

Policy paper on transfers of personal data to third countries in the framework of the Dutch Data Protection Act (WBP)

Diana Alonso Blas, LL.M.
Senior International Officer

Dutch Data Protection Authority
(College bescherming persoonsgegevens)

Table of contents

<u>INTRODUCTION</u>	<u>4</u>
<u>1. SCOPE OF APPLICATION OF THE RULES AND GENERAL CONSIDERATIONS</u>	<u>6</u>
1.1. SCOPE OF APPLICATION OF THE WBP	6
1.2. WHAT IS A TRANSFER OF PERSONAL DATA?	6
1.3. TO WHICH KIND OF TRANSFERS DO THESE RULES APPLY?	8
1.4. FROM WHAT DATE DOES THE WBP APPLY?	8
<u>2. THE RULES OF THE WBP ON TRANS-BORDER DATA FLOWS TO THIRD COUNTRIES: A THREE-STEP APPROACH</u>	<u>9</u>
2.1. IS THERE ADEQUATE PROTECTION? (ARTICLE 76)	10
2.1.1. WHAT IS ADEQUATE PROTECTION?	10
2.1.2. WHO DECIDES ON ADEQUACY ON A CASE-BY-CASE BASIS?	12
2.1.3. WHEN AND HOW DOES THE EUROPEAN COMMISSION MAKE AN ADEQUACY FINDING?	14
2.1.4. CONCLUSION	16
2.2. IS IT POSSIBLE TO MAKE USE OF ONE OF THE EXCEPTIONS OF ARTICLE 77.1?	17
2.2.1. UNAMBIGUOUS CONSENT OF THE DATA SUBJECT	17
2.2.2. TRANSFER NECESSARY FOR THE PERFORMANCE OF A CONTRACT OR FOR PRE-CONTRACTUAL MEASURES	18
2.2.3 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	19
2.2.4. TRANSFER NECESSARY ON IMPORTANT PUBLIC INTEREST GROUNDS OR FOR THE ESTABLISHMENT, EXERCISE OR DEFENCE IN LAW OF ANY RIGHT	20
2.2.5. TRANSFER NECESSARY FOR THE PROTECTION OF THE VITAL INTEREST OF THE DATA SUBJECT	20
2.2.6. TRANSFER FROM A PUBLIC REGISTER OR A REGISTER THAT CAN BE GENERALLY CONSULTED	20
2.2.7. CONCLUSION	21
2.3. IS IT POSSIBLE TO OBTAIN A PERMIT FOR THE DATA TRANSFER FROM THE MINISTER OF JUSTICE (ARTICLE 77.2)?	22
2.3.1. WHAT ARE “ADEQUATE SAFEGUARDS”?	22
2.3.2. REQUIREMENTS FOR CONTRACTUAL SOLUTIONS	23
2.3.3. CAN CONTRACTUAL SOLUTIONS BE USED IN ALL CASES?	25
2.3.4. USE OF THE MODEL CONTRACTS APPROVED BY THE EUROPEAN COMMISSION	26
2.3.5. PROCEDURE FOR THE GRANTING OF A PERMIT	29
2.3.6. WHAT HAPPENS AFTER A DECISION CONCERNING A PERMIT APPLICATION HAS BEEN TAKEN?	30
<u>3. A PARTICULARLY INTERESTING COMMISSION ADEQUACY FINDING: THE SAFE HARBOUR</u>	<u>32</u>

4. PRACTICAL CASE STUDIES	34
<hr/>	
4.1. A REAL CASE: IBAZAR-EBAY	34
4.1.1. FACTS OF THE CASE	34
4.1.2. SEARCHING FOR A SOLUTION	34
4.1.3. CONCLUSION	35
4.2. A TRANSFER FROM A DUTCH CONTROLLER TO A PROCESSOR IN INDIA	35
4.2.1. FACTS OF THE CASE	35
4.2.2. SEARCHING FOR A SOLUTION	35
4.2.3. CONCLUSION	36
4.3. A TRANSFER FROM A DUTCH PUBLIC-SECTOR INSTITUTION TO A PUBLIC-SECTOR INSTITUTION IN A THIRD COUNTRY	36
4.3.1. FACTS OF THE CASE	36
4.3.2. SEARCHING FOR A SOLUTION	36
4.4. A TRANSFER FROM A DUTCH COMPANY TO AN INTERNATIONAL DATABASE	37
4.4.1. FACTS OF THE CASE	37
4.4.2. SEARCHING FOR A SOLUTION	37
4.4.3. CONCLUSION	37
4.5. A TRANSFER FROM A DUTCH COMPANY TO A “LESS-DEMOCRATIC” THIRD COUNTRY	38
4.5.1. FACTS OF THE CASE	38
4.5.2. SEARCHING FOR A SOLUTION	38
4.5.3. CONCLUSION	38
4.6. A TRANSFER FROM A DUTCH FINANCIAL INSTITUTION TO SEVERAL FINANCIAL INSTITUTIONS OUTSIDE THE EUROPEAN UNION	39
4.6.1. FACTS OF THE CASE	39
4.6.2. SEARCHING FOR A SOLUTION	39
4.6.3. CONCLUSION	39
 ANNEXES:	 41
<hr/>	

Application form for a permit as defined in Article 77.2 WBP (mandatory use)

Introduction

Chapter 11 (Articles 76-78) of the Act on the protection of personal data of 6 July 2000¹ establishes a special regime for the transfer of personal data from the Netherlands to a third country. A third country is a country outside the EU. The requirements laid down in Articles 76 to 78 have been adopted to implement the provisions of Chapter IV of EC 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 data².

This Directive has a double objective: on the one hand, it aims to create a high level of protection of the right to privacy with respect to the processing of personal data and, on the other hand, it aims to ensure the free movement of such data within the European Union³. When personal data are to be transferred to a third country the Directive makes this transfer subject to special conditions. A transfer can only take place if the requirements imposed by the Directive are respected.

This policy paper aims to offer guidance concerning the application and interpretation of this chapter of the WBP to all those intending to transfer personal data to third countries. In order to facilitate understanding of the paper, examples will be used and a number of case studies will be included in the last chapter of the paper. Obviously they do not cover all possible questions a controller can face. In this context, the Dutch Data Protection Authority⁴ would like to emphasise that most of these practical questions can only be answered in the light of the specific circumstances of a given case; in other words, each situation should be dealt with on its own merits.

This paper will concentrate on Articles 76 to 78 WBP and will only refer to other articles of this Act when this is necessary for understanding of the text.

Needless to say, all other provisions of the WBP remain applicable. Any transfer to a third country falling under its scope will only be in conformity with it if it complies with all the provisions of the Act relevant to the specific case⁵.

It should be born in mind that, as the WBP implements the Directive into Dutch law, the text of the Directive sometimes plays an important role in the correct interpretation of the provisions of this Act. This is the reason why this paper will at times refer to the Directive. A number of documents approved by the so-called Working Party for the Protection of Individuals with regard to the Processing of Personal Data⁶ will also be mentioned at certain

¹ Official Bulletin 2000, no. 302, in Dutch Wet Bescherming Persoonsgegevens, often referred to as “the WBP”.

² Official Journal of the European Communities L 281, p. 31, Volume 38, 23 November 1995. From now on referred to as “the Directive”.

³ As the Directive applies as well to the countries of the European Economic Area, the same regime applies to these countries. Therefore, where the text refers to the EU, it should be read as EU/EEA.

⁴ In Dutch College bescherming persoonsgegevens, often referred to as CBP.

⁵ For all other questions concerning the application of the WBP see the explanatory memorandum to the act (memorie van toelichting) or the guidelines published by the Ministry of Justice (Handleiding voor verwerkers van persoonsgegevens), available in English on:

http://www.minjust.nl:8080/a_beleid/thema/wbp/manual/handleidingwbpuk.pdf

⁶ This Working Party was created by Article 29 of the European Directive, which defines its composition and tasks. See for more information the article by ALONSO BLAS, D., *Towards an uniform application of the European Data Protection Rules: The role of the Article 29 Working Party* in *Privacy & Informatie*, 4^e jaargang, nummer 1, February 2001. All documents approved by the Working Party are available on the website of the European Commission: <http://www.europa.eu.int/comm/privacy>

points, as they offer valuable interpretations of different aspects of the Directive. Practical experience has shown that these documents are often the basis for the discussions on trans-border data flows held in Brussels.

Both the Minister of Justice and the Data Protection Authority play important roles in the context of the granting of permits, which is one of the main issues dealt with in this paper. The Minister is entitled to take the final decision concerning a permit request, taking into account the advice given by the CBP. The Data Protection Authority has an advisory role to the Minister and is at the same time the supervisory authority for the processing operations in question, not only at the moment that the decision concerning the permit is taken but also subsequently.

The Minister of Justice is obliged to seek the advice of the CBP before issuing a permit. According to the text of the explanatory memorandum of the WBP⁷, the advice of the CBP will play an important role in this context and will contribute to the quality of the decisions concerning permits due to its expertise and experience in this field.

This paper has been drafted by the Dutch Data Protection Authority. However, in order to make the procedure for granting a permit more user-friendly and speedy, the CBP and the Ministry of Justice have agreed on the main issues covered by this paper. They have come to a common understanding of the subject that should enable them to deal with these cases in a coherent and co-ordinated way.

⁷ Page 195.

1. Scope of application of the rules and general considerations

The regime defined in Chapter 11 WBP applies to all situations where a controller falling under the scope of application of this Act is intending to transfer personal data to a third country.

1.1. Scope of application of the WBP

Article 4 WBP defines its scope of application. It applies to the processing of personal data in the context of the activities of an establishment of a controller in the Netherlands. It is therefore necessary to first determine who the controller is, i.e. who is actually responsible for the processing, and secondly to determine if the processing operations take place in the context of the activities of his/her establishment in the Netherlands.

The WBP also applies to the processing of personal data by or for controllers who are not established on the territory of the European Union, whereby for purposes of processing personal data, use is made of equipment, automated or otherwise, situated on the territory of the Netherlands, unless such equipment is used only for purposes of transit through the territory of this country. For example, when a controller established outside the European Union uses cookies to collect personal data in the Netherlands⁸ or uses a processor in the Netherlands.

Where the WBP applies, all relevant provisions of the Act should be complied with. The question of whether personal data may be legally processed and transferred to a third party is always regulated at national level, regardless of the possible international dimension of the transfer. One of the obligations contained in this Act is that controllers have to notify the Dutch Data Protection Authority of their processing operations unless they fall under one of the exceptions determined in the royal decree defining the exemptions to notification of 7 May 2001⁹.

1.2. What is a transfer of personal data?

Often the term “transfer of personal data” is associated with the act of sending or transmitting personal data from one country to another, for instance by sending paper or electronic documents containing personal data by post or e-mail.

This is indeed a type of transfer, but there are other situations that also fall under this definition: all the cases where a controller undertakes action in order to make personal data available to a third party that is located in a third country. The explanatory memorandum to the WBP¹⁰ makes clear that the notion “transfer” in Article 76 WBP refers to making personal

⁸ As mentioned in the document of the Article 29 Working Party - An integrated EU Approach to On-line Data Protection- adopted on 21 November 2001, WP 37 and its ‘Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based website’, adopted on 30 May 2002, WP 57 .

