the company receiving the information establishes privacy rights through appropriate contractual clauses.⁶

7.7 It is therefore possible to protect the privacy of information transferred to countries that do not provide “adequate protection” by relying on a private contract containing standard information protection clauses. This kind of contract would bind the data processor to respect fair information practices such as the right to notice, consent, access and legal remedies. In the case of information transferred from the European Union, the contract would have to meet the standard “adequacy” test in order to satisfy the Data Protection Directive.⁷

7.8 A number of model clauses that could be included in such a contract were outlined in a 1992 joint study by the Council of Europe, the European Commission and the International Chamber of Commerce.⁸

7.9 Although the EU Commission never issued a formal opinion on the adequacy of privacy protection in the United States, there were serious doubts whether the United States’ sectoral and self-regulatory approach to privacy protection would pass the adequacy standard set out in the Directive.

7.10 The European Union commissioned two prominent United States law professors, who wrote a detailed report on the state of United States privacy protections and pointed out the many gaps in United States protection.⁹

7.11 The United States strongly lobbied the European Union and its member countries to find the United States system adequate. In 1998, the United States began negotiating a “Safe

⁶ See further Bygrave *Data Protection* at 82; Bennett CJ “Prospects for an International Standard for the Protection of Personal Information: A Report to the Standards Council of Canada” August 1997 available at <http://web.uvic.ca/~polisci/bennett/research/iso.htm> at 9.

⁷ EPIC and Privacy International *Privacy and Human Rights Report 2002* at 16.

⁸ Joint Study of the Council of Europe and the Commission of the European Communities (1992), available at http://www.coe.fr/dataprotection/Etudes_Rapports/ectype.htm See also “Model clauses for use in contracts involving transborder data flows” prepared by the Working Party on Privacy and Data Protection of the Commission on Telecommunications and Information Technologies of the International Chamber of Commerce.

⁹ See EPIC and Privacy International *Privacy and Human Rights Report 2002* at 17 and reference to Schwartz PM and Reidenberg JR *Data Privacy Law* Michie 1996.

Harbor” agreement with the European Union in order to ensure the continued transborder flows of personal information. The idea of the “Safe Harbor” was that United States companies would voluntarily adhere to a set of privacy principles worked out by the United States Department of Commerce and the Internal Market Directorate of the European Commission. These companies would then have a presumption of adequacy and they could continue to receive personal information from the European Union. Negotiations on the drafting of the principles lasted nearly two years and were the subject of bitter criticism by privacy and consumer advocates.¹⁰

10

EPIC and Privacy International *Privacy and Human Rights Report 2002* at 17 and reference to Public Comments Received by the United States Department of Commerce in Response to the Safe Harbor Documents April 5, 2000, available at <http://www.ita.doc.gov/td/ecom/Comments400/publiccomments0400.html>.

7.12 The United States Department of Commerce and the European Commission in June 2000 announced that they had reached an agreement on the Safe Harbor negotiations that would allow United States companies to continue to receive information from Europe. On July 26, 2000, the Commission approved the agreement.¹¹ Over 200 companies have joined the Safe Harbor.¹²

7.13 The principles of the agreement require the following:

- All signatory organisations to provide individuals with “clear and conspicuous” notice of the kind of information they collect, the purposes for which it may be used, and any third parties to whom it may be disclosed.
- This notice must be given at the time of the collection of any personal information or “as soon thereafter as is practicable.”
- Individuals must be given the ability to opt out of the collection of information where the information is either going to be disclosed to a third party or used for an incompatible purpose.
- In the case of sensitive information, individuals must expressly consent to (opt in) the collection.
- Organisations wishing to transfer information to a third party may do so if the third party subscribes to Safe Harbor or if that third party signs an agreement to protect the information.
- Organisations must take reasonable precautions to protect the security of information against loss, misuse and unauthorized access, disclosure, alteration and destruction.
- Organisations must provide individuals with access to any personal information held about them, and with the opportunity to correct, amend, or delete that information where it is inaccurate.

