The current issue and full text archive of this journal is available at
http://www.emerald-library.com/ft

Implications of the new EU Directive on data protection for multinational corporations

Rita M. Walczuch and Lizette Steeghs
Maastricht University, Maastricht, The Netherlands

Keywords *Data protection, Privacy, European Union, Multinationals*

Abstract *The 1995 EU Directive on data protection legislation (DPL) ensures free flow of data within the EU. However, the transfer to countries without adequate DPL is generally forbidden. The effect of this Directive on the business of MNCs is still unknown but a few authors foresee major problems for MNCs doing business in Europe. On the eve of the implementation of the new EU data protection directive this preliminary study investigated some of the effects the new DPL Directive might have on MNCs doing business in Europe as seen by representatives of European and US MNCs. The study found that especially those companies transferring customer data across national boundaries are most affected by strict DPL. However, the effects mentioned by interviewees were, in contrast with popular literature on this topic, not exclusively negative. Several positive effects of strict privacy guidelines for MNCs could also be identified.*

Introduction

The concept of privacy is a central tenet of the democratic society. Individuals and organizations have long debated and are still debating the definition of privacy, and the potential use and abuse of personal, name-linked data. With the rapid computerization of our society and the impending onset of the information age, the debate about the access to personal information has taken on a hurried urgency (*The Economist*, 1993, 1996, 1999a). Over the last 20 years, governments, primarily European, have taken the lead in legislating on the use of personal data, issuing a variety of guidelines and directives. While there are many contributing factors, the main motivation for data protection legislation (DPL) is the socio-economic component of a society's culture (Walczuch *et al.*, 1995). Since the cultural values vary with countries, no universal guidelines have been established for data protection. At this point the dual nature of this issue should be stressed. On the one hand, it is concerned with the right of privacy of individuals. On the other hand, data protection negatively affects companies in their right to full disclosure and free flow of information.

In the age of expanding multinational corporations (MNCs) supported by global information systems, transborder data flow (TBDF) transfer has become ubiquitous. The lack of clear and internationally well accepted guidelines poses a real challenge to MNCs doing business in countries with strict DPL, for they often have to conform with a multitude of conflicting national DPL. Some

Information Technology & People,
Vol. 14 No. 2, 2001, pp. 142-162.

The authors would like to thank the reviewers of this paper for their valuable comments. The paper has been much improved due to their suggestions.

countries with a high level of DPL even interdict the transfer of protected data to countries with an inadequate level of protection.

In 1995 the European Union (EU) passed a DPL Directive, which had to be implemented by all EU member states by October 1998 (EU, 1995). This Directive ensures the free flow of all data within the EU. However, the transfer to countries without adequate DPL is generally forbidden. The effect of this Directive on the business of MNCs is still unknown but a few authors foresee major problems for MNCs doing business in Europe.

Most of the past research to address this issue has been based on analysis of the existing legislation. This research has lacked empirical rigor. An explaining argument could be the fact that the DPL are only in force for one year. However, data protection has been practiced in a very similar manner for about 20 years in a few of the EU countries. Therefore, this paper attempts to bring research on the issue of data protection one step further. It reports the findings of an exploratory investigation on the effect of the European DPL Directive on MNCs doing business in Europe. The report will first shortly discuss the contents of the EU Directive. Furthermore previous literature on the potential effect of the Directive on MNCs will be summarized and research questions are formulated. The core of this paper consists of the results of a field study on the effect of European DPL on 23 MNCs doing business in Europe and in the USA. A discussion of the implication of DPL for MNCs and policy makers will close the paper.

Background

DPL is a typically European phenomenon. Table I shows all countries, which had adopted or were planning to adopt DPL by 1998. Outside of Europe only a handful of countries have even considered DPL: Australia, Canada, Hong Kong, Israel, New Zealand, Singapore, South Korea and the USA. Many of these countries have a strong European heritage.

In addition, a study of the European Commission reviews six of the above mentioned countries by means of five categories: human resource data, sensitive data in airline reservations, medical/epidemiological data, data in electronic commerce, and subcontracted data procession. The study concludes that the degree of data protection in these countries varies notably (Raab *et al.*, 1998). However, among countries with DPL there exist large differences in the strictness and level of data protection. For example, "privacy rights in the USA are anything but ordered, with some issues protected by federal statute, some covered by individual states, and some left to industry self-regulation" (Kane, 1998a). So far in the USA privacy issues involving customer data have largely been left up to industry self-regulation (Schatz, 1998).

On the other hand, the German DPL can be described as one of the strictest in the world with all aspects regulated and enforced by federal government. A possible explanation for these differences is major cultural differences between national cultures within Europe and worldwide (Walczuch *et al.*, 1995).