⁹ Decree of 7 May 2001, specifying personal data processing operations that are exempt from the notification requirement made by Article 27 of the Data Protection Act (WBP Exemptions Decree), Official Bulletin 2001 250.

¹⁰ Explanatory memorandum, Lower House, parliamentary year 1997-1998, 25 892, no. 3, page 193.

data available to a person that is outside the legal jurisdiction of one of the countries of the European Union.

One example of a processing operation that falls under the definition of a transfer is the following.

A globally active multinational decides to make available to all its subsidiaries data on its employees. For this purpose, a database or server is installed in one of the countries in which the multinational is established. All subsidiaries have access to the database and can send, view or download the personal data. In practice, this means that two-way personal data traffic between the database and each of the countries involved takes place. As a result, personal data are geographically moved from the Netherlands to several third countries.

In this context, questions are frequently asked about information placed on a website. Does the fact that information on the Internet can potentially be accessible from all around the world mean that the action of placing personal data on a website should always be considered as a transfer to a third country? This question has been put to the European Court of Justice in Luxembourg by a Swedish judge who applied for preliminary ruling on the so-called Lindqvist case¹¹.

The Dutch government has submitted comments regarding this case, in particular referring to the notion of transfer. It is the view of the Dutch government that the term transfer should be understood to cover an action that is consciously taken in order to transmit personal data from the territory of a Member State to a third country. Making information available through the Internet by means of a website is a form of publication. Different forms or methods of publication or disclosure of personal data may require different methods of protection. Putting names and telephone numbers in a paper telephone directory is something different than putting the same personal data on a CD-ROM or putting them on a publicly accessible website. All these different forms of disclosure of data will bring specific risks with them that have to be dealt with in different ways.

One element that could play a role in this discussion is whether the web page in question is actually addressed to a local public (in the Lindqvist case it was a website in Swedish) or whether the master of the website really intends to address a more international public (for instance by including different language versions of the page and announcing this page through other international websites or publications).

The Lindqvist case is still pending so no definitive answer to this question is available for the time being.

A transfer is a kind of processing as defined in Article 1, letter b WBP. This means that a transfer will only be legitimate if it complies with all the requirements outlined in the Act: having a legal ground for this processing operation (Article 8), processing the data for specified, legitimate and determined purposes (Article 7) in accordance with the law and in a proper and careful manner (Article 6), no further processing the data for a purpose that is incompatible with the original purpose (Article 9) and so on.

A transfer of any kind, to a Member State of the European Union or to a third country, needs to comply with all the relevant requirements of the Act in order to ensure legitimate processing. The rules of chapter 11 WBP additionally apply to transfers to a third country.

¹¹ Case C-101/01, Bodil Lindqvist versus Aklagarkammaren i Jönköping.

1.3. To which kind of transfers do these rules apply?

As it has just been explained, any transfer of personal data (to a Member State or to a third country) has to comply with the general requirements of the WBP for legitimate and lawful processing.

No other requirements need to be fulfilled for transfers of personal data between Member States. As the Directive makes clear in Article 1, paragraph 2, Member States may not restrict nor prohibit the free flow of personal data within the European Union for reasons connected with the protection of the privacy of the individuals.

It follows that if the processing operation is in compliance with the general rules of the WBP, personal data may be freely transferred within the European Union. The rules of chapter 11 WBP do not apply to these situations.

The rules of chapter 11 WBP apply to transfers of personal data to third countries, regardless of whether such a transfer takes place between two controllers or between a controller and a processor. The explanatory memorandum to the Act¹² underlines the fact that the general prohibition on transferring personal data to third countries unless it complies with the rules of chapter 11 is addressed both to controllers and processors. It should however be pointed out that it is inherent to the nature of a processor that he will only be authorised to transfer personal data to a third country if so instructed by the controller; a processor is not allowed to decide on his own about a data transfer. This paper therefore assumes that there will always be a controller deciding about a transfer to a third country.

Like all other rules of the WBP, chapter 11 applies to both the public and the private sector. Companies and public sector organisations have to comply with these rules when transferring personal data to a third country. The different nature of the controller can however have consequences for the evaluation of the specific situation. For instance, some of the exceptions referred to in Article 77, paragraph 1 address public sector situations.

1.4. From what date does the WBP apply?

A royal decree of 5 July 2001¹³ specified that the WBP should come into force on 1 September 2001. This means that all new processing operations effected on or after that date have to comply with all provisions of the Act.

Controllers responsible for processing operations that were already in progress on this date have, according to Article 79, paragraph 1 WBP, one year as absolute deadline to make sure that the processing conforms with the Act.

These rules also apply to transfers to third countries, meaning that those transfers that were already underway on 1 September 2001 should be brought into line with the provisions of the WBP within one year of this date. New transfers will have to comply with chapter 11 of the Act from the very beginning.

¹² Page 193.

¹³ Decree of 5 July 2001, specifying the date on which the Data Protection Act comes into force, Official Bulletin 2001 337.

2. The rules of the WBP on trans-border data flows to third countries: a three-step approach

Articles 76 to 78 WBP contain detailed rules concerning transfers of personal data to third countries. These provisions implement Chapter IV of the Directive into Dutch law. Following the principles defined in the Directive, the WBP puts in place a three-step approach.

1. As a general principle, personal data may only be transferred to countries that provide adequate protection.
2. If the country in question does not offer an adequate level of protection, the transfer can still legally take place if it falls under one of the exceptions enumerated in the Act.
3. If this is not the case, the Minister of Justice can, if so requested by the controller and after having obtained the advice of the Data Protection Authority, issue a permit for the transfer.

These three steps are considered in turn below.

It should be emphasised that the order of these steps is not compulsory for the controller. He can for instance decide to apply for a permit without having analysed the exceptions of the Act or in circumstances where he considers that relying on the existence of adequate protection in a third country (if, for instance, no decision has been made by the European Commission concerning that country) or on one of the exceptions might be too risky.

The Directive gives Member States little room for manoeuvre, not only with regard to the national implementation of its provisions but also regarding the division of competences at international level concerning policy in this field.

In this respect it is important to consider that Article 25, paragraph 6 of the Directive gives the European Commission the power to issue adequacy findings with regard to the level of protection of a third country.

These decisions of the European Commission have direct consequences for the Member States. Article 78 WBP states that, when a decision has been taken at European level, the Minister of Justice will lay down by ministerial ruling or by decision that:

- transfers to a third country are prohibited;
- a third country is considered to guarantee an adequate level of protection, or that
- a permit issued under Article 77(2) is withdrawn or modified.

Furthermore, the same Article 78 of the Act contains an obligation for the Minister to inform the European Commission both of cases in which, in his opinion, a third country does not offer adequate protection and of the permits issued in accordance with Article 77, paragraph 2. As will be explained later, the European Commission and the other Member States are entitled to give their opinion concerning this communication of the Minister.

2.1. Is there adequate protection? (Article 76)

The general principle embodied in Article 76 WBP is that personal data shall only be transferred to a third country if, notwithstanding compliance with the provisions of this Act, that country guarantees an adequate level of protection. This principle is based on the Directive that imposes an obligation on the Member States to guarantee that only transfers to a third country that ensures an adequate level of protection are permitted.

2.1.1. What is adequate protection?

Neither the WBP nor the Directive contains a definition of the notion “adequate level of protection”. However, both legal texts contain a list of the circumstances that should be taken into account when assessing adequacy in a specific case¹⁴. These are the following:

- the nature of the data;
- the purpose and duration of the proposed processing operation/s;
- the country of origin and the country of final destination;
- the rules of law, both general and sectoral, in force in the country in question and
- the professional rules and the security measures which are complied with in that country.

In a letter of 9 March 2000¹⁵, the Minister of Justice informed Parliament of the application of Articles 25 and 26 of the Directive. In his letter, the Minister of Justice refers to the documents issued by the Article 29 Working Party dealing with the interpretation of Articles 25 and 26 of the Directive. These papers were brought together in a consolidated paper of 24 July 1998, document WP 12¹⁶.

The Article 29 Working Party is an independent body in which all European Data Protection Authorities are represented. Its tasks include advising the European Commission concerning data protection matters and examining all questions covering the application of the Directive at national level in order to contribute to its uniform application.

In practice, all Community decisions taken in this field up to now have used the criteria defined in this document as the basis for analysis of the situation in a given country.

The document of the Working Party develops a functional approach to this matter, basing its conclusions not on the nature of the rules that exist in a country, but on the practical results achieved there. It applies the basic principle that data protection rules only contribute to the protection of individuals if they are followed in practice. Therefore, any meaningful analysis of adequate protection must comprise two basic elements: the content of the rules applicable and the means for ensuring their effective application.

Using the Directive as a starting point and bearing in mind the provisions of other international texts, the Working Party defines a “core” of data protection “content” principles and “procedural/enforcement” requirements. The Minister of Justice also used these same criteria in his letter to the Lower House of March 2000 in order to explain how the notion of “adequate protection” should be interpreted.

¹⁴ See Article 76, paragraph 2 WBP and Article 25, paragraph 2 of the Directive.

¹⁵ Letter of the Minister of Justice to the Parliament of 9 March 2000; Tweede Kamer, vergaderjaar 1999-2000, 27 043, nr. 1.

¹⁶ Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. WP 12.

The basic content principles that should be embodied in the existing legal rules are:

- *Purpose limitation principle*: data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer.
- *Data quality and proportionality principle*: data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.
- *Transparency principle*: individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country and other information insofar as this is necessary to ensure fairness.
- *Security principle*: technical and organisational measures should be taken by the data controller that are appropriate to the risks presented by the processing.
- *Rights of access, rectification and opposition*: the data subject should have the right to obtain a copy of all data relating to him/her that are processed and a right to rectification of those data that are shown to be inaccurate. In certain circumstances he/she should be also be able to object to the processing of the data relating to him/her.
- *Restrictions on onwards transfers to non-parties to the contract*: further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (the recipient of the onward transfer) is subject to rules affording an adequate level of protection.

Where specific types of processing are involved the following additional principles should also be considered:

- *Sensitive data*: where sensitive categories of data¹⁷ are involved, additional safeguards should be in place.
- *Right to opt out when data are processed for direct marketing purposes*: when data are transferred for the purpose of direct marketing, the data subject should be able to opt out from having his/her data used for such purposes at any stage.
- *Automated individual decision*: where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the Directive, the individual should have the right to know the logic involved in this decision and other measures should be taken to safeguard the individual's legitimate interest.

These principles should be read and interpreted in the light of the European Directive.

Three criteria are listed in order to assess the effectiveness of the data protection substantive rules:

- *Good level of compliance with the rules*: Some elements such as the level of awareness of controllers and data subjects and the existence of effective and dissuasive sanctions play an important role in order to deliver a good level of compliance with the rules
- *Support and help to individual data subjects*: An individual should be able to enforce his/her rights rapidly and effectively and without prohibitive cost. To do so there should be some sort of institutional mechanism allowing independent investigation of complaints. In Europe this role is played by the independent supervisory authorities such as the CBP but other systems are as well admissible in a third country as far as the support and help to the data subjects is guaranteed.
- *Appropriate redress to the injured parties*: appropriate systems should be in place to provide redress to the injured party where rules are not complied with. This is an essential element that must involve a system of independent adjudication or arbitration, which allows compensation to be paid, and sanctions imposed where appropriate.