7.14 Privacy advocates and consumer groups both in the United States and Europe are critical of the European Commission’s decision to approve the agreement, which they say will fail to provide European citizens with adequate protection for their personal information. The agreement rests on a self-regulatory system whereby companies merely promise not to violate

¹¹ Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the United States Department of Commerce, available at http://europa.eu.int/comm/internal_market/en/media/dataprot/news/decision.pdf.

¹² Safe Harbor List <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+lis>.

their declared privacy practices. There is little enforcement or systematic review of compliance. The Safe Harbor status is granted at the time of self-certification. There is no individual right to appeal or right to compensation for privacy infringements. There is an open-ended grace period for United States signatory companies to implement the principles.

7.15 In February 2002 the European Commission issued a report on the practical operation of the European Union-United States Safe Harbor Agreement.¹³ This was the first report to evaluate the success of the agreement. It concluded that all the essential elements of the agreement are in place and that a structure exists for individuals to lodge complaints if they feel their rights have been infringed. It did find, however, that there is not sufficient transparency among the organisations that have signed up to Safe Harbor and that not all dispute resolution providers relied on to enforce Safe Harbor actually comply with the privacy principles in the agreement itself.

7.16 With the exception of the USA, the requirements set out in the EU Directive have resulted in growing pressure outside Europe for the passage of strong information protection laws. Those countries that refuse to adopt meaningful privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive information.

7.17 It is also important to consider that the transfer of information to South Africa from Europe is governed from the European side by the directive or country legislation that is implemented in terms of the directive. This issue is obviously of concern to business in South Africa.

7.18 Respondents to Issue Paper 24 were in general in favour of the principle that care should be taken to ensure that the South African model will be regarded as adequate in terms of sec 25. There was, however, a difference of opinion regarding the question whether adequacy necessarily implied a strong, regulatory information protection system.

13

European Commission Staff Working Paper, February 2002, available at http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf.

7.19 Respondents who were in favour of ensuring adequate protection of information through a comprehensive general statute argued as follows:

- * South Africa's international trade aspirations would be adversely affected by the adoption of a privacy model that is considered inadequate by international and EU standards. This impact would not only be felt on a bilateral basis, but on the multilateral level. It would result in lost opportunities for database warehousing, and possible cross border trade in financial and telecommunications services. Moreover, as the SADC region moves towards a trade bloc in 2008, South Africa's policies should be a guiding best practice for the region and capable of adaptation by our regional trading partners.¹⁴

- * It will definitely affect South African international trade negatively if we do not meet the requirements of article 25 of the EU directive.¹⁵

¹⁴ The Internet Service Providers Association.

¹⁵ The Banking Council; Gerhard Loedolff; Nedbank; Eskom Legal Department.

- * Currently, as South Africa does not have any information protection legislation in place, it has been impossible to meet the "adequate level of protection" standard required of countries within the European Union (in accordance with Article 25 of the applicable EU Directive). Nedbank has accordingly been forced, in the absence of such legislation locally which would have facilitated the bank processing information within South Africa, at great extra cost, to set up processing centres in Europe, in order to meet European information protection legislative requirements. This has resulted in the effective cost to market of the bank's outsourcing service being driven up and could very well be the reason for preventing the bank from obtaining further business processing outsourcing deals within Europe on the basis of not being cost competitive enough. ¹⁶Therefore, it is imperative that appropriate legislation is enacted urgently so that the business mentioned above and other similar South African businesses that process information emanating from offshore parent or affiliate companies or third party customers are not prevented from doing so. The bank is of the view that South Africa, as a country, could attract a substantial amount of information processing business from abroad should this legislation be in place. All the other factors which would make such a business option viable are already in place in favour of South African information processing businesses (such as the fact that we are an English speaking country, we have similar time zones to Europe, labour costs are reasonable etc.). ¹⁷The bank further faces the practical difficulty that it is currently precluded from transferring personal information relating to its customers from its branches in London, Hong Kong, New York and other jurisdictions to its head office in South Africa, for the reason that South Africa has not yet adopted adequate information protection legislation. This has an impact on various aspects of the bank's business, including forensic investigations, monitoring activities in the context of money laundering legislation and other aspects. The bank reiterates that the new information protection legislation must be in line with and satisfy the "adequate protection" requirement of the EU Directive. If it fails to satisfy this requirement, the bank is of the view that such legislation

¹⁶ Nedbank.