Country	Year first DPL in force
US[a]	1974
Sweden[b]	1973
Germany[b]	1977
Denmark[b]	1979
Luxembourg[b]	1979
Austria[b]	1978
France[b]	1978
Norway[c]	1978
Israel[a]	1981
Canada[a]	1983
Iceland[c]	1982
UK[b]	1984
Finland[b]	1988
Ireland[b]	1987
Australia[a]	1989
The Netherlands[b]	1989
Slovenia[c]	1990
Portugal[b]	1991
Czech Republic[c]	1992
Slovakia[c]	1992
Belgium[b]	1992
Hungary[c]	1993
Spain[b]	1993
Switzerland[c]	1993
Hong Kong[a]	Proposed
Greece[b]	Proposed
Italy[b]	Proposed
New Zealand[a]	Proposed
South Korea[a]	Proposed
Singapore[a]	Proposed
Poland[c]	Proposed

Notes: [a] not Europe; [b] EU; [c] Europe

Source: Adopted from Business Europe, 1995a; Franklin, 1996; Walczuch *et al.*, 1995

Table I.
Data protection laws worldwide by mid 1998

Another study about data protection distinguishes four elements that form a basis of DPL in Europe. These elements are (Schwartz and Reidenberg, 1996, pp. 13-17, 1996):

(1) the creation of norms for collecting and processing personal information;

(2) the establishment of an opportunity for affected individuals both to review information collected for themselves and to review the compilers information practices;

(3) the creation of special protection for sensitive data pertaining to ethnic origins, religion, or political affiliation; and

(4) the establishment of enforcement mechanisms and oversight systems to ensure that data protection principles are respected.

While comparing European law with these four elements, more compliance can be found with the first and third element. Also, the public sector complies to a large extent with the private sector (Schwartz and Reidenberg, 1996).

Some major differences between data protection laws worldwide are:

(1) the extent of the protection:
   - for example, does data collected by private and/or public entities fall under the DPL and what type of data is considered confidential?

(2) the definition of a data file:
   - for example, do only computer files or also manual files fall under the DPL?

(3) the definition of a data subject (exclusively human beings or also legal persons, i.e. companies):
   - for example, does DPL apply exclusively to human beings or also to legal persons, i.e. companies?

(4) the level of auditing, monitoring, and punishment exercised.

A concrete comparison shows the following differences between EU and the USA when approaching data protection (along the study of Swire and Litan, 1998).

Americans:

- are more trusting of the private sector and the market (not the government);
- believe in the power of the mass media to check possible abuses in the private sector;
- are inclined to think that technologies can contribute to the solutions of problems created by technologies;
- are fairly inclined to engage in a cost-benefit analysis of regulatory alternatives;
- are more inclined to adopt reactive rather than proactive regulations;
- are more prone to adopt regulations that give consumers information about private sector practices in order to enable them to exercise their market power to shop for firms with good policies.

Europeans:

- tend to think of self-regulation as being equal to no regulation;
- are inclined to overprotect rather than underprotect;
- craft relatively narrow exceptions to broadly applicable rules.

Furthermore, there is a big difference between the two cultures when conceiving the nature of people's interests in data about themselves. In the European Directives, data protection belongs to the "fundamental rights" of

citizens. In contrast to that, Americans favor a free flow of information, which is embodied in the First Amendment (Swire and Litan, 1998).

International efforts to develop harmonized data protection standards

As time progressed and an increasing number of countries passed DPL, tighter restrictions on TBDF across national borders were installed. Many countries with strong data protection interdicted the transfer of protected data to countries with less strong or no DPL. This could severely impede the business of some multinational companies. An example of this occurred in 1989, when the French authorities halted the transfer of personnel records from Fiat's French office to the Italian home office because Italy had at that time no DPL while France had high levels of protection (Mei, 1993).

To simplify the free flow of information between countries, several international attempts have been made to define an international data protection standard. The most important attempts were the OECD guideline, the Council of Europe Convention and the EU Directive related to data protection.

On September 23, 1980 the OECD passed the *Guidelines on the Protection of Privacy and Transborder Data Flow of Personal Data*. Although a great number of countries (all members of the OECD, including the USA) adopted the guidelines it was still felt by experts that the guidelines overstressed the principle of unrestricted TBDF at the expense of the privacy interest of the data subjects (Ellger, 1987). Since the guidelines are not legally binding on any of the member countries, it did not really serve as the international DPL that it was intended to be.

Similarly to the OECD guidelines, the *Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Data* aims at the harmonization of the data protection laws of its members. However, in contrast to the OECD guidelines, the Council of Europe Guidelines must be incorporated into domestic law by countries who have acceded to it. Although the convention has narrowed the range of possible solutions available to member states, it has not succeeded in bringing about full harmonization of already existing laws.

The 1995 EU directive

As early as 1975 the European Parliament passed a resolution demanding a directive on the freedom of individual and data processing in order to guarantee that European citizens enjoy maximum protection (Ellger, 1987). After many debates and some compromise, the EU finally adopted the *Directive on the Protection of Individuals with Regards to the Processing of Personal Data and the Free Movement of such Data* (from now on referred to as the Directive) on October 24, 1995.

As the title clearly states, the main interest of the Directive is again twofold: to protect the individual and at the same time ensure the free movement of personal data. Obviously, this implies that the level of protection must be

harmonized as much as possible across the EU. The final version of the Directive is based mainly on Germany's and France's existing national laws, two of the most restrictive national laws within the EU, thus ensuring the maximum protection for EU citizens.

Although the standards are rather high (the Directive applies to the public as well as to the private sector and demands the inclusion of automated as well as manual files), full harmonization has not been reached. The Directive leaves it up to the individual member states to decide if they want to protect legal persons, i.e. companies, or not. Also, deciding on the level of judicial remedies, i.e. severity of punishment for non-adherence, is left largely up to the member states.

The two main points of the Directive are (EU, 1996):

(1) data may only be collected for specific, explicit, and legitimate purposes; and

(2) data may only be held if they are relevant, accurate, and up to date.