¹⁷ For a definition of sensitive data see Article 8 of the Directive and Article 16 WBP.

These content principles and procedural/enforcement requirements should be viewed as a minimum requirement for protection to be considered as adequate in all cases. As it will be seen later, these principles will also play an important role for the evaluation of the existence of “adequate safeguards” in the context of a permit request.

Such a minimum list is however not set in stone. In some cases there will be a need to add to the list while for others it may be even possible to reduce the list of requirements. The degree of risk that the transfer poses to the data subject will be an important factor in determining the precise requirements of a particular case.

The Article 29 Working Party document deals in particular with the way in which the aforementioned approach applies when dealing with industry self-regulation. This is especially important as the Directive and the WBP mention amongst the circumstances to be taken into account in a specific transfer, the existence of professional rules and security measures which are complied with in that country.

The conclusions of this part of the document can be summarised as follows:

- Self-regulation should be evaluated using the criteria outlined above (content principles and procedural/enforcement requirements).
- For a self-regulatory instrument to be considered as valid component in a system of “adequate protection”, it must be binding on all the members to whom personal data are transferred and must provide for adequate safeguards if data are passed to non-members.
- The instrument must be transparent and include the basic content of all core data principles.
- The instrument must have mechanisms that effectively ensure a good level of general compliance. A system of dissuasive and punitive sanctions is one way of achieving that. Mandatory external audits are another.
- The instrument must provide support and help to individual data subjects who are faced with a problem involving the processing of their personal data. An easily accessible, impartial and independent body to hear complaints from the data subject and adjudicate breaches of the code must therefore be in place.
- The instrument must guarantee appropriate redress in cases of non-compliance. A data subject must be able to obtain a remedy for his/her problem and compensation as appropriate.

It can be concluded from the foregoing that the decisive factor is not the nature of the rules containing the basic principles, but the fact that the rules are binding and fulfil the procedural/enforcement requirements.

2.1.2. Who decides on adequacy on a case-by-case basis?

Before an individual transfer takes place, a specific decision will have to be taken as to whether there is an adequate level of protection in the given case. Article 76, paragraph 2 WBP states that a decision has to be made taking into account the individual circumstances of the cases. The explanatory memorandum underlines the fact that the assessment of the adequacy of a specific transfer is in first instance the responsibility of the controller¹⁸. The Minister of Justice confirmed this view when answering questions during the Parliamentary discussion in the Upper House as to whether a company can take a decision by

¹⁸ Page 193 of the explanatory memorandum. The same statement can be found in page 55 of the Guidelines published by the Minister of Justice.

itself concerning the adequate level of protection of a country. In his answer he pointed out that this is something that a company can judge by itself in the first place but that a court can obviously review such a decision subsequently. The Minister also pointed out that in such cases it is advisable to contact the CBP or the Ministry of Justice.

Like the other rules of the Act, Article 76 is a material rule that has to be applied and interpreted on a case-by-case basis. In the context of the WBP, the controller (in Dutch called “the responsible person”) is the responsible party for all the decisions concerning the processing and can also be held liable for loss or harm resulting from non-compliance with the provisions of the Act¹⁹.

One of the main elements that the controller should take into consideration is the existence of a Community decision or a ministerial ruling or decision of the Minister determining the level of protection of the country that he/she intends to transfer the personal data to. If a positive decision of the European Commission exists regarding the third country in question, the controller has legal certainty as to the legitimate character of the transfer insofar as any conditions imposed in the Commission decision are complied with.

Where no decision exists at Community level, the controller will have to consider the specific circumstances of the case (enumerated in Article 76, paragraph 2 WBP), assess the specific risks involved and the specific situation of the country in question, taking into account the criteria and the functional approach explained in section 2.1.1.

This will mean in particular that for a given transfer the controller will not necessarily consider the level of protection of the general legislation of the third country but the specific legally binding rules applying to the transfer in question (that could be for instance sectoral rules). Consideration should also be given to the enforcement/procedural mechanisms and to the existence of public independent bodies or institutions in charge of ensuring the compliance with these rules, the support and assistance to data subjects and their right to redress where necessary.

Where the controller has to take specific steps in order to guarantee the protection of the personal data in the specific situation, for instance by signing a contract with the receiving party in the third country, adequate protection cannot be said to exist. In such a case, the controller is taking steps to adduce adequate safeguards that could be the basis for the granting of a permit by the Minister of Justice²⁰

The explanatory memorandum²¹ to the Act clarifies that in case of doubt the CBP can provide further information to the controller. The controller can also consult other sources of information containing information about the data protection legislation all around the world²².

The policy of the CBP concerning this kind of case will mainly be focused on the provision of general information. The evaluation of the actual level of protection in a specific case will in principle have to be carried out by the controller, the one legally bearing the responsibility for such a decision. The CBP will only enter into the evaluation of specific cases if there is a sufficient interest justifying such an evaluation; for instance, if there is great risk involved in the transfer, an important interest at stake or if complaints have been filed by concerned data subjects.

¹⁹ See Article 49 WBP, paragraph 3.

²⁰ For more information on this issue, see section 2.3 of this paper.

²¹ Page 193.

²² Such as the websites of the European Union or the Council of Europe and the reports published by organisations such as EPIC or Privacy Laws and Business.

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 WBP. These mechanisms will be explained in detail in sections 2.2. and 2.3.

2.1.3. When and how does the European Commission make an adequacy finding?

Article 25, paragraph 6 of the Directive gives the European Commission the power to issue an adequacy finding. In order to do that, the Commission has to follow a specific procedure defined in Article 31 of the Directive and can come to a positive decision by reason of the domestic law of that country or of the international commitments this country has entered into.

This last possibility is especially interesting as it does not only refer to the existence of international conventions, treaties or other instruments of public international law but also to specific international arrangements put in place upon the conclusion of the negotiations that the Commission might enter into with a view to remedying the situation resulting from a negative finding²³.

In recent years, the Commission has in practice tended to choose to enter into negotiations without having taken a formal negative decision on adequacy, even though it is clear that the circumstances are such that such a decision could be taken. The safe harbour case, to which attention will be paid later on in this paper, is a prime example of this approach. This example shows that the Commission will try to avoid taking negative decisions because of the political consequences they might have.

The procedure for the Commission's decision involves the participation of the Article 29 Working Party, composed of the national data protection authorities, and the Article 31 Committee, composed of representatives of the Member States. Customarily, the Article 29 Working Party first gives an opinion, and then its view is taken into account by the Article 31 Committee when voting about the measures proposed by the Commission. The Commission will bear in mind the opinions delivered by both groups but can actually decide to take a different view in its final decision.

Article 31 of the Directive offers an additional guarantee in such cases. If the Commission decides to adopt measures that are not in accordance with the opinion given by the Article 31 Committee, this should be communicated to the Council. The Council may if it wishes, acting on the basis of qualified majority voting, take a different decision.

The European Parliament also plays a role in the procedure because it has the power to check that the Commission has not exceeded its powers and has acted according to the existing procedural rules.

According to the Directive, a decision of the Commission can be positive or negative. However, due to the political consequences of such a decision, it is expected that the Commission will be reluctant to make negative findings. Up to now the decisions taken by the Commission have all been positive.

The scope of a decision can vary: it can cover for instance the whole of a country (as it is the case in the decisions concerning Switzerland and Hungary), a group of controllers adhering to a specific system (as it is the case in the safe harbour decision) or those covered by a specific

²³ See Article 25, clauses 4, 5 and 6, of the Directive.

piece of legislation (as it is the case for Canada). In other words, a decision of the Commission can have consequences for the whole of a country or a specific sector or collective within that country.

The last paragraph of Article 25, paragraph 6 of the Directive states that the Member States shall take the measures necessary to comply with the Commission's decisions. This means in particular that the Member States will have to eliminate all existing obstacles that could arise from existing national legislation or other legal instruments that could stand in the way of the free flow of personal data with the country in question²⁴. The Commission's decisions have immediate effect²⁵.

Article 78, paragraph 2 WBP declares that a decision taken by the European Commission or the Council will be laid down at national level by a ministerial ruling or by a decision of the Minister of Justice. The purpose of these measures is to give adequate publicity to the Community decisions at national level and in this way to provide legal certainty. In order to contribute to the awareness of the general public concerning the existing Commission decisions, these will also be available via the website of the Dutch Data Protection Authority (CBP)²⁶. Up to now only four Commission decisions have been taken, concerning Switzerland, Hungary, the American safe harbour system²⁷ and the level of protection provided by the Canadian Personal Information Protection and Electronic Documents Act²⁸. Attention will be paid to the safe harbour system in section 3 of this paper.

A general decision concerning the level of protection in a given country at general or sectoral level can only be taken at Community level. When such a decision is taken it is legally binding on the Member States and on all controllers within the EU.

It can however be deduced from the explanations given that taking an adequacy decision is a complicated and time-consuming process involving several parties and making necessary a previous and thorough analysis of the legal framework and specific situation in a country. The decision is even more complicated and time-consuming if it involves negotiations with the third country in order to agree on a specific arrangement, as was the case with the United States. It can therefore not be expected that decisions concerning all countries of the world will be taken in the short run²⁹.

This fact means in practice that for the time being it can certainly not be concluded that the lack of a positive decision of the Commission means that the level of protection in a given country is not adequate³⁰.

²⁴ As stated in the letter from the Minister of Justice to the Lower House of 9 March 2000 concerning the application of Articles 25 and 26 of the European Directive, page 4. Proceedings of the Lower House, parliamentary year 1999-2000, 27 043, no. 1.

²⁵ See Article 31, paragraph 2 of the Directive.

²⁶ www.cbpre.nl

²⁷ Decisions of 26 July 2000, published in the Official Journal of the European Communities L215, 25 August 2000.

²⁸ Decision of 20 December 2001, published in the Official Journal of the European Communities L 2, 4 January 2002.

²⁹ This statement is supported by the text of recital 4 of the Commission decision of June 2001 on contractual clauses for controller-to-controller transfer: *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.*

³⁰ As also stated in the letter of the Minister to the Lower House of 9 March 2000, page 7.

2.1.4. Conclusion

For each specific transfer, a controller will have to assess the level of protection in the given case on the basis of an existing Commission decision or, in the absence of such a decision, on the basis of the circumstances of the case.

Such an assessment will have to take into account the criteria outlined in section 2.1.1.

- If the answer to question 1 *Is there adequate protection?* is ‘Yes’: the transfer can take place. Compliance with all other provisions of the WBP should be ensured.
- If the answer to question 1 *Is there adequate protection?* is ‘No’: the transfer is not permitted under Article 76 WBP. Go to sections 2.2 and 2.3 to see whether a solution can be found under Article 77 WBP

The Minister of Justice stated in his letter to the Lower House of March 2000³¹ that, where the CBP, after having investigated a case, comes to the conclusion that the level of protection concerning a given transfer to a third country is not adequate, the Minister should be informed of this fact. The legislator decided that, considering the impact and political implications involved, it was desirable to give the final responsibility to the Minister who can decide about the necessary measures to be taken and inform the European Commission accordingly.