¹⁷ Nedbank.

would be inadequate in that it will not assist local banks at all, either in their international business processing operations nor in their local banking operations *vis a vis* their offshore branches and banking operations¹⁸.

7.20 On the opposite side, the following arguments were posed:

- * Article 25 (2) offers a measure of flexibility by its reference to "...the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measure which are complied with in these countries."¹⁹ There is therefore a case for satisfying the adequacy provision through selfregulation and the courts.²⁰

18 Nedbank.

19 Sanlam Life; Legal Service.

20 Sagie Nadasen Legal Adviser : Sanlam Life Law Service.

* Du Motier and Goemans (*Data Privacy and Standardizaion 2000*) suggest that the assessment of “adequate level of protection” is analyzed on the basis of two core elements, namely: the content of the rules applicable and the means for ensuring their effective application. On the basis of this approach, they contend that countries which have, for example, ratified the Council of Europe’s Code 108/81 will benefit from a presumption to be allowed under article 25(1), provided that additional enforcement mechanisms are in place and that the country in question is the final destination of transfer. Commenting on the Directive’s reference to “...professional rules and security measures which are complied with in that country...” they observe that the Directive requires that regard be had to non-legal rules that may be in force in the third country in question, provided that these rules are complied with. In assessing these non-legal rules the applicable criteria are:²¹

(a) an objective analysis of the content of the non-legal rule by reference to core information protection principles and the transparency of applicable codes, and

(b) an evaluation of the effectiveness of the self-regulatory instrument. In the view of the Working Party, the following three functional criteria for judging the effectiveness of the protection must be met,

(i) a good level of compliance which depends often on the awareness of the code’s existence – a system of dissuasive and punitive sanctions is one way of achieving this while mandatory audits are another;

(ii) the existence of an impartial, independent support and help to data subjects who are faced with a problem involving the processing of their personal information. Accordingly, an easily accessible, impartial and independent body to hear complaints from data subjects and adjudicate breaches of the code must therefore be in place; and,

(iii) appropriate redress in cases of non-compliance must be provided to obtain a remedy and compensation.²²

* Possibilities exist for *ad hoc measures* where there are inadequate levels of

21 Ibid.

22 Ibid.

protection. Thus, a contract between the information provider in the EU and the recipient in the third country can be concluded whereby additional safeguards for the data subject are provided due to the absence of an enforceable set of information protection rules.²³

- * Carey (*Data Protection Act 1998* (1998)) notes one must have regard to the following in respect of the “adequate:” requirement , (a) the nature of the personal information ; (b) the country or territory of origin of the information contained in the data; (c) the country or territory of final destination of that information; (d) the purposes for which and period during which the information are intended to be processed; (e) the law in force in the country or territory in question; (f) the international obligations of that country or territory; (g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases); and (h) any security measures taken in respect of the information in that country or territory. Carey asserts that this list is not exhaustive and also refers to the possibility of a contract between the transferor and transferee – he contends that it is arguable that if the provisions of the contract are enforceable in the legal system of the transferee’s legal system, then that country is in fact providing protection.²⁴
- * Both the contractual provisions concluded between South African and foreign companies (which provisions will ensure that core principles and procedures are adequately addressed) and the existing Constitutional protection of fundamental freedoms and rights are more than sufficient to meet information protection concerns of the regulatory authorities in the EU. South African companies must of course ensure that any audit will confirm they have requisite systems and processes in place to meet the EU requirement of “adequate level of protection ”²⁵.
- * The majority of African States, if not all, have no information privacy legislation in place and subjectively it is foreseen that with the problems of the continent being what they are, the introduction of such legislation will not

23 Ibid.

24 Ibid.

25 Ibid.

be seen for some considerable time. South Africa is presently increasing its presence on the continent and many South Africa organisations have offices throughout Africa. In effect this will mean that South Africa would isolate itself from the rest of the continent in its attempt to blindly follow directives designed for economies far removed from Africa and South Africa. However having made this submission it is obviously necessary that the country must provide some form of “adequacy” in order to satisfy Article 25 and our major trading partners. It would therefore appear necessary to provide within the proposed legislation certain exemptions and to make submissions to the European Union in this regard.²⁶

7.21 A new initiative being explored by multi-national corporations to overcome the difficulties when transferring information on a global basis is the development of global codes of conduct that would govern all their practices worldwide at the same time.²⁷

7.22 Given the growing number of cross-border information transfers, the idea of relying on global rules for all cross-border information transfers is attractive. The code of conduct concept is a simple one. Related companies doing business in multiple countries would apply just one set of rules to govern their information transfers from within the European Union to outside the EU rather than having to comply with the specific requirements of each of the countries in which they operate. Companies could also draft these codes so that they comply with the privacy laws in non-EU countries.

7.23 The Directive makes provision for and encourages members to make use of codes of conduct. The primary obstacle to using codes of conduct for cross-border transfers is that there is no streamlined mechanism for approving enterprise-wide codes. Mutual recognition by different states or co-operation mechanisms between the regulatory authorities of the different states could, however, facilitate the needs of multinational companies with establishments in several jurisdictions.²⁸

²⁶ SAFPS; Credit Bureau Association.

²⁷ Wugmeister et al *Codes of Conduct* at 3.

²⁸ Wugmeister et al *Codes of Conduct* at 1; See also Art 29 Working Party Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Directive to Binding Corporate Rules for International Data Transfers June 2003.

7.24 In summary the following points should be noted:

a) If a country wants to compete in the international market, it will have to ensure that it provides adequate information protection in terms of international standards. Although the international community (as well as the Directive) is not prescriptive as to the way in which these standards are to be met, it is safe to say that having an appropriate comprehensive statute that meets the requirements of article 25 of the Directive, with an independent regulatory authority to champion this cause, will be a big step in the right direction. This will mean that adequacy will not have to be assessed in the context of each particular transfer, but rather on a per country basis. It is obvious that this will ease the way for South African companies interested in international exposure as well as for international companies wishing to trade in South Africa.

b) However, the fact that the Directive makes provision for other ways in which to acquire adequacy contradicts the argument that South Africa will be adversely affected, in so far as its trade with African countries are concerned, should it comply with sec 25. Trade with African countries will be more difficult than with Europe since adequacy will have to be established in each particular transfer. This is, however, the status quo at the moment and this position can not be ascribed to the effects of the information protection legislation. The legislation will however, improve the country's position regarding countries that do have proper legislation in place.

7.25 It is therefore the Commission's opinion that a general comprehensive law making provision for adequate information protection should be instituted. This will be achieved by making provision for the inclusion of the information protection principles as well as for the means to ensure their effective application. The Bill will furthermore stipulate that information will not be transferred to another country if proper safeguards for the protection of the information has not been made.

7.26 The legislative enactment will read as follows:

Transborder information flows

94. *A responsible party in South Africa may transfer personal information about a*

data subject to someone (other than the responsible party or the data subject) who is in a foreign country only if -

- (a) the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Protection Principles set out in Chapter 3 of this Act; or*
- (b) the data subject consents to the transfer; or*
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the data subject's request; or*
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or*
- (e) all of the following apply:*
 - (i) the transfer is for the benefit of the individual;*
 - (ii) it is reasonably impracticable to obtain the consent of the data subject to that transfer;*
 - (iii) if it were reasonably practicable to obtain such consent, the individual would be likely to give it.*

Comment is invited