The Directive defines six grounds for the legitimacy of personal data processing:

(1) consent of the data subject;

(2) contract with the data subject;

(3) legal obligation to collect the data;

(4) vital interest of the data subject;

(5) public interest (in the case of a public administrator); and

(6) the legitimate interest in processing data where it is not overridden by the interest of the data subjects;

and grants a number of important rights to data subjects including:

- the right to access data concerning them;
- the right to know where the data originated;
- the right to have inaccurate information rectified;
- a right of redress in the event of unlawful processing;
- the right to withhold permission to use their data in certain circumstances; and
- the right to opt out free of charge from being sent direct marketing material.

Member states had three years to implement the rules laid down in the EU Directive, i.e. new national laws had to be implemented by October 1998. However, even after the new DPL have been passed there will still be some differences between national law within Europe. No matter how the Directive is implemented, the main issues are harmonized and unrestricted flow of data between EU members ensured by law, i.e. no member state can restrict

transborder data flows to another member state as long as the level of protection required by the Directive is provided.

Data transfer to non-EU countries

Article 25 of the Directive treats the data transfer to non-EU countries. Here the Directive states that:

> (m)ember states shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if . . . the third country in question ensures an adequate level of protection (EU, 1995).

The definition of "adequate" is everything but clear today and must be assessed (by the national data protection officials) for each separate case. A close look to the assessment of adequacy in this context can be found in the European Commission report (Raab *et al.*, 1998).

What is clear, however, is that most countries in the world today do not have adequate DPL according to the EU Directive. Since US legislation does not protect personal data collected and processed by private companies the USA is not considered a safe third country by the EU as far as data protection issues are concerned (Amidon, 1992; Mei, 1993). This would mean that under article 25 no transfer of personal data would be allowed to the USA, one of the main trading partners of the EU.

There are however, certain exception to article 25. For one, codes of conduct which are used in some industries, for example bank secrecy, can be used to argue for adequate protection. Also, the Directive states that the transfer of protected data to unsafe third countries will be allowed if:

- the data subject has given consent;
- the transfer is necessary for the performance of a contract between the data subject and the data controller;
- it is necessary for the conclusion of a contract between the data controller and a third party in the interest of the data subject;
- it is of important public interest; and
- it is necessary to protect the vital interest of the data subject.

The level of protection guaranteed by the European Directive on data protection is rather high. The interdiction of TBDF to countries without adequate protection might significantly stifle international data exchange. However, there are certain exceptions to this interdiction. The research study described here tries to investigate if and to what extent MNCs are affected by DPL. The following section will present a short summary of previous literature on this topic and develop the research question and three sub-questions.

Research questions

Several authors have discussed the new EU Directive and its effect on MNCs. Since the new EU Directive on data protection is rather restrictive and has a

clear stance on TBDF, US lawyers and journalists predict severe impediments to free flow of information for US multinationals doing business in Europe because of the lack of DPL for the private sector in the USA (Trubow, 1992; Kane, 1998a). Other potentially negative effects of the EU Directive for MNCs are increased operating costs, disrupted international business transactions, and required adjustments of the organizational structure such as a loss of central control over databases, marketing, personnel and manufacturing (Mei, 1993; Business Europe, 1995b; Cole, 1985; Kane, 1998b). Even the Clinton administration criticized the directive for its "extra-territorial" nature. The implications of the directive are predicted to be significant and no resolution of the issue between the EU and US governments is in sight (Kane, 1998b). None of the authors provide any empirical evidence for their predictions.

However, an empirical study of IS managers of transnational corporations interviewed on the restrictions of data transfer DPL indicated that the variety of DPLs was more of a concern than their rigor (Guynes, 1994). This would imply that MNCs might welcome a harmonization of DPL within Europe and are less concerned about the rigor of the new EU directive.

From this review of the literature it was concluded that an empirical investigation of the real effect of the Directive on MNCs in Europe is needed. Thus, the following research question was formulated.

Research question: How will the EU Directive on data protection affect the business of a MNC in Europe?

Although some authors go as far as calling the Directive a non-tariff barrier to trade (Kobielus, 1992; Mei, 1993), a review of European DPL does not give any indication of unfair treatment of foreign enterprises (Ellger, 1987). Since the Directive was based on European laws, one could argue that the new EU Directive does not qualify as a non-tariff barrier to trade. If the Directive were a non-tariff barrier to trade, non-EU-based MNCs would experience more problems than EU-based MNCs. To investigate this the following sub-question was formulated.

Sub-question 1: Are there differences between the effect of the EU Directive on data protection on EU-based MNCs versus non-EU based MNCs?

Mei expects the greatest impacts of the EU Directive on the US service industry (Mei, 1993). It can be assumed that service MNCs, whose business is largely based on information collection and dissemination, experience more problems than production MNCs who have comparatively little value added from information or data exchange. The main difference thus lies in the type of data processed by these companies and possibly transferred across EU borders. Companies transferring personal (and thus protected) data are more likely to experience difficulties with stricter DPLs. The following sub-question was thus formulated.

Sub-question 2: Are there differences in the effect of the EU Directive on MNCs transferring personal data across national borders versus those not transferring personal data?

As we have discussed earlier the level of protection of personal data offered by the various DPLs worldwide varies widely. Some countries in the EU, for example Germany and France, always have had strict DPL whereas other countries have taken a much less restrictive view on the protection of personal data. From this it follows that some countries have to adapt their data protection laws considerably, whereas in other countries some small adjustments will suffice. It would be conceivable that companies in the countries with traditionally strict DPL have learned to live with these rules and will be less concerned about the new EU directive. The following sub-question was formulated.