³¹ Page 15 of the letter.

2.2. Is it possible to make use of one of the exceptions of Article 77.1?

Article 77, paragraph 1 WBP is the national implementation of Article 26 of the Directive. The main idea behind this Article is that, even in situations where there is no adequate level of protection that would allow a transfer under Article 76 WBP, transfer can still legally take place if it is possible to make use of one of the exceptions exhaustively enumerated in this Article.

This Article contains a list of alternative criteria. If the conditions imposed by one of the exceptions mentioned in this Article are met, the transfer to that country can take place. It is self-evident that in such cases all the other requirements/obligations of the WBP that would apply inside the EU need to be complied with as well³².

As the Minister of Justice pointed out in his letter to the Lower House of March 2000, the list of exceptions in Article 77, paragraph 11 should be interpreted in a restrictive and strict way³³. A key element for this interpretation is the word “necessary” that appears in the wording of most of the exceptions.

In the following paragraphs, each exception will be dealt with individually and some guidance will be given as to its interpretation. This guidance will include all elements of interpretation given in the explanatory memorandum of the Act, the Guidelines published by the Minister of Justice and the document of the Article 29 Working Party (WP 12) mentioned in the previous section.

2.2.1. Unambiguous consent of the data subject

The first exception refers to the case where the data subject has given his/her unambiguous consent to the data transfer. The following elements should be taken into consideration for the correct interpretation of this exception:

- Consent, as defined in Article 1, paragraph i WBP, is any freely given, specific and informed indication of wishes by which the data subject signifies his agreement to personal data relating to him being transferred.
- The consent should specifically be given for the transfer, not for the processing in general.
- The requirement for information is especially important as it means in this case that the data subject should be aware or made aware of the particular risks of the transfer and of the level of protection in the country to which his/her data are to be transferred. The consent will only be valid if the data subject has been sufficiently informed. If the relevant information is not provided, this exception will not apply.
- It is not sufficient if the data subject has been informed about the intended transfer and has not objected to the transfer (opt-out construction). This is not a clear indication of the wishes of the data subject.
- Because the consent must be unambiguous, any doubt about the fact that the consent has been given would also render the exception inapplicable.

This exception will be especially useful in the situations where there is direct contact between the controller and the data subject since under such circumstances it will be easy for the controller to provide the necessary information and to obtain unambiguous consent.

This exception will be more difficult to apply when the transfer envisaged would cover data concerning numerous data subjects. In such a case, the information has to be given in a

³² See explanatory memorandum to the WBP, page 194.

³³ Page 5 of the letter.

complete and appropriate way to all the data subjects and the consent has to be obtained from all of them in order to enable the transfer.

In addition to the fact that this whole operation can be time-consuming and might involve considerable expense (for instance if the data subjects are at different locations), the use of consent for this kind of case is impractical for various other reasons:

- What does the controller do if some of the data subjects give their consent and others do not? As consent should be freely given, it should be made clear to the data subjects that they are free to say “Yes” or “No” to the envisaged transfer without facing any negative consequences. This is especially important in the employment context, where data subjects may feel “obliged” to say “Yes” to an envisaged transfer proposed by the employer if they do not know what the consequences of saying “No” might be.
- What does the controller do if some of the data subjects decide to withdraw their consent at a later stage? It should be borne in mind that data subjects (or where applicable their legal representatives) are free to withdraw their consent at any time³⁴. The decision to withdraw consent does not have retroactive effect but the processing of the data concerning that data subject will have to be terminated from that moment on.

For all the above-mentioned reasons, it is not advisable to use this exception where numerous/several data subjects are involved and the intended transfer is only useful if it covers the data on all the data subjects. For instance, when an employer in Europe decides to put all the workers’ data in a database outside the EU and requires all the workers to sign a consent form.

It should also be mentioned that the Working Party has dealt with the use of consent in the context of employment in a document of September 2001³⁵. It is the opinion of the Working Party that reliance on consent in this field should be confined to cases where the worker has a genuinely free choice and is subsequently able to withdraw the consent without detriment. Even where consent is relied on, it must be valid and the employer must still satisfy the other requirements of the Directive including Article 6 and Article 15, which addresses automatic decisions. Furthermore, the worker must have information on the processing as required by Articles 10 and 11.

In particular, in the section of the paper dealing with transfer of workers' data to third countries, the Working Party states that it is preferable to rely on adequate protection in the country of destination rather than relying on the derogations listed in Article 26, for example the worker's consent. Where consent is relied on, it must be unambiguous and freely given. Employers would be ill advised to rely solely on consent other than in cases where, if consent is subsequently withdrawn, this will not cause problems.

2.2.2. Transfer necessary for the performance of a contract or for pre-contractual measures

The second exception refers to the circumstances where the transfer of data to a third country is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject’s request. The following elements should be taken into consideration for the correct interpretation of this exception:

³⁴ As stated in Article 5, paragraph 2 WBP.

³⁵ Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, 5062/01/EN/Final, WP 48.

- The transfer in question should be necessary. In other words, this exception does not apply if a transfer would be useful or facilitate the performance of the contract, but is not really necessary as there is a way in which performance of the contract could also be guaranteed while keeping the data within the EU.
- It refers to a contract to which the data subject is a party or to pre-contractual measures requested by the data subject.
- The exception is strictly limited to the data necessary for the given purpose. If additional non-essential data are transferred or if the purpose of the transfer is not the performance of the contract but rather some other purposes (follow-up marketing for example) the exception does not apply.

A typical example of a case falling under this exception is the case in which the data subject enters into a contract with a travel agency to book him/her a trip to a third country. In that case, it will be necessary for the performance of the contract to send data concerning the data subject to the airline company and hotels in the third country in order to obtain the tickets and make the hotel reservations.

Another example mentioned in the explanatory memorandum is the case where a payment takes place for the performance of a contract and it is not possible to know in advance through which countries this bank payment will be routed. The data subject is the one that asks the bank to arrange the payment for him/her and his/her data are necessary for this purpose.

A case of pre-contractual measures initiated by the data subject would be for instance when he/she requested information about a particular service in order to be able to decide whether he/she wants to enter into a contractual relation with this company in the third country or not. This exception will not apply if the data have been transferred in response to direct marketing approaches made by the controller.

2.2.3 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

The third exception refers to the case where the transfer of data to a third country is necessary for the conclusion or performance of a contract between the controller and a third party in the interest of the data subject. The following elements should be taken into consideration for the correct interpretation of this exception:

- This exception refers to a contract to which the data subject is not a party but that has been concluded in his/her interest. The purpose of the contract should be to do something in the interest of the data subject.
- This exception can never be the legal ground for a transfer of personal data to a third country for direct marketing purposes, because such a transfer does not take place in the interest of the data subject but in the interest of the person who approaches the data subject for DM purposes using the data subject's personal data.
- As in the previous case, the application of this exception is limited by the "necessity test": all the data transferred must be necessary for the performance of the contract.

An example of a transfer falling under this exception could be the case of reinsurance with companies outside the EU. If a data subject enters into an insurance contract with a Dutch insurance company, this company may need, due to the high amount insured in the case, to enter into a reinsurance contract with a third party. It could be necessary to transfer some personal data concerning the data subject to the reinsurance company that might be established outside the EU. In this case, the exception would apply as it refers to a contract between the insurance company in the Netherlands and the reinsurance company outside the

EU that is concluded in the interest of the data subject (as an extra guarantee to his/her insurance), who is a third party to the contract.

Another example is a situation in which the data subject is the recipient of an international bank payment. In that case, it would be necessary to transfer the data on the data subject to a third country in order to perform the transaction in the context of a contract to which the data subject is not a party but that is concluded in his/her interest. The contract is actually concluded between the transferring controller and the bank.

2.2.4. Transfer necessary on important public interest grounds or for the establishment, exercise or defence in law of any right

The fourth exception covers two kinds of situation:

1. The case in which a transfer is necessary on important public grounds. Here the transfer does not take place in the interest of the data subject but because an important public interest is at stake. This exception might cover certain limited transfers between public administrations although care must be taken not to interpret this provision too widely. A simple public interest justification for a transfer is not sufficient, it must be a question of *important* public interest. Recital 58 of the Directive suggests that data transfers between tax or customs administrations or between services responsible for social security will generally be covered. Transfers between supervisory bodies in the financial services sector may also benefit from this exception.
2. The case in which the data need to be transferred for the establishment, exercise or defence in law of any right. This could be for instance the case where the personal data have to be transferred to a credit-reporting agency outside the EU before a judicial procedure. This exception concerns transfers taking place in the context of international litigation or legal proceedings, especially transfers that are necessary for the establishment, exercise or defence of legal claims.

2.2.5. Transfer necessary for the protection of the vital interest of the data subject

This fifth exception covers transfers necessary in order to protect the vital interests of the data subject. It should be borne in mind that recital 31 of the Directive interprets the notion of “vital interest” narrowly as an interest “which is essential for the data subject’s life”. This will normally exclude financial, property or family interests. Here again, the necessity test should be applied.

An obvious example of this transfer would be the urgent transfer of medical records to a third country where a tourist that had previously received medical attention in the EU has suffered an accident or has become dangerously ill. In these cases, given the urgency of the situation and the condition of the patient, it would be impossible to obtain the consent of the data subject.

2.2.6. Transfer from a public register or a register that can be generally consulted

The last exception refers to the case where the transfer is made from a public register set up by law or from a register that is open to consultation either by the general public 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.

The intention of this exception is that where a register is available for public consultation or by persons demonstrating a legitimate interest, then the fact that the person who has the right to consult is actually situated in a third country, and the act of consultation in fact involves a data transfer, should not prevent the information from being transmitted to that person.

Recital 58 of the Directive makes clear that it should not be permitted to transfer the entire register or entire categories of data from a register under this exception. Given these restrictions this exception should not be considered to be a general exception for the transfer of public register data. For instance, it is clear that mass transfers of public register data for commercial purposes or the trawling of publicly available data for the purpose of profiling specific individuals should not benefit from the exception.

The wording of this exception in the Directive refers to “a register intended to provide information to the general public”. In this sense, it applies to registers such as the register of traffic car plates or the commercial register of companies.

2.2.7. Conclusion

- If the answer to question 2 *Is it possible to make use of one of the exceptions of Article 77.1?* is “Yes”: the transfer can take place. Compliance with all other provisions of the WBP should be ensured.
- If the answer to question 2 *Is it possible to make use of one of the exceptions of Article 77.1?* is “No”: the transfer is not permitted under Article 77, paragraph 1 WBP. Go to section 2.3 to see if a solution can be found under Article 77, paragraph 2 WBP.

The Minister of Justice stated in his letter to the Lower House of March 2000 that in the cases where none of the grounds is applicable, the transfer is unlawful. The CBP can, where necessary in order to stop such a transfer, use administrative measures of constraint³⁶.

³⁶ Page 15 of the letter.

2.3. Is it possible to obtain a permit for the data transfer from the Minister of Justice (Article 77.2)?

Article 77, paragraph 2 WBP states that the Minister of Justice, after consulting the Dutch Data Protection Authority (CBP), may issue a permit for a personal data transfer or category of transfers to a non-Member State that does not ensure an adequate level of protection. If considered necessary to protect the individual privacy and fundamental rights and freedoms of persons and to guarantee implementation of the associated rights, detailed requirements can be attached to this permit.

This article implements Article 26, paragraph 2 of the Directive into Dutch law. This provision deals with the situation where a controller wants to transfer data to a third country that does not ensure an adequate level of protection and it is not possible or desirable to make use of any of the exceptions explained in the previous section. In this case, the Member State may authorise such a transfer if the controller adduces adequate safeguards with regard to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. These safeguards may in particular result from appropriate contractual clauses.

It is compulsory for the Minister of Justice to ask the opinion of the CBP before issuing a permit. According to the text of the explanatory memorandum to the WBP³⁷, the advice of the CBP will play an important role in this context and will contribute to the quality of the decisions concerning permits due to its expertise and experience in this field.

A controller does not need to obtain a permit for each individual transfer. It is possible to request a permit for a category of transfers, in other words, a well-defined set of transfers having common elements and in which the same circumstances play a role. A permit can only be given on the basis of the specific and well-defined circumstances and safeguards foreseen to address the specific risks at stake and where the scope of the permit can be determined at all times.

Having a permit from the Minister of Justice authorising a specific transfer or set of transfers will offer a high degree of legal security to a controller wishing to transfer personal data to a third country.

2.3.1. What are “adequate safeguards”?

The text of Article 77 WBP does not specify what kind of measures a controller can adduce in order to obtain a permit from the Minister. However, the explanatory memorandum³⁸ to this Article contains a sentence that, when referring to the special requirements that can be attached, contains language similar to the Directive: the rules attached to the permit can be related to the contractual provisions that the controller has included in a contract with the person to whom the personal data are transferred.

Article 26 of the Directive determines that the adequate safeguards to be adduced by the controller in the cases where personal data are to be sent to a third country which does not ensure an adequate protection, may result in particular from appropriate contractual clauses. Recital 59 of the Directive does not use the term "contractual clauses" but refers to "particular measures which might be taken to compensate for the lack of protection in a third country".

³⁷ Page 195.

³⁸ Page 195.

The Directive gives in Article 26, paragraph 4 the power to the Commission, acting in accordance with the procedure laid down in Article 31, to decide that standard contractual clauses offer the adequate safeguards envisaged in Article 26, paragraph 2.

In both cases, it is clear that the legislator sees contractual clauses as the most evident way to provide adequate safeguards but does not exclude the possibility that other instruments could be possible.

One could think of several possibilities in which both the exporter and the importer could play different roles or in which other parties could be involved as well (an external auditor or a Data Protection Authority, for instance), with bilateral or unilateral obligations. The performance of the obligations agreed upon in an enforceable instrument would be the basis for the granting of a permit.

From the data protection viewpoint, the nature or denomination of the instrument in question is not relevant as far as the instrument is able in itself, or in combination with contractual arrangements backing it, to produce the desired effect: offer adequate safeguards for the transfer. For example, the global privacy policy of a company would in itself not be sufficient as it is as such not enforceable and can be modified unilaterally by the company. The situation would however be different if some institutional guarantees are added to the policy such as for instance contracts backing the policy, the policy being given adequate publicity or being deposited at the Data Protection Authority and so on. This kind of question will have to be analysed by the Dutch Data Protection Authority on a case-by-case basis bearing in mind the principles set out by the Working Party concerning self-regulation³⁹.

In order to facilitate the reading of this paper we will refer in the following paragraphs to “contractual solutions” with the meaning of any instrument, being contractual clauses or not, that could produce the same legal effects, presented by a controller as a basis for obtaining a permit from the Minister of Justice under Article 77, paragraph 2 WBP.

Any instruments presented by data controllers as a basis for the granting of a permit will be examined by the CBP and the Minister following the criteria defined in the next section of this policy paper.

2.3.2. Requirements for contractual solutions

The main function of contractual solutions in this context is to satisfactorily compensate for the absence of a general level of adequate protection by including the essential elements of protection, which are missing in any particular given situation⁴⁰. The provisions of a contractual solution need to be detailed and properly adapted to the data transfer in question.

The starting point for interpreting the notion of “adequate safeguards” as used in Article 77, paragraph 2 WBP should be the notion of “adequate protection”, already dealt with at length in section 2.1.1 of this paper. As has already been explained, this notion consists of a series of basic data protection principles together with certain conditions necessary to ensure their effectiveness.

The first requirement of the contractual solution is therefore that it must result in the parties to the transfer being obliged to ensure that the full set of basic data protection principles set out

³⁹ See for more information the document of the Working Party of 24 July 1998 or the summary given in section 2.1.1 of this paper.

⁴⁰ Document WP 12 of the Article 29 WP contains a whole chapter (chapter 4) dealing with the role of contractual provisions. This section is inspired by this text.

in section 2.1.1 apply to the processing of the data transferred to the third country. The contractual solution should set out the detailed way in which the recipient of the data transfer (often called the data importer in contractual terms) should apply the principles.

The criteria outlined in section 2.1.1 as to the effectiveness of a data protection system must also apply when judging the effectiveness of a contractual solution. It is a question of finding means which can make up for the absence of supervision and enforcement mechanisms, and which can offer help, support and ultimately redress to the data subject who may not be a party to the contract.

The degree of autonomy that the recipient of the data in a third country has to process the data after the transfer will influence largely the risk inherent to the transfer. In a transfer between a controller in the EU and a processor outside the EU the risks are more limited as the processor can only act on the instructions of the controller and has no freedom to take any decisions concerning the processing and, more importantly, because the law of the country of the controller continues to apply to the processing.

This is the consequence of the way in which the scope of application of the Directive (and subsequently of the WBP) is defined, in both cases in Article 4. The control over the data processed by the processor outside the EU is exercised by an entity established in an EU Member State and the law of the EU country in question will continue to apply to the processing in the third country and therefore the data controller will be liable under that law for any damage caused as a result of an unlawful processing operation⁴¹.

Insofar as the controller transferring the data retains decision-making control over the processing carried out in the third country, the risk will be more limited for the data subject as they will be able to address any claims to a controller within the EU and any requests for redress to a judicial or supervisory authority within the EU.

It is often assumed that the data subject and the controller within the EU will be in the same country and that therefore the data protection law of the country of the data subject will apply to the processing. This will however not always be the case in practice as data within the EU may be centralised under a single controller that is the party that transfers the data to a controller/processor in a third country. In any case the fact that EU data protection legislation applies, guarantees the data subject a harmonised high level of protection and gives him/her the possibility to file any complaints or enquiries with the data protection authority of his/her own country, which will then forward the case to the correspondent authority of the country of the controller. This is due to the obligation imposed on the European data protection authorities to co-operate with each other under Article 28, paragraph 6 of the Directive⁴².

For all the above-mentioned reasons, contractual solutions for a transfer between a controller in the EU and a processor outside the EU will need to be less detailed than in the case of the transfer from a controller to another controller outside the EU⁴³.

In cases involving contractual solutions between a data controller in the EU and a data controller outside the EU, the situation is more complex, as no EU law applies after the transfer has taken place. Other more sophisticated mechanisms need to be put in place to provide the data subject with an appropriate legal remedy. As the data subject will not be a

⁴¹ See Article 23 of the Directive.

⁴² See also Article 61, paragraph 6 WBP.

⁴³ This fact is also underlined in recital 8 of the Commission decision on standard contractual clauses of June 2001: *This Decision does not cover the transfer of personal data by controllers established in the Community to recipients outside of the territory of the Community who act only as processors. Those transfers do not require the same safeguards because the processor acts exclusively on behalf of the controller.*

party to the contract as such it will be essential to include in the contract a third-party beneficiary clause creating certain rights for the data subject under the contract. This system is presently admissible in all legal systems of the EU Member States.

The contractual solution should furthermore include adequate provisions as to the liability and responsibility of the parties to the agreement. In that respect, given the practical and legal difficulties that a data subject has to face when trying to obtain compensation from a party outside the EU, any contractual solution capable of providing adequate safeguards should guarantee that the data subject should be entitled to receive compensation from the party to the controller that is established within the territory of the European Union. This can be achieved by the inclusion of a joint and several liability clause binding the parties to the contract.

An additional difficulty with this kind of transfer is that the data importer is established in a country outside the EU, making any supervision by the controller or any authority in the EU rather complicated. The contractual solutions should address this problem by obliging the importer to co-operate in the cases where the controller or the supervisory authority consider that an investigation or audit at the premises of the data importer is needed.

2.3.3. Can contractual solutions be used in all cases?

Contractual solutions may be appropriate in many situations, but there might be others where it is impossible for a contract to guarantee the necessary adequate safeguards.

This is particularly to be the case in less democratic countries where the powers of State authorities to access information go beyond those permitted by internationally accepted standards of human rights protection. In these cases, including provisions in a contractual solution that would limit the capacity of the controller/processor in the third country to provide this information to the State will not have any legal effect as the existing legal requirements of the country in question will often take precedence over any contract to which the data importer is subject.

Countries where the obligations to disclose information to the State authorities go beyond the needs of a democratic society and the public order reasons set out in Article 13, paragraph 1 of the Directive are simply not safe destinations for transfers based on contractual solutions.

As has already been stated, contractual solutions need to be detailed and adapted to the specific circumstances surrounding the transfer in question. Therefore, a contract will be particularly suited to situations where data transfers are similar and repetitive in nature. The difficulties regarding supervision mean that a contractual solution may be most effective where the parties are large operators already subject to public scrutiny and regulation. Large international networks, such as those used for credit card transactions and airline reservations, demonstrate both of these characteristics and are therefore situations in which contracts could be most useful⁴⁴.

Equally, where the parties to the transfer are affiliates or parts of the same company group, the ability to investigate non-compliance with the contract is likely to be reinforced, given the strong nature of the ties between the recipient in the third country and the Community-based

⁴⁴ In the cases where contractual solutions are needed. As explained in section 2.2, these companies might in some cases and under the circumstances defined in Article 77, paragraph 1 WBP, be able to make use of the exceptions of the Act. Under such circumstances, a contract will not be essential, although such a company is of course free to use a contractual solution if it wishes.

entity. Intra-company transfers are therefore another area where there is a clear potential for effective contractual solutions to be developed.

2.3.4. Use of the model contracts approved by the European Commission

Article 26, paragraph 4 of the Directive gives the European Commission the power to take decisions as to the fact that certain standard contractual clauses offer sufficient safeguards in the sense of Article 26, paragraph 2. For this kind of decision, the same procedure applies as in the case of an adequacy finding concerning a third country, meaning that both the Article 29 Working Party and the Article 31 Committee will be involved in the preparation of such a decision.

In recent years, some internationally recognised organisations such as the ICC (International Chamber of Commerce) and the CBI (Confederation of British Industries) have had contacts with the Article 29 Working Party and the European Commission concerning model contracts prepared by them. These contacts led to several opinions of the Working Party addressed to these organisations, but the Commission did not go as far as actually approving the opinions in question.

Under the circumstances, and as it was considered that the existence of standard clauses would facilitate trans-border data flows considerably, the Commission decided to draft a set of clauses of its own with the help of the expertise of the Article 29 and 31 groups and benefiting from outside comments. This initiative has led to a first Commission decision of June 2001⁴⁵, for transfers between two controllers. A set of contractual clauses for transfers between controllers in the EU and processors in third countries has been approved on the 27th of December of 2001⁴⁶.