Sub-question 3: Are there differences in the effect of the EU directive on companies in EU countries with traditionally strict DPL and other countries?

Methodology

An exploratory field study was performed to obtain a first impression of the effect of DPL on the activities of a MNC doing business in Europe. This paper focuses on two EU countries, Germany and The Netherlands. For Germany no major changes were expected with the implementation of the EU directive, whereas in The Netherlands some significant changes to the existing laws were expected.

To reduce the scope of this first exploration the study was limited to Dutch and German MNCs doing business in The Netherlands and the USA and Germany and the USA respectively. We chose MNCs doing business in the USA because the USA is one of the major trading partners of the EU but its DPL has been deemed to be not adequate to permit free data exchange of protected data. Also, current high-level talks between EU and the USA show that this is considered an important aspect of EU-US relations (*The Economist*, 1999b). Thus, MNCs doing business in the USA and Europe are likely to experience negative effects of the directive if there are any. Germany and The Netherlands were chosen to represent the EU in this study. Only two countries were chosen to control for the formerly major differences between DPL in various EU countries. Germany was chosen for two reasons:

(1) because Germany had and has one of the strictest DPL laws in Europe (and the world) at the moment; and

(2) the EU directive was modeled largely based on the German "Bundesdatenschutzgesetz".

The German data protection officials interviewed for this study indicated that they did not expect any major changes when the German DPL is adjusted to the requirements of the EU directive in 1989 (question 7b in the Appendix). This

supports the choice of Germany for this study to represent EU countries with traditionally very strict DPL.

The Netherlands was chosen to represent the countries where changes to existing DPL are expected. The Netherlands have had DPL since 1989 and now had to implement new DPL containing significant changes. The major changes are:

- the new law uses a much wider definition of protected and sensitive data;
- the information requirement towards the data subject has been enlarged; and
- jurisdiction has been given more options to act against illegal data processing.

MNCs doing business in The Netherlands will thus experience more changes in the way personal data is protected.

To investigate the research questions listed above, an exploratory field study was considered most appropriate since a review of the literature yielded only legal discussions of the possible effects but no empirical evidence. Semi-structured personal interviews were chosen to obtain the most useful information. The interview questions were developed based on the effects of DPL proposed by previous literature (see the Appendix for the interview outline).

The interview was performed with data protection officials (or in one case a close colleague) in the German headquarters of seven German and four US MNCs doing business in Germany and the responsible person for data protection questions of eight Dutch and four US MNCs doing business in The Netherlands. It was rather difficult to find the correct person in the Dutch firms. In some MNCs different people were responsible for different DP issues. For our interview we tried to identify the person that had the most overall knowledge on DP issues. In most cases this person was located in the legal or the personnel department.

Nine of the interviewed companies are active in various sectors of the production industry and 14 in various sectors of the service industry. All companies are significantly active in the German or the Dutch and the US markets and are among the largest in their sector in Germany or The Netherlands. The names of the interviewed companies are kept anonymous. All interviews were carried out in German or in Dutch and most were realized on-site. On request of the participants two interviews were performed via telephone and one in written form. Table II shows the sample by home country and industry.

To analyze the interview data, all interviews were first transcribed and then entered in summarized form into a large matrix, which was then analyzed further. Similarities and differences between EU and US companies, service and production industry companies, and companies doing business in

Germany or The Netherlands were thus visible. In addition, some other patterns became apparent. The following section summarizes the results of this analysis.

Results

Initial analysis showed that no differences between US-based and EU-based companies could be detected. Thus, in the further discussion we will not refer to sub-question 1 any more. In this chapter the results regarding the interview questions will be presented dividing the sample according to the two remaining sub-questions. Each result will be presented by:

- type of data transferred (sub-question 2); and
- country (sub-question 3).

Related to sub-question 2, we will first take a closer look at the type of data actually transferred across national borders by MNCs in our sample.

Type of data

All interviewed companies transfer protected, i.e. personal, data across national borders. However, the specific type of protected data flows that were mentioned by the interview partners could be grouped into three major classifications. The most common data flows are employee data transferred for internal reasons. All companies we interviewed in this study used this data flow when transferring employees or because they make use of a central personnel database, which keeps files on employees working in various countries. In general, companies experience no major problems with these types of data flows since asking the employee's explicit agreement in his work contract or in a special contract can easily legalize them.

The second type of data flow is data concerning other companies. These companies are mostly suppliers and/or customers of the MNC. In general, data of legal persons (i.e. companies) is not protected under the EU DPL. However, often a contact person within the company is included in these data files and their data is protected, even if it is just a name, company telephone number and office number. Thirteen interviewed companies (four in Germany and seven in The Netherlands) mentioned the transfer of this type of data. Again, no major problems are experienced with the transfer of this data.

In contrast to employee data flows and company data flows, the third type of data flows, private customer data flows, pose a much larger and more sensitive issue for the MNCs. Often, customer data includes highly sensitive data such as

Table II.
Sample by home country and industry

	German	US in Germany	The Netherlands	US in The Netherlands
Production	3	2	3	1
Service	4	2	4	2

salary, savings, travel patterns, and buying patterns. This data is very interesting to companies for marketing purposes but also very private for many people.

One specific phrase of the EU directive is the interdiction to use data for anything else than what it was collected for. This also includes that companies are not allowed to enrich data by combining two databases, as is common practice in the USA. Most likely for cultural and historical reasons the issue of the "transparent customer" is very sensitive among some European people (especially the Germans). Three companies in this study mentioned the relatively high level of media attention to DP issues related to the transparent customer or employee. A company whose data protection practices have been criticized openly will quickly lose the trust and respect of its customers.