The standard contractual clauses approved by the European Commission can be used by a controller falling under the scope of application of the WBP as the basis for obtaining a permit under Article 77, paragraph 2 of this Act. As the Act does not include any provision excepting those using the Commission clauses from the requirement of obtaining a permit, this requirement applies in these cases as well. The Commission decision of June 2001⁴⁷ makes clear that this decision should be without prejudice to national authorisations that Member States might grant in accordance with national provisions implementing Article 26, paragraph 2 of the Directive; in the WBP, Article 77, paragraph 2.

However, the procedure and time limits for obtaining a permit will be greatly simplified as the role of national authorities is limited considerably by the Commission decision. This will be explained in detail in the following paragraphs.

⁴⁵ Official Journal of the European Communities, L 181, 4 July 2001. The website of the European Commission also provides a set of Frequently Asked Questions concerning the use of the standard contractual clauses: http://www.europa.eu.int/comm/internal_market/en/dataprot/news/clauses2faq.htm

⁴⁶ Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, Official Journal of the European Communities, L 6, 10 January 2002.

⁴⁷ Recital 6.

2.3.4.1. Main features of the standard contractual clauses approved by the European Committee

- The Commission decision of June 2001 only applies to transfers of personal data between a controller in the EU and a controller outside the EU. This instrument does not cover transfers to processors⁴⁸.
- The standard contractual clauses relate only to data protection. The data exporter (the controller in the EU) and the data importer (the controller in the third country) are free to include any other clauses on business-related issues such as clauses on mutual assistance in cases of disputes with a data subject or a supervisory authority which they consider as being pertinent for the contract as long as they do not contradict directly or indirectly the standard clauses⁴⁹ or prejudice the fundamental rights or freedoms of the data subjects. In all cases, the standard clauses have to be fully respected if they are to have the legal effect of providing for an adequate safeguard for the transfer of personal data as required by the Directive⁵⁰.
- The standard clauses contain provisions dealing with issues such as the obligations of the exporter and the importer, the third-party beneficiary clause for the data subjects, the joint and several liability of the parties to the contract, co-operation of the parties with the supervisory authorities, mediation and jurisdiction in case of disputes between the parties, termination of the clauses, governing law and the obligation of the parties not to vary the terms of the clauses.
- The details of the transfer, and in particular the categories of personal data and the purposes for which they are transferred should be specified by the parties in appendix 1 to the contract that forms an integral part of the clauses.

2.3.4.2. The role of the Dutch Data Protection Authority in relation to the standard contractual clauses

As explained at the beginning of section 2.3, the roles of the Minister of Justice and of the Data Protection Authority in the context of the granting of permits should be distinguished. The Minister is entitled to take the final decision concerning a permit request taking into account the advice given by the CBP. The Data Protection Authority has an advisory role to the Minister and is at the same time the supervisory authority for the processing operations in question, not only when the decision concerning the permit is taken but also thereafter. In the context of the standard contractual clauses, the advisory role of the CBP in relation to the permit is limited but its powers as supervisory authority concerning all other provisions of the WBP remain unaffected.

A transfer of personal data to a third country is a processing operation in the sense of the WBP, which means that all other requirements of the Act are applicable in addition to the provisions of Part 11.

The contractual clauses of the Commission aim at guaranteeing that when data are transferred to a third country sufficient guarantees are adduced by the controller on the basis of the

⁴⁸ See Article 2 of the Commission Decision.

⁴⁹ See recital 5 of the Commission Decision.

⁵⁰ See FAQ *Can companies implement standard contractual clauses in a wider contract and add specific clauses?* on the Commission's website.

contract. The decision of the Commission⁵¹ has the effect of requiring Member States not to refuse to recognise the contractual clauses described in the decision when used in accordance with the text of the decision as providing adequate safeguards. The power of the national supervisory authorities to assess compliance with all other provisions of the national law, in this case the WBP, remains unaffected by this decision.

When controllers use the contractual clauses of the Commission, the CBP and/or the Minister will be free to raise any issues that might affect compliance with the rest of the provisions of the WBP regarding the processing operations. These issues might in particular arise from the information filled in by the contracting parties in the appendix 1 to the contract, which forms an integral part of the contract and whose completion by the parties is compulsory.

This has been clearly stated in the text of recital 7 of the Commission decision of June 2001 that reads as follows: *The scope of this Decision is limited as establishing that the clauses in the Annex might be used by a controller established in the Community in order to adduce sufficient safeguards within the meaning of Article 26 (2) of the Directive 95/46/EC. The transfer of personal data to third countries is a processing operation in a Member State, the lawfulness of which is subject to national law. The Data Protection Supervisory Authorities of the Member States, in the exercise of their functions and powers under Article 28 of Directive 95/46/EC, should remain competent to assess whether the Data Exporter has complied with the national legislation implementing the provisions of Directive 95/46/EC and, in particular, any specific rules as regards the obligation of providing information under the Directive.*⁵²

This recital underlines the fact that the data protection authorities might in particular check whether the controller has sufficiently informed the data subject concerning the data transfer to a third country without adequate protection that is about to take place.

As indicated earlier, the parties to the contract might wish to introduce additional clauses to the standard contractual clauses. This will only be possible if these clauses do not contradict directly or indirectly the standard clauses or prejudice the fundamental rights or freedoms of the data subjects. When assessing a request for a permit, the CBP and/or the Minister will have to determine whether the introduction of additional clauses respects these requirements. It should be emphasised that the clauses only have the legal effect given to them by the Commission decision if they are fully respected. In cases where additions to the contract affect the content of the clauses, the CBP will evaluate in its advice the consequences of these additions and advise the Minister accordingly.

In some cases, the parties might also wish to amend or modify the text of some clauses included in the Commission decision. The Commission clauses for transfers between two controllers contain a provision in clause 11 obliging the parties not to vary or amend the text of the clauses.

Amendments to the clauses will therefore have implications for the legal effect of the clauses. The parties could, however, choose the option of modifying and amending the clauses in order to adapt them to the specific situation of the transfer and present these “new” clauses as the basis for an application for a permit to the Minister. In these cases, the CBP will examine the clauses without being bound by the effects of the Commission decision. However, if the clauses respect the requirements explained in section 2.3.2, the CBP may come to the conclusion that the clauses offer sufficient protection and advise the Minister accordingly.

⁵¹ Recital 6 of the Commission Decision of June 2001, recital 5 of the Commission Decision of December 2001.

⁵² See also recital 6 of the Commission Decision of June 2001.

Article 4 of the Commission decision of June 2001 also gives the data protection authorities intervention powers to prohibit or suspend data flows to third countries in order to protect individuals in connection with the processing of their personal data in cases where:

- it is established that the law to which the data importer is subject obliges him/her to derogate from the relevant data protection rules beyond the restrictions necessary in a democratic society as provided for in Article 13 of the Directive where those derogations are likely to have a substantial adverse effect on the guarantees provided by the standard contractual clauses, or
- a competent authority has established that the data importer has not respected the contractual clauses, or
- there is a substantial likelihood that the standard contractual clauses in the annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.

It is expected that this safeguard clause will be very rarely used as it caters for exceptional cases only. As provided for in Article 3 (3) of this Decision, the European Commission will be informed of any use made by the Member States of this safeguard clause and will forward the information received to other Member States. The Commission may take appropriate measures in accordance with the procedure laid down in Article 31 (2) of the Directive.

2.3.5. Procedure for the granting of a permit

In order to make the procedure for granting a permit more user-friendly and speedy, the application form for a permit should be submitted directly to the CBP, which will deliver its advice and then forward the complete file to the Minister of Justice. For the same reasons, the CBP and the Ministry of Justice have agreed on the main lines contained in this paper and have come to a common understanding of the subject that should enable them to deal with these cases in a coherent and co-ordinated way.

The permit applicant will normally be the controller. The law does not, however, prevent a possible application by a representative of a group of controllers sharing common features, provided that the application in question contains a complete list of the names of the individual controllers involved and that the transfers from the different controllers can be defined as a category of transfers, i.e. a well-defined group of transfers having common elements and in which the same circumstances play a role.

A permit applicant has to fill in a form, a copy of which is appended to this paper. In addition to the form, the applicant should send to the CBP a copy of the instrument that will be used by the parties to adduce adequate safeguards and which will therefore constitute the basis for granting the permit. The parties do not need to send the complete text of any such instrument, but should make sure that all relevant sections or articles of the instrument are included. The applicant bears the responsibility for this selection, as he will have to sign a declaration stating that all relevant documentation for the evaluation of the adequacy of safeguards is sent to the CBP together with this form.

The information given on the form allows the CBP to quickly place applications in different categories. This division will have direct consequences for the degree of evaluation to be given to the application and therefore for the time limits within which the permit should be granted.

The following categories are distinguished:

2.3.5.1. Applicants using the Commission's standard contractual clauses with no additions or modifications

Here the evaluation of the CBP will be limited to determining that the parties have correctly filled in the contract and that nothing in the file indicates that the WBP is not being complied with.

The CBP will also have to check whether the exceptional circumstances described in Article 4 of the Commission decisions on contractual clauses of June 2001 and December 2001 exist in this case and, if so, decide whether action should be taken to prohibit the transfer. This can only occur if the conditions of Article 4 of this decision (as explained in section 2.3.4.2) are complied with.

These cases can therefore be dealt with quickly and are normally sent to the Minister of Justice with the recommendation that a permit should be granted.

2.3.5.2. Applicants using the Commission's standard clauses with certain additions

Here the evaluation made by the CBP will concentrate on the additional clauses and should establish whether the additions directly or indirectly contradict the text of the clauses or prejudice the fundamental rights or freedoms of the data subjects. If this is not the case, the evaluation will be limited to what is outlined under section 2.3.5.1. Should the CBP come to the conclusion that the additions to the clauses are not in line with what is described in the Commission decision, it will inform the permit applicant of this provisional conclusion. The applicant then has the opportunity to reconsider his/her request and to amend the text of the clauses within a period indicated in the letter from the Data Protection Authority. When this additional step is needed, the procedure will inevitably take some extra weeks before the advice is given to the Minister.

2.3.5.3. Applicants using the Commission's standard clauses with amendments or using self-drafted contractual solutions

Here the evaluation made by the CBP will have to be in-depth and will necessarily take more time than in the previous cases. Applicants falling under this category will be informed by the CBP as to how much time will be needed to make a recommendation to the Minister concerning their file.

The evaluation made by the CBP will concentrate on the requirements that should be fulfilled by the contractual solutions outlined in section 2.3.2 of this paper.

The way in which the Commission's clauses are used (without addition or amendments, with additions but no amendments or with amendments) will have a direct influence on the way in which the CBP is to evaluate the clauses and to advise the Minister. Parties are free to draft their own contractual clauses or solutions. In this case, the CBP will evaluate them according to the requirements outlined in section 2.3.2.

2.3.6. What happens after a decision concerning a permit application has been taken?

If the Minister, after taking advice from the CBP, decides to grant a permit to an applicant, he will also have to notify the European Commission⁵³ accordingly. As stated in Article 26,

⁵³ Article 78, paragraph 1, letter b WBP.

clause 3, of the Directive, all other Member States will also have to be informed about the permits granted. This Article also specifies that if a Member State or the Commission objects on justified grounds involving the protection of the privacy of the individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 and the Member States will have to take the necessary measures to comply with this decision. This could mean in practice that in these cases the Minister might have to withdraw or modify the conditions of a permit and to communicate this fact to the European Commission⁵⁴.

There might be other reasons that could justify the withdrawal or modification of a permit by the Minister. For instance, as mentioned in the explanatory memorandum to the Act⁵⁵, if the European Commission were to reach a negative adequacy finding regarding the country to which the personal data are transferred⁵⁶. The fact that the European Commission considers that the level of protection in a given country is not adequate, will in principle not have consequences for a decision taken concerning a permit for a transfer to that country as this decision is based on the adequate safeguards demonstrated by a controller to compensate for the lack of adequate protection in a third country. However, the Commission's negative finding could be based on new facts about the situation in the third country that could shed new light on the considerations made in the context of the specific case for which the permit had been granted.

A similar situation could occur in the exceptional cases in which the CBP, on the basis of Article 4 of the Commission decision on contracts, might decide to prohibit or suspend a given data flow to a country. If the Minister decides that the level of protection in a third country is not adequate, he will have to inform the European Commission of this decision.⁵⁷

The situations in which a permit will be withdrawn or suspended are quite exceptional. In general this instrument will offer substantially more legal security than a transfer to a country with no Community adequacy finding on the basis of Article 76, paragraph 2 or Article 77, paragraph 1.

⁵⁴ Article 78, paragraph 2, letter c WBP.

⁵⁵ Page 196.

⁵⁶ Article 78, paragraph 2, letter a WBP affirms that the Minister will lay down by ministerial rule or decision, when this follows from a decision of the Commission or the Council, that transfers to a given country outside the EU are prohibited.

⁵⁷ Article 78, paragraph 1, letter a WBP.

3. A particularly interesting Commission adequacy finding: the Safe Harbour

Up to now the Commission has only taken four decisions concerning the adequacy of a third country: three decisions concerning Switzerland, Hungary and the safe harbour arrangement in the United States of America (26 July 2000⁵⁸). A fourth decision concerns Canada (20 December 2002⁵⁹).

The decisions concerning Switzerland and Hungary have not been very controversial as both countries have comprehensive data protection legislation, have an independent supervisory authority and have both signed, ratified and effectively implemented the Council of Europe Convention⁶⁰.

A much more complicated case is the one of the United States of America. The Directive states in its Article 25 that the European Commission may, after having come to the conclusion that a country does not offer an adequate level of protection, enter into negotiations with that country with a view to remedying the situation.

No official decision has been taken determining that the level of protection in the United States would not be adequate. However, it was a commonly shared view that the existing legal framework in America, composed of sectoral legislation and self-regulation schemes, was in itself not sufficient.

Technically speaking, no real negotiations have taken place between the European Commission and the US Department of Commerce regarding the safe harbour arrangement. The European Commission can only undertake international negotiations with a view to concluding an international agreement if it has a mandate from the Council.

In the present case, a dialogue or discussion between the two parties was entered into, in order to exchange views and to come to a common understanding concerning a possible arrangement which would offer sufficient safeguards to those transferring personal data to companies who would join the envisaged scheme.

This dialogue lasted more than two years and both the Article 29 Working Party and the Article 31 Committee have been involved all the way through. After several opinions of the Article 29 Working Party⁶¹ underlying the outstanding issues which needed to be addressed by the American side, the Article 31 Committee took a unanimous positive view during its meeting of May 2000. The official decision of the Commission was taken in July 2000.

The safe harbour arrangement is rather complex, containing a set of seven principles that should be respected by the companies adhering to the system, fifteen Frequently Asked Questions and a whole set of annexes containing different documents.

One of the most interesting facts of this Commission decision is that it only concerns those companies that adhere to the safe harbour; in other words, it is not a decision affecting a whole country or a sector or sectors of one country but a group of companies that voluntarily

⁵⁸ Official Journal of the European Communities, L 215, Volume 43, 25 August 2000.

⁵⁹ Decision of 20 December 2001, published in the Official Journal of the European Communities L 2, 4 January 2002.

⁶⁰ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention opened for signature on 28 January 1981, Council of Europe.

⁶¹ See opinion 4/2000 of 16 May 2000, opinion 3/2000 of 16 March 2000, opinion 7/99 of December 1999, working document of 7 July 1999, opinion 4/99 of 7 June 1999, opinion 2/99 of 3 May 1999 and opinion 1/99 of 26 January 1999.

decide to join the system. Signing up is indeed voluntary: companies will only join if they want to. However, the rules are binding for those who do sign up.

In order to allow controllers in the EU to know when an American company should be considered as having adequate protection in the sense of this decision, the American Department of Commerce maintains a list of organisations that have joined the safe harbour. The list also makes clear if any "harborites" lose their safe harbour status, for example because they have not complied with the rules. The list is publicly available through the website of the Department of Commerce⁶².

As to the enforcement of the arrangement, many companies in the safe harbour will have their compliance checked annually by an independent body, but this is not obligatory. For them, there are rules about how to conduct effective self-verification. Beyond that, enforcement will largely be through alternative dispute resolution mechanisms. Independent private sector bodies will investigate and try to resolve complaints in the first place. If "harborites" fail to comply with the rulings of these bodies, these cases will be notified to the Federal Trade Commission or the Department of Transportation, depending on the sector, which have legal powers to oblige them to comply. Serious cases of non-compliance will result in companies being struck off the Department of Commerce's list.

The European data protection authorities also play an important role as enforcement bodies for organisations in the safe harbour through the so-called safe harbour panel. More information about this panel can be found at:

<http://forum.europa.eu.int/Public/irc/secureida/safeharbor/home>

Recent information concerning the safe harbour and the current list of companies having adhered the system can be found on: http://www.export.gov/safeharbor/

⁶² <http://www.export.gov/safeharbor/>

4. Practical case studies

In this chapter attention is given below to a number of cases that serve to illustrate the way in which Chapter 11 WBP can be applied in practice. The case of iBazar-eBay is an example based on facts.

4.1. A real case: iBazar-eBay

A few months before the WBP came into force, in July 2001, the Dutch Data Protection Authority was asked for advice regarding a controversial case concerning an envisaged transfer of customers' data to the USA⁶³. The advice of the Data Protection Authority was at that time based on the text of the Directive.

4.1.1. Facts of the case

iBazar, a company operating auction websites in different EU countries, had been taken over by the US company eBay. To ensure the transfer of iBazar customers to the eBay system as smoothly as possible, eBay wanted to transfer the customer data from iBazar Netherlands to the United States. eBay proposed that the transfer be made unless the customer opposed it ('opt-out'), but that the data could only be used in the US once the customers had given permission ('opt-in').

The lawyer acting for iBazar proposed in his letter to the Data Protection Authority two additional exceptions that could in his view also serve as grounds for the transfer: the transfer was necessary for the performance of a contract between the data subject and the controller or the transfer was necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party.

4.1.2. Searching for a solution

4.1.2.1. Is there adequate protection?

The decision of the European Commission on the safe harbour system of July 2000 made it clear that the positive adequacy finding was limited to companies joining this system. As eBay had not joined the system, a legal basis for transfer could not be found on the basis of adequate protection.

4.1.2.2. Is it possible to make use of one of the exceptions?

The lawyer acting for the company suggested three possible legal grounds for the transfer.

- The first option for a planned transfer of data is to obtain the unambiguous consent of the data subject. The definition of consent makes clear that it should be a voluntary act of will. This was not the case here, as the company proposed to use an opt-out construction, meaning that those clients who failed to make their views known would be assumed by the company to have agreed to the transfer.

⁶³ More detailed information and the exchange of letters with the company in English and in Dutch can be found at: www.cbpweb.nl

- The second option is that the transfer is necessary for the performance of a contract between the data subject and the controller. In the case under consideration, there was no agreement between the consumer and eBay, and it did not appear that the planned transfer was necessary for the execution of an agreement between the consumer and iBazar.
- The third option concerns an agreement concluded between the controller and a third party in the interest of the data subject. This exception is subject to the strict condition that the agreement should be *concluded* in the interest of the data subject, but this was not the case here, since the takeover of iBazar by eBay was done in the commercial interest of the contractual parties.

4.1.3. Conclusion

When this case was under consideration, the option of applying for a permit was not available, as the WBP had not come into force.

Two possibilities were open to the company:

- eBay could decide to join the safe harbour and in this way guarantee an adequate level of protection.
- A system could be put into place, whereby all clients had to opt in (consent) before the transfer took place. The investigation of the Data Protection Authority showed that such a procedure was used by eBay for the transfer of customer data from iBazar France to the USA⁶⁴.

eBay has accepted the recommendation of the Dutch Data Protection Authority and has put in place an opt-in system for all clients prior to transfer.

4.2. A transfer from a Dutch controller to a processor in India

4.2.1. Facts of the case

A Dutch company with about five thousands clients decides to look for a processor outside the European Union in order to reduce the cost of processing operations involving its customer database. A company with experience in this field is found in India.

4.2.2. Searching for a solution

4.2.2.1. Is there adequate protection?

There is no Commission decision and/or ministerial decision concerning the level of protection in India. After having checked several data protection surveys, the controller comes to the conclusion that neither general nor sectoral data protection legislation is available in this third country.

4.2.2.2. Is it possible to make use of one of the exceptions?

The controller examines the list of exceptions enumerated in Article 76, paragraph 1 WBP. Three of the listed exceptions could potentially play a role in this case:

- Unambiguous consent of the data subjects: It could be possible to ask all clients to give their consent to the transfer to India. This would not be a practical solution, however, as it

⁶⁴ In the procedure used by iBazar France the user had to write out "J'accepte: que mes coordonnées personnelles ainsi que mes informations de facturation soient transférées et traitées aux Etats-Unis" ("I accept that my personal data and billing information may be transferred to and used in the United States").

could be reasonably expensive and time-consuming to go through this procedure for five thousands customers. Furthermore, there is a risk that some of the customers would not agree to the transfer.

- Transfer is necessary for the performance of a contract between the data subjects and the controller: This exception is not applicable in this case as the transfer is not necessary for that purpose. The only reason why this transfer is taking place is to cut costs for the company.
- The transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the controller and third parties in the interest of data subjects: This exception does not apply here as the contract with the processor will not be concluded in the interest of the data subjects but in the interest of the controller.

4.2.2.3. Is it possible to obtain a permit for the data transfer?

Following the obligation outlined in Article 14, paragraph 2 WBP, the controller and the processor should lay down their mutual obligations in a contract. In addition to the points mentioned in Article 14 of the Act, this contract between the parties could include clauses aimed at offering adequate safeguards for the transfer (see sections 2.3.1 and 2.3.2). Such a contract could be used as a basis for a request for a permit.

The European Commission approved model contracts for transfers between controllers and processors on the 27th of December 2001. Parties can therefore choose between using the Commission's model contracts (in which case they will benefit from a speedy and more simplified procedure) and drafting their own contracts.