Thus, for the further more detailed analysis of the interview transcripts, the results are presented pointing to a difference between companies that transfer personal customer data (four out of 11) and those that do not. Sub-question 2 should thus be reformulated as:

> *Sub-question 2 rev.*: Are there differences in the effect of the EU Directive on MNCs transferring personal customer data across national borders versus those not transferring personal data?

Table III shows the sample according to type of data transferred. The numbers in parentheses indicate the nationality and sector of the subgroups. Both US-based and EU-based MNCs belong to the group of MNCs transferring private customer data across national borders.

Incidentally, all companies that transferred private customer data across national borders were service companies but this does not mean that the results can be generalized to all service companies and not to production companies since:

- service companies that do not transfer private customer data do not experience the same problems; and
- one production company is foreseeing more problems in the future because it might start to transfer private customer data across borders.

Thus, although companies that transfer customer data are more likely to be in the service industry, this does not imply that all companies in the service

Table III. Sample according to type of data transferred

Type of personal data	Number of firms (US, German) (service, production)	Number of firms (US, The Netherlands) (service, production)
Employee	All (4US; 7G) (6S; 5P)	All (4 US, 8 NL) (8S, 4P)
Other company	4 (1US; 3G) (2S; 2P)	7 (2 US, 5 NL) (3S, 4 P)
Private customer	4 (1US; 3G) (4S; 0P)	4 (1 US, 3 NL) (4S, 0P)

industry and no companies in the production industry will experience the same problems.

Detailed qualitative analysis of interview transcripts

A more detailed analysis of the interview transcripts was performed comparing the answers of the companies which transfer customer data across national borders (from now on referred to as the Cs), with those of the other companies. The interview results of Dutch and German based firms will also be presented separately.

Resources spent on DP. Two interview questions referred to time and money spent on data protection (see Appendix questions 5a and 5b). For several reasons these were very difficult questions to answer. Only one of the (German) companies had ever formally attempted to assess the cost of data protection and had not come to a satisfactory result. Most others also indicated that their answers were at best educated guesses. Often they were not able to name a sum of money spent on DP but could only provide an indication, e.g. "not much" or "a lot". A careful estimate could be made to assess person-years.

Complicating this issue was that some firms tried to separate their resource expenses into DP issues that would have been accrued even if no DPL existed (e.g. data security, bank secrecy) and extra cost caused by the law. The interviewer tried to focus the interviewees on the additional costs if possible. Thus, for the reasons indicated above, the following numbers are at best very rough estimates and should not be misunderstood as a statistical analysis. However, it was felt that they nevertheless provide an interesting finding since the Cs indicate that they spend considerably more money on DP issues than other companies (see Table IV).

Overall the range of person-years spent on DP issues was very large. Interviewees indicated that between 0.1 (0.5 hour per week) and ten person-years (ten people working full time) were spent on DP each year. Two Dutch interviewees could not provide any indication of the time they spent on DP issues. The data indicates that German MNCs spend more time on DP issues than Dutch MNCs.

As mentioned earlier, it was impossible for most interviewees to provide a precise indication of money spent on DP issues. Table V summarized the answers to this question. Several interviewees were not able to give any indication at all. Again, the Cs seem to also spend more money on DP issues than the rest of the interviewed companies. German Cs seem to spend more resources on DP issues than Dutch Cs whereas no discernible difference

Table IV.
Time spent on DP issues (in person-years)

	Germany		The Netherlands	
	Cs	Other companies	Cs	Other companies
Range	1.5 to 10	0.1 to 2.5	1 to 7	0.2 to 1 No idea (2)
Average	4.6	1.4	3.4	0.6

between German and Dutch MNCs not transferring customer data across borders can be detected.

A third question (see Appendix question 6) related to resources spent on DP issues tried to assess how often MNCs had to deal with DP problems that involved foreign countries. Table VI presents the averages for each group of companies. Apparently, the Cs spend a much greater part of their resources on issues involving foreign countries while the other companies hardly ever have to deal with DP issues involving foreign countries. However, as the range shows there are large differences among C-companies regarding this aspect. The findings are remarkably similar between German and Dutch firms.

Importance of DPL for business and effect on business. When asked about the importance of DPL for their business (question 11 in the Appendix), six of the eight Cs indicated that they perceived DPL as very important to their business. None of the other companies felt that DPL was important to their business. To illustrate this, summarized quotes of the interviewees are presented in Table VII. This clearly shows how differently DPL is perceived by MNCs which transfer private data across national borders. The results indicate that Dutch MNCs that do not transfer customer data actually see DP issues as more important than German firms. This may be a reaction to the (during the interview) current implementation of stricter DPL in The Netherlands. Dutch MNCs need to learn about the new and stricter laws even if they do not transfer sensitive customer data. German MNCs on the other hand do not expect any major changes and are thus more relaxed.

Also, when asked if they perceived a negative effect of DPL on their business (question 7 in the Appendix), five of the Cs answered in the affirmative, while none of the other companies agreed. Two of the German affirmative answers

Germany		The Netherlands	
Cs	Other companies	Cs	Other companies
A lot (1) DM 10 Mio. (1) No idea (2)	App. 2 person-years in wages Not much (4) No idea (2)	3 person-years in salaries (1) 2 person-years in salaries (1) No idea	ca. 2 person-years in salaries (1) ca. 1 person-years in salaries (1) Not much (2) No idea (4)

Table V.
Money spent on DP issues (number of companies)

	Germany		The Netherlands	
	Cs	Other companies	Cs	Other companies
Average	64 Germany 36 foreign	97 Germany 3 foreign	69 The Netherlands 31 foreign	98 The Netherlands 2 foreign
Range	From 5-99 in Germany	From 95-100 in Germany	From 50-95 in The Netherlands	From 95-100 in The Netherlands

Table VI.
Percentage of resources spent on DPL by region (averages)

were both related to lost business because of strict DPL. The three Dutch affirmative answers were related to the expectations of problems related to transborder data flows related to stricter DPL. Thus, companies that transfer private data across national borders seem to be more likely to perceive a negative effect of DPL on their business. The summarized quotes are listed in Table VIII.

Very interesting in this context, were the answers of two interviewees who stated that DPL had a positive effect on their business. They argued that customers were more likely to trust a company if they knew that their private data was well protected. One could use this fact as a marketing argument to attract more customers from other countries where data protection guidelines are not as strict. Incidentally these two interviewees work for MNCs doing business in Germany. However, a few Dutch interviewees also mentioned these side-effects of strict DPL. Thus, no differences in answers between Dutch and German MNCs can be identified.

Question 12 of the interview asked the interviewees if they perceived DPL as a non-tariff barrier to trade. Unanimously, all interviewees indicated that they did not consider DPL as a non-tariff barrier to trade. The general tenor was that if a company establishes a business in a foreign country it must adopt the local laws and regulations. By none of the interviewees were EU companies perceived to be treated any differently than US companies. The initial analysis of the data collected in this study seems to support this assessment since no differences between US and German-based companies could be found. However, some interviewees made some interesting additional comments, which were added here.

Additional comments. Of the Cs a few interviewees had some comments regarding the new DPL. One German interviewee thought that strict DPL

Table VII.
Importance of DPL to business

Germany		The Netherlands	
Cs	Other companies	Cs	Other companies
Important (1) Tortured (1) Plays large role (1) Not important (1)	Not important (7)	Important (3) Not important (1)	Important (3) Plays a role (2) No important (3)

Table VIII.
Perceived effect of DPL on business

Germany		The Netherlands	
Cs	Other companies	Cs	Other companies
Higher profits without DPL (2) Positive (1) Not negative (1)	Positive (1) Not negative (6)	Possible problems with TBDF (3) Not negative (1)	Not negative (8)

"caused difficulties" for the (US) company to set up business in the EU and another German interviewee felt that the "restrictions were too severe".

One interviewee supplied an interesting frame on the question by saying that DPL "might become a minimum requirement" just as quality or environmental standards have in some industries become *de facto* standards. This would exclude or at least hinder companies from countries without adequate data protection from participating in trade with the EU and other countries with high levels of protection.

A Dutch interviewee suggested an even stronger solution by arguing that the EU has chosen the correct path regarding personal data protection and thus demanding that *all* countries worldwide should follow the lead of the EU regarding DPL and adapt their legislation to comply with the EU directive.

When asked how the DPL should be improved to better fit their business needs (question 13), there was surprising agreement between all German interviewees that in general the DPL in Germany is good as it is.

A minor criticism by Dutch and German interviewees was that DPL is sometimes difficult to understand, which is not helped by contradictory commentaries on the law. One interviewee mentioned that the law must be explained to be understood. One interviewee described the German DPL as too formalized and suggested following the example of The Netherlands and Canada who had based their DPL on codes of conduct in place of formalized law. However, codes of conduct would not satisfy the demand of the EU Directive and The Netherlands has changed their laws accordingly. Dutch interviewees were concerned about the bureaucracy associated with the new DPL.

Question 10 asked interviewees if their organizational structure was in any way adjusted as a result of DPL. None of the interviewees indicated that this was the case.

The results have provided evidence for the fact that the EU directive will have an effect on MNCs doing business in the EU. However, the directive is not perceived as non-tariff barrier to trade by EU and US MNCs doing business in Europe and the effects expected are limited to MNCs that are transferring personal customer data across EU borders. Some positive effects have also been stated.

Conclusions

Concluding this paper a short summary of the findings is presented. Afterwards the implications of these findings for MNCs and policy makers are discussed and directions for future research are formulated.

Summary of the findings

This paper presented the results of an exploratory study which investigated the possible effect of the new EU *Directive on the Protection of Individuals with Regards to the Processing of Personal Data and the free Movement of such Data*

(EU, 1995) on MNCs doing business in the EU. A review of the existing literature found a few analyses of the possible effect but none supplied any empirical evidence.

Interviews with data protection specialists in 23 MNCs provided enough qualitative data to formulate findings about the effect of European DPL on MNCs.

Major findings. Summarizing the results of this study are:

- The EU Directive is expected to have the strongest effect on MNCs which transport personal customer data across EU borders.
- The EU Directive will have a slightly stronger effect (compared to the historical situation) on MNCs operating in EU countries with traditionally less strict or even non-existing DPL because the companies have to learn how to handle the stricter laws.
- No differences are expected between EU-based and US-based MNCs doing business in Europe and the Directive is not perceived as a non-tariff barrier to trade.

Implications for managers of MNCs

Managers of MNCs which are doing business in Europe and are transferring private data to non-EU countries, can expect more problems with the new EU Directive implemented. The most drastic changes can be expected in countries where the current DPL is very different from the EU Directive. Specifically MNCs in countries like Belgium, Italy, Spain, Portugal and Greece will have to deal with major changes in DPL since these countries have only recently started to work on DPL. On the positive side, data exchange between EU states will be simplified.

Some US companies have already implemented the EU directives when dealing with European data. This can rather easily be done on a contractual basis in which the company agrees to adhere to EU directive guidelines. An initiative of the US government and the EU are the "Safe harbor" principles which have just recently been finalized. "Safe harbor" refers to a model contract, with which non-EU companies can show their compliance with the EU directives (ITA, 1999). However, according to the EU, these contracts should be the exception rather than the rule, which may complicate matters especially for non-EU companies with a large stake in the European market (Kane, 1998c). Another approach to the issue was taken by Microsoft, which has established a server farm in the EU to ensure operation without any data transfer to the USA (Kane, 1998b).

Companies that do not transfer private customer data across EU-borders or companies that transfer data only within the EU will not experience a significant effect of the new DPL. However, an increase in bureaucratic effort may be expected for all companies dealing with protected data.

Implications for policy makers

Implications of this study for policy makers must be separated into implications for EU policy makers and implications for non-EU policy makers. With the advent of globalization and stricter DPL, many EU policy makers can expect an increase in requests for personal data transfers to countries with inadequate protection, which almost all non-EU countries are. It can be expected that the governments of both countries will be included in the negotiations regarding data protection requirement in the foreign country. Possibly standard procedures should be developed to deal with these cases to simplify the process for all involved parties.

Policy makers of non-EU states should evaluate their own DPL in light of the EU requirements. For countries with non-existing or weak DPL it may be wise to consider revising these laws if the EU is a major trading partner. Many countries have passed or proposed data protection legislation in order to continue free trading with countries that have enforced the concept of adequate protection (Roche, 1992). For example, Hungary was the first country from the eastern bloc to consider TDFL and has made it very clear that it feels a need to adopt conforming legislation because it fears it will be excluded from trade with the EU (BBC, 1992a, 1992b). For these countries the potential economic loss in not being able to gain access to another nation's data is often seen to outweigh the loss over reduced control of their own data (Samiee, 1984).

Recent news coverage on DPL developments in the USA indicate that the Clinton administration will most likely opt for self-regulation in privacy matters. The USA will "seek to find practical solutions that would satisfy the core concerns underlying the European directives while not unduly encroaching on US prerogatives"(Schwartz and Reidenberg, 1996, pp. 172-4). A possible model would be a set of codes of conduct and rules, which a company can agree to comply with. Non-compliance could result in the company being prosecuted under US anti-fraud laws. However, the USA and the EU have not been able to resolve this issue yet (*The Economist*, 1999b; Kane, 1998a, 1998b, 1998c; Meeks, 1997).

Limitations of the study and directions for future research

Future research efforts should try to triangulate the results of this exploratory research. A replication of this study in other EU countries could provide interesting results. German and Dutch MNCs have been used to at least some data protection laws since several years. We may expect very different results for MNCs operating in EU countries which until 1998 did not implement DPL and are now forced to adopt the strict DPL set forth by the EU Directive. Also, in place of an exploratory study, a quantitative research project dealing with ways of coping with strict DPL would be a good proposal for future research.

Also, a larger survey study could be performed to test the finding that companies transferring personal customer data are most affected by the strict EU Directive. A more detailed study of particularly affected MNCs might be warranted. What are the strategies these companies use to comply with EU

DPL? What are possible solutions regarding TBDF to countries with non-adequate protection?

Furthermore, the interviews with the corporations were subject to the vagaries of being opinions of one person, who may or may not represent the organizational perspective. A future study should therefore test the generalizability of the results presented in this paper.

Also, a more specific investigation of the nature of the relationship of culture and DP might be an interesting and rewarding project.

References

Amidon, P. (1992), "Widening privacy concerns", *Online: The Magazine of Online IS*, Vol. 16 No. 4, pp. 64-7.

Betts, M. (1993), "Computerized records: an open book?", *Computerworld*, Vol. 9 No. 1, August.

British Broadcasting Corporation (1992a), "Bill on personal data protection submitted to national assembly", *Summary of World Broadcasts*.

British Broadcasting Corporation (1992b), "Telecommunications bill presented to parliament", *Summary of World Broadcast*.

Business Europe (1995a), "Data protection: part two", 23 October.

Business Europe (1995b), "Updates", 6-12 March.

Cole, P. (1985), "New challenges to the US multinational in the European Economic Community: data protection laws", *New York University Journal of International Law and Politics*, Vol. 17, pp. 893-947.

(The) Economist (1993), "No hiding place: the technologies that make life easier are eroding people's privacy", 7 August.

(The) Economist (1996), "We know you are reading this: the rape of privacy", 10 February.

(The) Economist (1999a), "Direct hit: direct marketing, focused on individual consumer, has become a potent way to sell. Should consumers worry?", 9 January.

(The) Economist (1999b), "Data dogfights: America and Europe should not fight a privacy war over the protection of data gathered by companies about consumers", 9 January.

Ellger, R. (1987), "European data protection laws as non-tariff barriers to the transborder flow of information", in Mestmaecker, E.-J. (Ed.), *The Law and Economics of Transborder Telecommunications – A Symposium*, Nomos Verlagsgesellschaft, Baden-Baden, pp. 121-43.

EU (1995), "European Parliament and council directive 95/. . ./EC on the protection of individuals with regard to the processing of personal data and the free movement of such data", 24 July.

EU (1996), "Data protection: protection of personal data ensured at EU level", http://www.cec.lu/en/comm/dg15/smn/data.html, version of 20 June.

Franklin, C.E.H. (1996), *Business Guide to Privacy and Data Protection Legislation*, ICC Publishing, Paris.

Guynes, J.L. (1994), "Information system activities in transnational corporations: a comparison of US and non-US subsidiaries", *Journal of Global Information Management*, Vol. 2 No. 1, pp. 12-26.

ITA (1999), Draft: International Safe Harbor Privacy Principles Issued by the US Department of Commerce, http://www.ita.doc.gov/td/ecom/Principles1199.htm, data revised: 15 November, data accessed: 20 December.

Kane, M. (1998a), "International fight coming on privacy", http://www.zdnet.com/zdnn/content/zdnn/0124/278135.html, date revised: 24 January, date accessed: 26 January.

Kane, M. (1998b), "Privacy Czar not likely in US", http://www.zdnet.com/zdnn/content/zdnn/0124/278137.html, date revised: 24 January, date accessed: 26 January.

Kane, M. (1998c), "Some US firms already practice EU privacy", http://www.zdnet.com/zdnn/content/zdnn/0124/278136.html, date revised: 24 January, date accessed: 26 January.

Kobielus, J. (1992), "EC's new privacy proposals could hobble global nets", *Network World*, 27 January.

Meeks, B.N. (1997), "Industry group unveils privacy rules", http://www.zdnet.com/zdnn/content/msnb/1208/261700.html, date revised: 8 December, date accessed: 26 January 1998.

Mei, P. (1993), "The EC proposed data protection law', *Law and Policy in International Business*, Vol. 25, pp. 305-34.

Raab, C.D., Bennett, C.J., Gellman, R.M. and Waters, N. (1998), *Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method of Several Categories of Transfer – Final Report*, European Commission, http://europa.eu.int/comm/dg15/en/media/dataprot/studies/adequat.htm, data accessed: 20 December 1999.

Roche, E.M. (1992), *Managing Information Technology in Multinational Corporation*, Macmillan Publishing Company, New York, NY.

Samiee, S. (1984), "Transborder data flow constraints: a new challenge for multinational corporations", *Journal of International Business*, Spring/summer, pp. 144-50.

Schatz, W. (1998), "Profit versus privacy", *Information Strategy*, Vol. 3 No. 7, September.

Schwartz, P.M. and Reidenberg, J.R. (1996), *Data Privacy Law: A Study of the United States Data Protection*, Michie, Charlottesville, VA.

Swire, P.P. and Litan, R.E. (1998), *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directives*, Brookings Institution Press, Washington, DC.

Trubow, G. (1992), "The European harmonization of data protection laws threatens US participation in transborder data flow", *Northwestern Journal of International Law and Business*, Vol. 13, pp. 159-76.

Walczuch, R., Singh, S. and Palmer, T. (1995), "An analysis of the cultural motivations for transborder data flow legislation", *Information Technology and People*, Vol. 8 No. 2, pp. 37-57.

Appendix. Semi-structured interview outline

To be read to the interviewee

The following interview is part of a research undertaking to investigate the impact of European data protection legislation on multinational business and trade. This interview will be performed with the German data protection officials in 10-12 large multinational German and US companies. We will provide a copy of the final report to all interview partners.

Your answers will be treated anonymously and the name of your company will not be mentioned in any report or publication.

Background

(1) What is your position at <company name>?

(2) In what functional department is data protection organizationally placed (IS, Controlling,. . .)?

(3a) How many countries does your company operate in?

(3b) Are there transborder data flows involving personal data to all of these countries?

(4) What percentage of your job are data protection issues?

Questions related to data protection in general

(5a) Could you try to give an estimate of how much money is spent on data protection in your company?

(5b) . . . estimate of how many people work how many hours on data protection issues in your company?

Data protection issues related to transborder data flow

(6) Could you try to estimate what percentage of time and money is spent on. . .

(a) . . .data protection issues within Germany (collection of employee data, etc.)

(b) . . .data protection issues dealing with transborder data flows within the EU?

(c) . . .data protection issues dealing with transborder data flows with non-EU countries?

(7a) Do you feel like your company's business is being adversely affected by data protection legislation specifically regarding data transfer between Germany and the USA and on a global scale in general?

(7b) Do you expect any important changes to occur in this regard once the German legislation has been adjusted to the new EU data protection directive?

(8a) Do you face resistance/difficulties in explaining the German/EU data protection legislation to your counterparts in US/non-EU countries? How do you reach an agreement?

(8b) How does your company typically deal with data protection issues in data transfers from EU to non-EU countries? Are there codes of conduct, special contracts with business partners or data subjects, etc.?

(9) For which purposes does your company use transborder data flows? Which of these transborder data flows involve protected data, i.e. name-linked personal data?

(10) Was the organization adjusted in any form to satisfy data protection laws, e.g. decentralized control over marketing, personnel or manufacturing?

(11) Do you think that your industry branch is especially affected by data protection legislation? How important is data protection legislation to your business?

(12) Do you perceive data protection barriers as non-tariff barriers to trade? Do you feel that non-EU companies are unfairly treated by the European data protection legislation?

(13) What are the major problems with data protection legislation today and the new EU data protection Directive? How would you like to improve data protection legislation to better fit your business needs?

Thank you very much!