4.2.3. Conclusion

In the given case, no adequate protection exists in the third country in question. One of the exceptions of the Act, consent, could possibly be used but would not be a very practical solution.

A permit from the Minister of Justice could be obtained on the basis of the contract between the controller and the processor.

4.3. A transfer from a Dutch public-sector institution to a public-sector institution in a third country

4.3.1. Facts of the case

A Dutch public-sector institution is interested in exchanging personal data with another public-sector institution in a third country called X concerning Dutch citizens who have emigrated to that country.

Country X is a democratic developed country with a sound judicial system and appropriate means for the redress of data subjects.

4.3.2. Searching for a solution

4.3.2.1. Is there adequate protection?

For the time being, no Commission decision exists concerning the adequacy in country X. After having consulted the Dutch Data Protection Authority, the Dutch controller hears that a positive decision will be taken by the Commission in the near future. This decision will, however, be directly linked to a piece of legislation only applicable to the private sector in X. The controller discovers that an international Treaty exists between his/her Ministry in the Netherlands and the Ministry in X. The Treaty contains a whole chapter dealing with data

protection, in which the basic content principles and the procedural/enforcement aspects dealt with in section 2.1.1 are satisfactorily regulated.

The controller concludes that there is an adequate level of protection for the transfer in question.

4.4. A transfer from a Dutch company to an international database

4.4.1. Facts of the case

The Dutch controller at a globally active multinational decides to make employee data available to all its subsidiaries. For this purpose, a database is created in Amsterdam. All subsidiaries have access to the database and can send, view or download the personal data. In practice, this means that two-way personal data traffic takes place between the database and each of the countries involved. As a result, personal data are geographically moved from the Netherlands to several third countries.

4.4.2. Searching for a solution

4.4.2.1. Is there adequate protection?

The multinational has subsidiaries all around the world. As far as the countries of the European Union are concerned, there is no problem, nor for the countries for which a Community decision has been taken.

The American subsidiary of the company has decided not to join the safe harbour. Similar problems are faced with all the subsidiaries established in countries with no or very limited data protection rules in place.

This case study would require a detailed evaluation of the level of protection in many countries of the world. It can in any case be concluded that the transfer will concern a good number of countries with no adequate protection.

4.4.2.2. Is it possible to make use of one of the exceptions?

The same situation exists as that described in section 4.1.2.2. Consent could be a legal ground for the transfer, but this would mean that the consent of all employees all around the world would need to be obtained. As the consent form would have to make it clear that an employee is free to agree or disagree to this transfer, there is a considerable risk that some of the employees would not give consent to the transfer or would decide to withdraw consent at a later stage. This situation would jeopardise the usefulness of the database.

As explained in section 4.1.2.2, no other exceptions could offer a legitimate ground for the transfer.

4.4.2.3. Is it possible to obtain a permit for the data transfer?

The controller could envisage a contractual solution binding all the subsidiaries to comply with the principles embodied in the agreement. This contractual solution could be put in place through different instruments that in themselves, or in combination with contractual arrangements backing them, would offer adequate safeguards for the transfer.

The Dutch controller would need to ask for a permit on the basis of the contractual solution chosen.

4.4.3. Conclusion

In a situation in which a transfer of personal data concerning numerous data subjects to various countries around the world is envisaged, the most practical solution would be to choose for contractual solutions that would be the basis for a permit of the Minister.

Where several data protection legislations are applicable to some part of the processing operations, the procedures outlined in the legislation of the different countries will have to be followed. Using the model contracts of the European Commission, if possible in the given situation, would facilitate the procedure in all European countries involved.

4.5. A transfer from a Dutch company to a “less-democratic” third country

4.5.1. Facts of the case

A Dutch company is interested in transferring personal data for processing purposes to a company in a third country called “Banana Republic”, where processing costs are very low. In this country, a military “coup d’Etat” has recently taken place and the political climate is not stable. According to the latest news, the police and the army have taken over the country.

4.5.2. Searching for a solution

4.5.2.1. Is there adequate protection?

The controller verifies that no Community decision has been made concerning “Banana Republic”. This third country has very comprehensive data protection legislation in which all European basic data protection principles have been incorporated. However, the analysis of the enforcement/procedural requirements in the present situation shows however a very unsatisfactory situation. There is therefore no adequate protection presently in the country.

4.5.2.2. Is it possible to make use of one of the exceptions?

The only possible exception the controller can think about in this case is that relating to the consent of the data subject. In addition to the practical problems described in previous section, the controller realises that, in order to obtain the informed consent of the data subject, information should be provided explaining that the data are to be transferred to “Banana Republic”. It is very unlikely that the data subjects will be willing to give their consent under these circumstances.

4.5.2.3. Is it possible to obtain a permit for the data transfer?

The controller could envisage presenting a request for a permit on the basis of the contractual arrangements put in place with the processor in the third country.

The situation in “Banana Republic” would however mean in practice that the processor, even if acting in good will and willing to comply with the contractual arrangements, would probably not be able to do so. Including provisions in a contractual solution that would limit the capacity of the processor in the third country to provide information to the State would not have any legal effect, as the existing legal requirements and factual circumstances of the country in question will take precedence over any contract to which the data importer is subject.

As concluded by the European Data Protection Authorities, countries where the obligations to disclose information to the State authorities go beyond the needs of a democratic society and the public order reasons set out in Article 13, paragraph 1 of the Directive are simply not safe destinations for transfers based on contractual solutions.

4.5.3. Conclusion

Transferring personal data to “Banana Republic” in the present situation would imply an unacceptable risk for the data subjects. If a permit would be applied for, the Data Protection Authority would recommend rejection of the permit application by the Minister.

As mentioned in Article 78 of the Act, he might then decide to notify the Commission of the European Communities of the fact that, in his opinion, this third country does not provide guarantees for an adequate level of protection within the meaning of Article 76, paragraph 1.

4.6. A transfer from a Dutch financial institution to several financial institutions outside the European Union

4.6.1. Facts of the case

A Dutch financial institution would like to exchange personal data with other financial institutions outside the European Union as a part of a programme for the prevention and detection of fraud.

4.6.2. Searching for a solution

4.6.2.1. Is there adequate protection?

The financial institution has subsidiaries all around the world. As far as the countries of the European Union are concerned, there is no problem, nor for the countries for which a Community decision is taken.

The American subsidiary of the company has decided not to or cannot join the safe harbour. Similar problems are faced with all the subsidiaries established in countries with no or very limited data protection rules in place.

This case study would require a detailed evaluation of the level of protection in many countries of the world. It can in any case be concluded that the transfer would concern a good number of countries with no adequate protection.

4.6.2.2. Is it possible to make use of one of the exceptions?

At first sight, one might think that the exception made by Article 77, paragraph 1, letter d (transfer necessary on important public interest grounds or for the establishment, exercise or defence in law of any right) could apply in this case.

However, it is not that easy in practice. The first part of this exception has been interpreted by the Working Party as covering certain limited transfers between public administrations. A simple public interest justification for a transfer is not sufficient; it must be a question of *important* public interest.

The second part of this exception, transfer of data needed for the establishment, exercise or defence in law of any right would not justify general measures taken for the prevention and detection of fraud either, even if as a consequence of the measures taken some fraud cases might be detected and brought before a court.

4.6.2.3. Is it possible to obtain a permit for the data transfer?

The controller could envisage a contractual solution binding all the subsidiaries to comply with the principles embodied in the agreement. This contractual solution could be put in place through different instruments that in themselves, or in combination with contractual arrangements backing them, would offer adequate safeguards for the transfer.

The Dutch controller would need to ask for a permit on the basis of the contractual solution chosen.

4.6.3. Conclusion

In a situation in which a transfer of personal data concerning numerous data subjects to various countries in the world is envisaged, the most practical solution would be to implement contractual solutions that would be the basis for a permit of the Minister.

Where several data protection legislations are applicable to some part of the processing operations, the procedures outlined in the legislation of the different countries would have to be followed. Using the model contracts of the European Commission, if possible in the given situation, would facilitate the procedure in all European countries involved.

Annexes:

- Mandatory form for the use of those applying for a permit.
- Contracts approved by the European Commission for transfers between controllers (Commission decision June 2001):
http://www.europa.eu.int/comm/internal_market/en/dataprot/news/index.htm
- Contracts approved by the European Commission for transfers between controllers and processors (Commission decision December 2001):
http://europa.eu.int/eur-lex/en/dat/2002/l_006/l_00620020110en00520062.pdf
- Commission decisions concerning Switzerland, Hungary and USA, 26 July 2000:
http://www.europa.eu.int/comm/internal_market/en/dataprot/news/index.htm
- Commission decision concerning Canada, 20 December 2001:
http://europa.eu.int/eur-lex/en/dat/2002/l_002/l_00220020104en00130016.pdf

Application form for a permit as defined in Article 77.2 WBP (compulsory use)

This application form should be completed and signed by the data exporter.

To be addressed to the Minister of Justice
P/A College Bescherming Persoonsgegevens, Prins Clauslaan 20, NL 2509 AJ The Hague

Data concerning the parties involved in the transfer

Data exporter

Data exporter is ... (please specify briefly your activities relevant to the transfer) established in country ... (please specify)

Data importer

Data importer is ... (please specify briefly your activities relevant to the transfer) established in country ... (please specify)

Data subjects

The personal data transferred concern the following categories of data subjects (please specify). Where appropriate a distinction should be made according to the different types of data.

Purposes of the transfer

The transfer is necessary for the following purposes (please specify). Where appropriate a distinction should be made according to the different types of data.

Categories of data

The personal data transferred fall within the following categories of data (please specify)

Sensitive data (if appropriate)

The personal data transferred fall within the following categories of sensitive data (please specify)

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients (please specify). Where appropriate a distinction should be made according to the different types of data.

Storage limit

The personal data transferred may be stored for no more than (please indicate). Where appropriate a distinction should be made according to the different types of data.

Contact-person

Please indicate the name and contact-details of a contact-person for the exporter and the importer for further communication with the Data Protection Authority

Basis for the permit

Which instrument has been used by the parties in order to adduce “adequate safeguards” for the intended data transfer? (Please indicate. A copy of the relevant parts of the instrument should be sent together with this form)

Have you made use of the model contracts approved by the European Commission? (please tick one of the boxes)

Yes

No

If your answer to the previous question was positive please answer the following additional questions.

- Please indicate the complete reference of the European Commission model contract you have used

- Have you added any provisions to the existing model contract? Yes No

If so, please indicate which ones

- Have you amended any of the provisions of the standard contract? Yes No

If so, please indicate which ones.

Have you used any other existing contract non-approved by the European Commission such as the ones of ICC, CBI, Council of Europe 1992...? Yes No

If so, please specify which one.

Additional information (*not obligatory*)

Have you, or your affiliates, demanded authorisation in other EU Member States for a similar transfer, on the basis of the same or a similar instrument?

Yes No

If so, please specify in which Member State(s).

Please use this space to indicate any additional information you would like to communicate to the CBP regarding this transfer.

Signature

Data exporter

The exporter hereby declares that all relevant documentation for the evaluation of the adequacy of safeguards is sent to the CBP together with this form.

Name:

Date:

Authorised signature: