DATA PROTECTION IN EU FINANCIAL SERVICES

ALFREDO SOUSA DE JESUS

ECRI RESEARCH REPORT NO. 6
APRIL 2004

The European Credit Research Institute (ECRI) is a non-profit international association established in March 1999 in partnership with the Centre for European Policy Studies (CEPS) in Brussels. Its principal goal is to promote the study of the retail financial services sector at the EU level. ECRI's activities include the creation of a database on consumer credit in the European Union, research and analysis of developments in retail financial markets and the organisation of seminars on all issues affecting the industry.

This report was prepared by Alfredo Sousa de Jesus, Research Fellow at CEPS. The views expressed in this study are attributable only to the author in a personal capacity and not to any institution with which he is associated.

ISBN 92-9079-494-1

European Credit Research Institute
Place du Congrès 1, B-1000 Brussels
Tel: 32(0)2 229.39.11 Fax: 32(0)2 219.41.51
E-mail: info@ecri.be
Website: http://www.ecri.be

CONTENTS

DATA PROTECTION IN EU FINANCIAL SERVICES

ECRI RESEARCH REPORT NO. 6

ALFREDO SOUSA DE JESUS

Executive Summary

Individual privacy has always been a source of concern for common citizens, but mainly from the perspective of human rights and civil liberties.

Nowadays, the internet has focused attention once again on the issue of data protection. The major barrier to full development of the internet and e-commerce precisely remains consumers' reluctance to provide private and confidential information. With globalisation of the economy and the IT revolution, the banking industry is going through an evolutionary process, readapting the relationship with clients through new products and new means of delivery. In order to reap all the benefits from these new potentialities, however, financial services should not undermine the privacy issue.

National legislation on data protection is often out-of-date, ineffective and unenforceable owing to jurisdictional limitations, whereas at international level, a multiplicity of initiatives has led to a situation that is plagued by inconsistencies. Nevertheless, international instruments serve as an example for other national and EU legislation. As an alternative to the legislative approach, self-regulation, i.e. a code of conduct, appears particularly well suited to the issue of data protection in the context of the internet.

In 1995 and 1997, the EU adopted the directives on data protection based on a careful balance of interests between consumer protection and completion of the Internal Market through the free movement of information. This legislative framework provides a reasonable level of security within the EU area. Consumer confidence is reinforced through rights and obligations controlled by supervision authorities. Nevertheless, the system for international transfer of data outside EU territory appears impracticable and not easily enforceable. International movements are restricted to third countries providing an adequate level of protection, which represents a complex and incommensurate verification procedure. As far as the transfer of data to the US is concerned, the existing agreement provides an adequate level of protection but does not cover financial services. Therefore, the EU directive does not provide full protection all over the world, but simply grants people covered by its scope with a guarantee of an adequate level of protection for transfers.

Regarding this EU legislative framework, several problems remain since full harmonisation and effective and uniform implementation are not yet in place. Further to the adoption of the EU rules, national legislations continue to diverge, creating additional obstacles to the completion of the Internal Market. Furthermore, each member state uses the margin of manoeuvre allowed them by the directive in opposite ways, thereby creating legal uncertainty. Hence, the EU market continues, in practice, to be fragmented.

In addition, some other EU initiatives address indirectly the problem of data protection, such as the investment services or consumer credit directives. If most of the legislation is concerned with consumer privacy, some rules are derogating to the general framework, again creating inconsistencies and additional barriers.

Confronted with this unpromising situation, the EU launched in 2002 a revision process of the current legislative framework on data protection. It appears that most of shortcomings experienced are not caused primarily by the EU instruments themselves but mainly because of their national application. Therefore, it's improbable that the text would be amended. However, others discrepancies are clearly up to the EU directive itself, such as the international data transfer system and the negotiation of the Safe Harbour Agreement.

In any case, technological developments will always be ahead of the EU's political willingness to address the issue of data protection and of the member states' ability to transpose and implement related legislation.

DATA PROTECTION IN EU FINANCIAL SERVICES

ECRI RESEARCH REPORT NO. 6

ALFREDO SOUSA DE JESUS

Introduction

This paper deals with the issue of financial privacy, i.e. with rules on data protection that apply to financial services provided to consumers. The report aims at raising the awareness of EU consumers as regards threats to their privacy and at providing an overview of the current system of protection. In this context, it is also intended to contribute to the understanding of the legal framework of data protection in the European Union.

By the end of the 20th century, the free movement of information, the globalisation of economies and IT developments require a comprehensive review of all regulatory regimes, including the current consumer protection policy. This report is precisely concerned with the role of the law in regulating the privacy of financial transactions at national, international and European level.

The paper is structured as follows:

- Section 1 introduces a general background on data protection and consumer concerns when operating on the internet. This section expands the preliminary description into a detailed analysis of the impact of the IT revolution on the regulation of data protection and on the banking sector.
- Section 2 analyses the findings and limitations of national initiatives prior to any EU protection. This section also reviews precisely the impact of the EU regime on member state legislation. In parallel, several initiatives at international level are also considered, because of their influence on the EU legislative framework. As an alternative to the traditional legislative framework (national, international and European), this section concludes by addressing the contribution of the industry through the application of voluntary codes of conduct.
- Section 3 goes to the heart of the issue: the analysis of the EU framework on data protection. This section illustrates such rules with concrete examples and applies them to practical cases occurring in the banking sector. Due to globalisation, this chapter also describes in more detail the cross-border transfers of information to third countries, through different types of existing mechanisms (adequacy of the protection, contractual clauses and the Safe Harbour Agreement).
- Section 4 is devoted to the specific-sector EU legislation referring explicitly to privacy concerns, as an application or a derogation of the EU directives.
- As the EU legislation on data protection became outdated, section 5 provides an overview of the preliminary conclusions drawn by the current consultation process, carried out by the European Commission on the implementation of the directive on data protection.
- In the last section, the report draws an overall conclusion, followed by a wide range of recommendations addressed to all relevant actors: consumers, industry and policy-makers.

This report aims to provide a critical and informative contribution to the debate about challenges posed by the new technologies to EU law on privacy in the field of financial services.

To conform with ECRI's mandate, the scope of the report is restricted to 'Business-to-Consumers' (B2C) activities and the related legislation, as it is precisely at this level of relationship that barriers to the completion of the Single Market emerge.

The report focuses exclusively on issues of data protection arising in the private sector, choosing to ignore the concerns raised by the possible use of personal data made by the Government. In the same way, the approach followed is restricted to civil law matters, thus excluding criminal law and procedure. In assessing the effect of the legal framework, the scope of the report is therefore limited to the consumer point of view and does not address the issue of the fundamental human rights enjoyed by all EU citizens.

Finally, financial services and data protection are analysed both in the traditional and the on-line market, under a legal perspective, excluding any IT technical considerations.

1. The Importance of Data Protection in Financial Services

1.1 Data protection and on-line concerns

Data protection concerns began to appear in the early 1980s. The reality of IT (information technology) was in its infancy at the time: there were few computers in the world, all of which were very expensive, with restricted storage capacity and used only by public administrations. A few years later, the context had changed totally, with the arrival of the PC in every household and developments in the private sector. The EU adopted then a general legislative framework to respond to threats to personal privacy.

Since the early 1990s, an increasing number of PCs are connected to the internet, the symbol of an open space without territorial boundaries. Since the adoption in 1995 of the directive (95/46/EC) on the protection of individuals with regard to the processing of personal data and on the free movement of data, the provision of services has substantially changed. The online world has developed, changing the relationship between business and consumers through e-commerce. The EU has always seen the use of the information society as a major priority to turn the European economy into one of the most competitive in the world, as was stated in the Lisbon priorities (December 2000). The EU is perfectly aware of the benefits that the new economy brings to consumers and industries alike, but it also knows that such technological developments have to be addressed within a policy framework to avoid potential adverse effects on human rights, civil liberties and privacy. Methods of data protection have therefore to be brought totally up-to-date in light of new concepts, processes and products. The EU is thus facing a paradox: it has to find a balance between the need to protect the fundamental rights of the consumers and the need to foster the Single Market by making full use of the free movement of goods, persons and services in the context of the information society.

The EU is right in considering that one aspect of the IT revolution has generated significant concerns amongst its citizens: the potential risks to individual privacy. With the dramatic reduction of costs to access and process information, it has become easier than ever before to track down other individuals and find out plenty of information about them. It becomes impossible in practice for governmental authorities or regulators to keep track, on a real-time basis, of the processing and transfer of personal data. An online survey of citizens' views on data protection shows that 45% of those surveyed believe that the current level of protection in their home country is of a minimum standard, while only 10% believe that their country has a high level of data protection. 82% of those surveyed consider that the public awareness of data protection measures is insufficient, bad or very bad. In this context, data protection concerns have evolved from a niche sector to one of vital importance for business.

The internet has provided practical examples of breaches of data privacy, most of which occur without the awareness of the user, such as the interception of e-mails. A simple connection to the internet, even if the aim is not to communicate data, poses risks. Cookies and JavaScript have the aim of collecting and disclosing private information without the consent of the user. By using such information obtained free of charge, detailed user profiles are constructed, based on consumer preferences and spending habits. Such profiles, having an important economical and commercial value, are then sold to marketing and advertising companies to target specific segments of the population. Consumers then begin to receive unsolicited e-mails of a commercial nature at their private address. This technique, known as 'spamming' is analysed below. In a consumer society, complete tracking of consumption is very revealing. Other examples could be cited, such as spywares.

1.2 Traditional financial services and e-banking activity

E-commerce, as with any traditional business, involves payment of a service or goods (tangible or intangible). Concerns about the security risks of sending credit card details over the internet and the possibility of confidential personal information being disclosed to unauthorised third parties, are two of the limiting factors to any further development of e-commerce. Only 10% of respondents in a Eurobarometer survey[1] reported having used credit cards for an on-line payment. Amongst the remaining 90%, 30% are not interested in paying that way and 25% consider it unsafe.

Along with many other industries, the banking sector was deeply affected by the technological revolution. The main forces behind the reshaping of the banking industry are indeed the globalisation of the economy, deregulation and innovation in IT. On-line banking has developed, from virtual insignificance to being used by millions of clients. E-banking has doubled almost annually since the mid-1990s. Some Nordic countries have achieved more than 25% of e-banking clients. [2]

The banking industry is sensitive to those IT clients: 27% of the European banks surveyed in a consultancy report[3] considered that the "internet has a major impact on financial business". It leads the banks and financial institutions to innovate and develop a new relationship with clients through new products and new means of delivering them. Regarding the customer network, 24% of the surveyed companies were of the opinion that the internet will become by 2007 the major channel of contact with clients, even if 61% continue to think that bank desks will remain in first place.

Consumers take indeed all the benefits from e-banking without frontiers: time convenience, speed, a large choice of products and services and finally low prices. This new support of services offers clients a full range of possibilities:

- the daily management of bank accounts (consultation of balances, transfers, savings, …)
- bills payment and loans transactions
- brokerage & securities services
- credit & loan contracts
- services and products requests (cheques, credit cards, rate level)
- insurance and mutual funds

[1] Eurobarometer survey No. 56 on public opinion on financial services, Eurostat, European Commission.

[2] See OECD (2001).

[3] See Forrester Research (2002).

- e-commerce through secure payment system provided by banks.

The still growing number of clients using on-line services attests to the relative success of e-banking, even if it closely correlates to internet penetration. In some countries, such as Spain and Portugal for example, figures related to e-banking activities are even higher than the internet penetration would seem to justify. The main reason is simply a more pro-active on-line strategy pursued by the banks of those countries.

Despite the advantages of e-banking, many consumers are still hesitant to do cross-border shopping. The same Eurobarometer survey cited above (see fn 1) demonstrates that the public's major concern is precisely the processing of personal financial data. 40% of EU citizens responding felt that their national legislation on new means of payment does not guarantee the protection of confidential information and the security of transactions.

Most people understand that financial transactions are becoming more traceable over the time. Historically, consumers began with cash payments, moved on to checks and ended in the present situation, where even small amounts of money are paid through debit/credit cards. This shift in the methods of payment shows an evolution towards creating records in databases with the full history of the purchaser. This phenomenon is not expected to be reversed.

Indeed, marketing and advertising firms have developed a series of consumer behaviour encouraging more traceable transactions. Affinity programmes such as 'frequent flyer' schemes give incentives for on-line purchases and payment by credit cards. Banks provide for wider protection in case of credit card loss which is welcomed in relation to a loss of cash which can not be protected in any event. Electronic payments are more traceable but also more transparent, which is a positive point for a good audit trail. Even governments adopt measures promoting direct or indirect use of electronic payments, such as on-line VAT declarations with automatic payments. The several points made so far illustrate that people are making electronic payments more often, allowing databases to accumulate information on the payer, the payee and the items sold or the service provided.

In this atmosphere of distrust, the incentives for the banking industry to protect privacy are of both a legal and a financial nature. As such, a company's privacy policy may become part of its overall marketing efforts to develop brand equity and an image of quality service. More broadly, an entire industry might be able to gain sales by developing a reputation for protecting privacy, like the most famous example of the Swiss banking system.

At this point, the following conclusion can already be drawn:

❶ Data protection concerns had clearly emerged before the IT revolution. Nevertheless, the internet has focused attention on **privacy** again, but at a higher level of concern. The internet was indeed conceived as a world open network through which information could be shared. It is necessary to find the **appropriate balance between the open nature of the web and the protection of online users' data**. This is the crucial condition for any further development of the internet and e-commerce.

❷ On-line retailing has rapidly moved from being an interesting consumer experiment to a well-accepted retail alternative. However, any further development of e-commerce must increase consumer security by turning the internet into a **consumer-friendly place**.

2. National and International Law on Data Protection

Before moving on to the main part of this report – i.e. the EU framework on data protection applied to financial services – a few words have to be said on the domestic situations prior and

further to the EU directive. In parallel with the national and EU approach, one also needs to review the broad legal and political context occurring at international level.

Domestic legislation alone could not be effective to protect private data. Moreover, member states are divided as regards the approach to regulation. International and European organisations had therefore taken it upon themselves to legislate for data protection in order to harmonise divergent national approaches.

In addition to national, international and European regulation, this report draws attention to the voluntary codes of conduct that are emerging as a credible alternative to traditional legislation.

2.1 The legislative framework

2.1.1 The national legislative approach

By the middle of the 1970s, most EU countries considered the protection of personal data as a constitutional principle, derived from the right to private life. The scope of privacy legislation differs widely from one member state to another.

The UK and the Nordic countries are generally more in favour of codes of conduct supporting legislation on broad principles. On the other hand, the other member states prefer detailed technical regulations.

Independently of the approach selected (broad principles or detailed regulations), 45% of EU citizens consider that their national legislation does not guarantee transparency of financial information. Furthermore, 42% are of the opinion that their national legislation does not guarantee protection of consumers' rights, while 38% think their country's legislation does not guarantee the protection of the confidentiality of information. Those surveyed were asked if national standards should be harmonised throughout the EU. The answers were astonishing: 2.5 out of every 3 persons are in favour of EU legislation, of which 53% support full harmonisation against 19% in favour of a partial harmonisation.[4]

Before the early 1990s, most member states had enacted first-generation legislation, covering on-line data protection. For some of them, the transposition of the 1995 and 1997 EU directives aiming at the harmonisation of national rules led to the creation of an entirely new legal framework and of supervisory authorities. For the others, the EU regulation obliged them at least to make significant modifications to existing regimes.

Some member states (UK, Ireland and Luxembourg) did not hide their reluctance to adopt the EU directives. The Commission took several member states to court for failure to pursue all the necessary measures to implement the directives. Furthermore, some of them (France and Luxembourg), as evidence of the controversy, transposed the EU legislation well after the deadline of October 1998. The implementation of the directive into German law was done in … May 2001!

According to the Association of Consumer Credit Information Suppliers (ACCIS), in the current revision process of the data protection regime, "the status of application of the directive differs significantly in the various countries. In the majority of countries, it has not yet been possible to make a conclusive assessment of the actual effects. Several countries are still going through the transition phase of adaptation to the new requirements; in others, negotiations are currently still in progress between credit bureaus and data protection authorities with regard to the interpretation and application in conformity with the law. Official commentaries on the new

[4] See Eurobarometer survey No. 56 regarding public opinion in the EU concerning financial services, Eurostat, European Commission.

laws are still lacking for the most part, which means that there is still a higher degree of uncertainty regarding the interpretation of specific provisions of the directive".[5]

Further to the adoption of the EU legislation on data protection and during its implementation, member states used and abused the margin of manoeuvre granted by the EU directives. On some issues of major importance, the directive leaves the possibility to pursue certain options to member states. As a consequence, rights, obligations, administrative requirements and formalities simply differ from one member state to another. For example:

- Article 7 of the directive provides that personal data might be processed only if one of the conditions has been met, including the unambiguous consent of the data subject. Further to the transposition into national law, the German, French and Spanish legislation allows the individual the possibility to refuse consent, applying the 'opt-out' procedure. By contrast, the UK law deleted the unambiguous character. Moreover, Italian law (Law No. 675 of 1996 and Decree No. 467 of 2001) requires many more formalities, lying down that the consent must be freely expressed, specific and documented in writing, thereby imposing the solution of the 'opt-in' procedure. Moreover, Italian rules require that consent has to be given not only for data processing, but also for their communication. This requirement is not present in the directive where communications, as such, is part of the processing.
- Austrian and Italian laws (Law No. 675 of 1996 and Decree No. 467 of 2001) apply data protection to legal persons, which is not the case in the EU directive.
- In Spain, the requirement for data controller (i.e. the processor) is to delete all customer data from records as soon as the relationship ends. In the UK, data could be kept for a reasonable period of time after the end of the relationship, while in Greece the retention time for data could be extended.

Due to excessive use of the margin of manoeuvre, the aim of the EU directive to harmonise national rules remains partially unachieved. Moreover, divergences are so significant that both consumers and industry complain of additional barriers to the Internal Market.

Later in section 3, which is dedicated to the analysis of the EU legislation, the report considers in detail the cases where member states dispose of a 'margin of manoeuvre'.

2.1.2 The international approach

Several international organisations have launched various initiatives to address data protection. Some of them, such as the Council of Europe, have had tremendous influence on the legislative framework at EU and national level. In order to provide a full picture, it is worthwhile to undertake a chronological analysis of international initiatives.

In 1953, the Council of Europe's Convention on Human Rights and Fundamental Freedoms came into force, establishing for the first time 'the right to privacy' in Article 8. Even if the EU is not part of such a Convention, Article 6.2 of the EU Treaty states the same rule, namely that the EU must respect fundamental rights in all its activities.

During the 1960s and part of the 1970s, developments in information and communication technologies (ICT) gave rise to concerns on the need for measures to protect individuals from massive processing of private information. In 1974, the Committee of Ministers of the Council of Europe adopted several resolutions to establish minimum standard of protection.

[5] ACCIS (Association of Consumer Credit Information Suppliers) Position Paper (2002) on the reform of the data protection regime.

In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. Known as Convention No. 108, this text lays down a number of basic data protection principles, providing for a maximum degree of harmonisation between signatory states.

Even if the EU has meanwhile adopted the directive on data protection, the Convention remains relevant in several areas, namely in case of data transfers to third countries. The Convention represented a major contribution to the current legal framework, mainly with regard to principles applying to the processing of data, the rights conferred to data subjects, the basic rules applying to third countries' data transfers and mutual assistance between national supervisory authorities. The Convention was however limited to automatic processing of data.

In 1981, the Organisation for Economic Cooperation and Development (OECD) adopted some Guidelines aiming at the protection of personal information. Most of the principles to be found in the EU directives were already present in this document.

In the early 1980s, the European Parliament noted that several member states did not sign the Convention No. 108. In Italy and Greece, the very first legislation was introduced only in 1997!

In 2000, the Nice Summit formally endorsed the Charter of Fundamental Rights of the EU. Its Provision 8 states that the protection of personal data is a fundamental right of the individual, autonomous and separate from the traditional broader right to respect for private and family life, which the Charter also covers in Article 7. It is of particular relevance that the Charter goes beyond simply stating the right to the protection of personal data and also mentions a vital tool for ensuring actual compliance, which is subject to control by an independent authority. In the meantime, the Charter of Fundamental Rights has been integrated into the EU Constitutional Treaty (Part II), adopted by the European Convention on the Future of the EU. Once accepted by the Council, data protection will be recognised at the highest level of binding legislation in the EU.

2.2 An alternative to the legislative approach?

The mere identification of a problem does not create the presumption that the policy-maker should regulate. It is necessary to ask whether and why market-based solutions would not emerge.

The industry and trade associations have always shown their preference for voluntary codes of practice to regulate some problems. Drafted by professionals and trade associations, the intervention of any political or administrative regulation is avoided.

Self-regulation allows for flexibility and informality of the regulatory regime. The EU directive on data protection recognises this and takes into account any contribution giving an added-value to the legislative framework. Whenever the adequacy of third countries' laws should be assessed, specific reference is made not only to national laws but also to "professional rules and security measures which are complied within that country".

In order to overcome some of the shortcomings of the codes of practice and to improve the importance of self-regulation, member states should accept more easily its usefulness and recognise an added value in legal terms, by an official recognition of codes of conduct. In the meantime, self-regulation is influenced by private legal norms regarding torts, contracts, rights and obligations, which themselves influence the legislation.

The quality assessment of codes of conduct should be based on several indicators: Is the body in charge of the code representative of the sector? Is the code able to be adequately enforced?

What are the levels of sanctions? Is the body able to impose sanctions to the sector in case of non-compliance? In short, such an assessment could be structured as follow:

- **Good level of compliance.** Codes of conduct are drafted by a body, representing a sector or profession. Once drafted, the code applies to all members. The level of compliance depends not only on the awareness of the content by the members, but also on the transparency of the code to consumers, on an external system of assessment and on the nature and enforcement of the sanctions (remedial and punitive).
- **Support and help to individual data subjects.** A high quality code of conduct provides consumers with support in case of problems of private data. This support should be impartial, independent and equipped with the necessary powers to investigate any complaints.
- **Appropriate redress.** In case of non-compliance, remedies should be granted. The remedy must find a solution to the problem (e.g. correction of inaccurate data) and in case of damages, allow the payment of an appropriate compensation, including physical damages and financial loss.

The EU has begun however to consider this form of regulation. The directive promotes the use of self-regulation. Moreover, the Working Group, created by the directive, had adopted a series of conclusions going in the same direction.

At this point in the analysis, the following conclusions may be drawn:

❶ **National approaches are territorially limited.** Discrepancies between different national laws are sufficient to warrant further harmonisation between member states. However, even beyond the adoption of the EU directives, national **disparities arising from their implementation** have a negative effect on the movement of data within a member state and within the EU, by creating additional barriers to the completion of the Internal Market. Also, most citizens do not trust national legislation and the vast majority of them are in favour of maximum EU harmonisation.

❷ The multiplication of international initiatives leads to a situation of **inconsistencies (forms, content).** Each initiative follows **a different aim (human rights, economics and consumers).** Nevertheless, international instruments remain still relevant and were considered as an example for other national and EU legislation.

❸ **Codes of practice emerged as a credible alternative,** demonstrating that the traditional legislative approach is not entirely appropriate to ensure data protection. Therefore, industry self-regulation, whenever presenting a high-quality assessment, appears useful, even if it is not yet recognised by most member states. Although the EU directive promotes codes of conduct, in practice this instrument is still being used under its real capacity.

3. General EU Legislation on Data Protection

Data protection represents a key issue for EU citizens as individuals and mainly for EU consumers who would benefit from the perfect completion of the Single Market.

This report analyses in detail all European regulation applying to data protection, within the EU territory but also in the cross-border context of data transfers to third (non-EU) countries.

3.1 EU directive on data protection

3.1.1 Political context of the legislative initiative

In 1990, the EU adopted a package of measures in order to secure an EU approach to data protection.

The goals were ambitious and somewhat irreconcilable: "to protect fundamental rights of natural persons, in particular the right of privacy", but also "to prevent barriers to the free flow of personal data across the EU". The scope was much broader than the Council of Europe Convention No. 108, which applies to manual and automatic data processing, both within private and public sectors.

In 1992, the European Commission proposed a version of the proposal that was much closer to Convention No. 108 (minimalist approach) and similar to the current national systems.

Some member states, namely the UK and Ireland, were strongly against any directive on data protection and maintained that Convention No. 108 satisfactorily protected consumers. Industry (banks, insurance companies and credit reference agencies) was also opposed to such a directive, due to financial and administrative costs of its implementation.

The directive, known as the "directive on the Protection of Individuals with regards to the Processing of Personal Data and on the Free Movement of such data", was finally adopted on 24 October 1995 and had to be implemented within three years.

3.1.2 Definitions and scope

There are wide differences of views as to what should be regarded as private information. Variations exist between individuals depending on culture, age, social position, country ... but also depending on time. What was considered private 20 years ago may not be so today.

Therefore it is imperative to define rules regarding data protection as broadly as possible to cover the current situation, but also to anticipate the natural evolution of the near future. The present directive is perfectly in line with this philosophy, resorting to a broad definition and using abstract legal concepts.

The scope of the directive is clearly set out in the text. It applies to any operation or set of operations that is performed upon personal data, including storage, disclosure, collection, processing … It does not apply to natural persons in the course of a purely personal or household activity (e.g. an electronic personal diary or a file with details of family and friends). It applies to data processed by automated means and to data that are part of a non-automated "filing system", in which they are accessible according to specific criteria, including manual and paper filing systems. This basically means that the directive applies from the last up-dated model of computer database customers to the oldest manual card file with details of clients.

The directive states that it does not apply to a list of state activities such as those falling outside the scope of EU competences (Title V (PESC) and VI (JAI) of the Treaty) as well as to the process operations concerning public security, defence, state security (including the well-being of the state) and criminal law. It has been pointed out that such derogations could turn any state into a "Big Brother" country monitoring the life of all its citizens.

3.1.3 Applicable law and competent Jurisdictions

The internet totally changed the face of civil and criminal jurisdiction, introducing disputes for small amounts of money, extra-territorial issues, difficulties in the choice of the competent jurisdiction and finally, in the enforcement of judicial decisions.

The directive defines clearly which jurisdiction is responsible for which data. A member state has jurisdiction on the processing of data if:

- the data controller is established in the said member state;
- the controller is established outside but at a place where the national laws of the member state apply according to international public law; or
- the controller is outside the EU territory but the processing is done through equipment established in the member state.

When a data controller is not established in a member state, it must designate a representative. This provision intends to be a solution for the internet cases: internet service providers could then be considered controllers in e-mail transmissions with data, with all the obligations this implies.

In this context, the relation between a controller and non-EU customers could be particularly complex. For example, banks are required to go through all relevant data protection controls to see whether non-EU customers need to be notified about EU rules, depending on the location of the controller.[6]

Furthermore, a data controller established in several member states must comply with the obligations laid down in each one of them, facing the application of different national laws depending on where it is established. If each establishment sends a customer database to a single and centralised data controller, several laws apply to the personal data contained in one single database.

At least at criminal level, the directive is clear: it applies the principle of territoriality. One exception is stated: the directive does not apply if data are simply transmitted through EU territory, e.g. a transfer from Turkey to the US using telecommunication links passing through EU territory.

3.1.4 Obligations in the processing of data

The directive contemplates several fundamental articles under the title of "General rules on the lawfulness of the processing of personal data". In conformity with those provisions, member states are entirely free to determine more precisely their own rules for data processing regarding two elements: data processors and data subjects. Member states therefore enjoy a broad margin of manoeuvre in the implementation of the main provisions.

As a statement of good business practices, the directive provides that data should be:

- Fairly and lawfully processed

[6] For the British Bankers' Association (BBA), this situation makes no sense at all to the customers involved, as they are not aware of any law that gives them the rights provided by the directive in their home country. Therefore, the BBA is of the opinion that the directive should not apply whenever a data controller is not established in a member state, but uses equipment in that member state. In addition, there is little point in requiring a data controller to appoint a representative in the member state where the processing takes place.

e.g. In this context, the use of cookies is illegal when made without the knowledge of the internet user, and is not fair when used for any other purposes.

- Collected for specified, explicit and legitimate purposes, and used accordingly. Further processing remains possible when the member state provides appropriate safeguards.

  e.g. A banking institution processes data, including medical information of each client. The bank argues that the processing is being carried out for the mere purpose of retail activities, whereas it is also used/sold for marketing activities in the insurance branch, belonging to the same group. This financial institution is breaching several provisions of the directive: even if the data processing is fairly and lawfully carried out by the bank itself, data are being used for an illegitimate purpose and are not used according to the initial purpose. Even more, the collection of medical information on clients is unacceptable and excessive, and is considered as "sensitive data".

- Adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed.

  e.g. A bank should not need any information about the religious and political commitments of its client when processing a demand for a home loan. In one case, the Irish data protection authority disallowed the practice of disclosing information for credit referencing. In fact, when requested by a bank to provide the credit history of a named individual, the Irish credit bureau gave the credit history of all individuals having the same name. The national authority considered this information as inadequate and called on financial institutions to make better efforts to identify the customers.

- Accurate and, whenever necessary, up-to-date. Data controllers are required to take any reasonable step to ensure the rectification or erasure of inaccurate data.

- Kept in a form that permits identification of data subjects for no longer than necessary.

  e.g. In Belgium, draft legislation was discussed in order to enhance the quality of data integrated in the national consumer credit database, which is under the control of the central bank (Banque Nationale de Belgique). This database will not only include credit information related to defaults of payment, but also all information related to consumer credit contracts. The Belgian data protection authority made some observations related to the duration of the storage of information related to defaults of payment, and expressed concern about the possible use of national identification numbers by the national bank.

In this context, a privacy policy might become a marketing tool in order to develop an image of quality service, and therefore to gain sales and new customers.

e.g. AT&T has advertised nationally that it will not use customer calling records to contact potential new customers, as MCI apparently did under its 'friends and family' programme.

The legitimate purpose and the adequacy of processing data according to the purpose represent abstract conditions, imposing a proportionality principle which is particularly difficult to apply. Therefore, the directive elaborates by explaining in detail the rules of legitimate data processing.

The directive requires member states to ensure that personal data may be processed only if:

- The data subjects gave their consent;

- The processing is necessary in a pre-contractual or contractual context involving the subject (e.g. loans, mortgages, …);
- The processing is compulsory according to a legal obligation applying to the controller;
- The processing is needed to protect vital interests of the subject;
- The processing is needed in order to disclose information of public interest or in the course of the exercise of an official duties (e.g. tax authorities, …); or
- The processing is necessary for the purposes of the legitimate interests pursued by the controller, a third party or parties to whom the data are disclosed, except where interests are overridden by concern for the protection of the fundamental rights and freedoms of the data subject.

  e.g. Through a home banking connection, one financial institution is placing unauthorised cookies and JavaScript inside its clients' computers. The collection of information allows the bank to draw a consumer profile and send information on financial products through advertising banners. This behaviour runs against the EU directive: firstly, the collection and disclosure of information is not carried out fairly and lawfully, and secondly, the information is collected without the consent of the client and, therefore, the processing is not legitimate.

The directive prohibits the processing of "sensitive data", unless one of a series of conditions is met. In most cases, sensitive data cannot be processed without the explicit consent of the data subject. The industry evidences some difficulties in understanding the scope of "sensitive data". In some cases it looks obvious, whereas in others, the borderline between sensitive and personal information is blurred.

e.g. Could information about a data subject's credit rating be considered as sensitive?

What about the sensitive data provided by a third person and not by the data subject? Is it still "sensitive" according to the directive?

e.g. Before the conclusion of a home insurance or a motor insurance policy, the insurance company (data controller) will ask questions about individuals who may live with the policyholder (data subject) or who may drive his car. Those questions could possibly include criminal convictions. In this context, a policyholder could be denied insurance because of circumstances that could be considered as sensitive data but pertaining to a third party.

Therefore, the industry is reluctant to establish a definitive list of sensitive data. Again, member states have developed their own national legislation, which in practice implies the lack of a harmonised EU regime on this issue.

Access to data is decided by the controller, who is in charge of giving instructions on the processing and control of data. It is also paramount that data are securely stored, through appropriate measures, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected. The controller must implement all technical and organisational measures, such as the installation of fire systems or alternative energy systems, to protect data and information of a personal nature.

e.g. Some controllers, most of the companies, are developing their own privacy-related software. The Royal Bank of Canada designed a programme to show clients how the bank is using information about them. For example, in the case of a checking account or a home mortgage, the bank does not share account data with its brokerage

operations and avoids making marketing calls about investments. In the menu of the programme, each client is able to choose their preferred level of privacy.

It is important to note that in the last on-line survey carried out by the Commission, the majority of the controllers surveyed were of the opinion that the level of protection is good, but noted that the disparities between member states' legislation are too significant to allow data to move freely within the Community, or that some further harmonisation would be desirable, suggesting therefore that the main aim of the directive has not been achieved.

3.1.5 Rights of the data subject

Data subjects have a right to be informed of the processing of data about them. Whether the collection of information is done directly or indirectly by the subject himself, the controller must inform the subject about his identity, the purposes of the processing, the recipients of the data and the right of access to and the ability to rectify the data.

e.g. Amazon.com informs its clients that their purchase history will be used to develop product recommendations, exposing the clients to a list of items selected according to their profile and behaviour. This system is known by each consumer and is not particularly intrusive, as it is limited to Amazon.com.

The exceptions to this requirement of information are very narrow and limited to cases where the provision of information implies a disproportionate effort, but they are not compulsory and may not apply in the case of information collected directly from the data subject.

e.g. In the context of consumer credit, it is not a disproportionate effort for the company to inform the subject that the data are intended to prevent over-indebtedness, money laundering and fraud, for marketing purposes and even for statistical analysis and market research.

Nevertheless, even if the data subject has a right of information, most of the time the vast majority of consumers – already overloaded with information – do not take time to read the statements. While transparency is important, too much explanation becomes confusing. When information is collected by phone, statements about their rights are considered by most consumers to be tedious and boring, and they may even be reluctant to listen.

The directive also provides data subjects with the right of access to the personal data that are being processed in order to verify, in particular, the accuracy of such data and the lawfulness of the processing. The data subject can obtain from the controller the rectification, erasure or blocking of data whose processing does not comply with the provisions of the directive, in particular whenever data are inaccurate and incomplete. In this case, the controller has to notify any third parties to whom such data have been disclosed. This right of access must not, however, lead the data subject to the systematic refusal to provide information.

e.g. In the UK, credit reference agencies receive thousands of requests each day, for which a maximum fee of £10 each is charged. Excessive abuse of the right of access could lead to an increased fee. According to the BBA (British Bankers' Association), UK lawyers advise their client to use the subject right of access as a cheaper means of obtaining material for a possible court case. The treatment of such frivolous requests entails significant costs for banks in terms of both time and human resources.

Nevertheless, the data subject has the right to object to the processing of data relating to him in certain circumstances. Whenever a justified objection is made, the processing carried out by the controller may no longer involve those data. The directive also contemplates the right for any

data subject to object to the processing of personal data for the purpose of direct marketing, therefore affecting one of the selling techniques used in the financial and banking sector.

Furthermore, the directive provides that member states shall grant every person the right not to be subject to a decision that has legal effects or significantly affects him, and that is based solely on the automated processing of data intended to evaluate certain personal aspects, such as performance at work, creditworthiness, reliability, conduct, etc… The purpose and the content of this right is particularly confused. The aim of this provision seems to be the protection of the data subject from any risks of abusive use of IT, in the context of a decision solely taken by a machine, such as is the case for retail credit consumers. The industry does not find it reasonable to assume that decisions are automatically made solely on the basis of a single parameter, such as the credit bureau scoring. A provision should provide for the transfer of applications rejected by the automated system.

> e.g. Many credit providers now use decision support systems which incorporate data from a variety of sources into business policy guidelines on credit decisions.[7]

The last right referred to by the directive is the right to a judicial remedy in case any rights are breached that are granted by national law in accordance with the directive. For any damage stemming from an abusive data processing operation, the subject is entitled to receive a right of compensation from the controller. According to the "margin de manoeuvre" of the member state, sanctions could differ widely from one country to another, depending on the national level of protection.

3.1.6 The supervisory authority and the notification procedure

One of the requirements of the directive is that member states provide for one or more supervisory authorities to monitor and promote the application of data protection laws, and to investigate complaints of non-compliance.

Every processing operation has to be previously and formally notified to such authority, in order to ensure that the data processing activity is being carried in accordance with national measures. Member states decide on the content of information to be provided to the authority, taking into consideration that the directive is limited to the definition of some requirements. Member states also decide which data processing is at risk for data subjects, justifying prior examination by means of an opinion or an authorisation procedure.

When the investigation of a complaint highlights non-compliance with the law, the Supervisory Authority has the power to ban the processing of specific data.

The notification principle also provides for some exemptions, or alternatively a simplified procedure of notification, in cases where:

- the proceeding is unlikely to adversely affect the rights and freedoms of the data subject, or
- an independent officer in charge of the data protection process has been appointed in conformity with national law.

Member states have to carefully specify the types of data processing to which an exemption may apply. In case data processing operators do not require the notification procedures, the data controller has to make information available in the appropriate form to any person on request.

---

[7] Such as supported by the ACCIS (Association of Consumers Credit Information Suppliers), it may longer be sufficiently clear to the employee of a credit provider which data or which business policy rule triggers the automatic acceptance of an application.

As the last word is left to the member states, it appears that a heterogeneous implementation of notification requirements results in increased expenditure and administrative burdens for companies operating in more than one member state. Moreover, it is not uncommon to hear complaints from the industry about the fact that the notification regime does not provide any added data protection value for individuals.

In this context, the industry favours an EU-wide notification regime, so that each controller needs to issues only one notification. Where a company has several subsidiaries through the EU and in third countries, the industry is of the opinion that a country could be designated, where the group must be formally registered for data protection purposes; the group would then comply with the legislation of that country within the EU and beyond.

For the BBA (Position Paper on the revision of the data protection regime, 2002), this means the application of cross-border provisions for financial services and the country of origin approach when looking at financial services. Moreover, the notification procedure should only be required in limited cases, and, in the event of failure to comply, sanctions should be more proportionate.

In order to correct for some eventual excesses of this margin of manoeuvre and to ensure a smooth harmonisation, the directive set up a Committee, the "Article 29 Working Group", composed by a data protection representative of each member state and the European Commission. This body is in charge of:

- examining the application of national measures adopted under the directive,
- providing an opinion on the level of protection in the EU and third countries and on codes of conduct drawn up at EU level, and
- advising the Commission on any new amendments to the directive, on any specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data.

The foregoing considerations confirm that:

❶ The protection of human rights and the completion of the Single Market are the grounds of the directive, which leads the consumer to a **high level of expectations**. However, due to the implementation problems (deriving not so much from the EU rules, but mainly from the transposed laws), **harmonisation still remains a project** and is far from being achieved.

❷ Definitions of concepts, such as sensitive data, left in some cases **too much room for interpretation**.

❸ The notification procedure appears to be **too formal and divergent** from one member state to another. In practice, this situation prevents any EU firm from developing a cross-border activity. An EU-wide notification regime seems to be, in this context, more appropriate.

3.1.7 Data processing and transfer outside the EU territory

The directive is based on territorial application of national laws. Member states therefore have jurisdiction only with regards to data processing carried out by entities within its territory.

Nevertheless, in the context of globalisation, data processing and transfers are being carried out at low cost, which means increasingly outside the EU jurisdiction. The directive, however, establishes rules to ensure the continuity of EU protection. The directive does allow transfers to third countries, but only if they can provide an adequate level of protection for personal data. It also offers guidance on criteria to be used in defining an adequate level of protection, such as the nature of the data, the circumstances of the transfers and the purpose and duration of the processing.

An adequate level of protection

Article 25 suggests a three-fold approach to assess the level of adequacy:

- A case-by-case approach. The level of protection in a third country is analysed in relation to a specific transfer or a category of transfers.
- A soft and open approach. The assessment of adequacy takes into consideration not only the particularities of the data transfers, but also the solutions presented by each member state.
- A functional approach. The level of protection is assessed in relation to risks occurring during transfers, but also in relation to specific or general measures implemented by the controller established in the third country to cover those risks.

Some questions need to be addressed regarding the notion of adequate level of protection. Where the adequacy is difficult to evaluate, the directive does not provide any additional information. Adequate, but adequate in relation to what? In addition, the criteria provided by the directive to evaluate such adequacy are not exhaustive and others could be taken into consideration. Moreover, the directive provides criteria of evaluation (duration of the transfers, nature, circumstances…) without defining them.

The Article 29 Working Group set out a series of criteria, called 'risks factors', to assess the 'adequacy' of the protection, suggesting that risks of privacy could appear in the following:

- Transfers of sensitive data (e.g. sex, religion, union membership);
- Transfers carrying the risk of financial loss (e.g. credit card payments through the internet);
- Transfers carrying the risk of personal safety;
- Transfers made for the purpose of taking a decision which significantly affects the individual (e.g. the granting of credit);
- Transfers carrying risk of embarrassment or tarnishing of an individual's reputation;
- Transfers that may constitute an intrusion into an individual's private life (e.g. unsolicited phone calls);
- Repetitive transfers involving massive volumes of data (e.g. the internet); and
- Transfers involving the collection of data in a particular covert or clandestine manner (e.g. internet cookies).

Further to the content of data transfers, the procedural mechanisms are also of relevance to ensure the effectiveness of such rules. Basic principles should be followed to ensure the 'adequacy', such as those defined by the directive: the limitation of the purpose of data processing, the quality of data, the principles of proportionality, transparency and security, the rights of access, rectification and opposition. The Working Group suggested that national authorities of the third country where data are to be delivered should apply the following principles:

- to deliver a good level of compliance with rules with effective/dissuasive sanctions;
- to provide support and help to individual data subjects in the exercise of their rights with a fast enforcement and without prohibitive cost; and
- to provide appropriate redress to the injured party where rules are not complied with, through an independent system of arbitration with compensation and sanctions.

Whenever a member state notices that an adequate level of protection is not provided, it informs the European Commission, which opens an investigation. In this task, the Commission is assisted by a committee, set up by Article 31 of the directive and composed of national officials, but also assisted by a working party, set up by Article 29 of the directive, composed of national

data protection commissioners or independent supervisory authorities. If the results indicate the lack of an adequate level of protection, member states may as a last resort prevent any transfer of data to such country. In practice, the sanction of preventing any data transfer to non-secured countries seems unrealistic and even utopian, considering modern communications networks where a single e-mail could transfer a significant amount of information in just a few seconds. This is but one amongst several examples where the data protection directive was not carefully thought through in the context of the internet, as recognised by the Commission itself during the revision process of the data protection directive.

On the other hand, Article 26 makes possible, if certain limited conditions are met, to transfer data to countries with inadequate levels of protection, whenever the transfer:

- is carried out with the unambiguous consent of the data subject;
- is necessary for the performance of a contract between subject and controller or the implementation of pre-contractual measures in response to the data subject's request;
- 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;
- is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;
- is necessary in order to protect the vital interests of the data subject; or
- is made from a register which, according to laws or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in the law for consultation are fulfilled in the particular case.

The list of exemptions appears to be so broad that it seems unrealistic for a member state or its supervisory authority to check the validity of the transfer.

In addition to this list of exemptions based on the context where the transfer takes place, the directive allows a second category of exemptions: a transfer with a non-secured country could be realised if the data controller itself (e.g. a company) provides safeguards to ensure the protection of the privacy and fundamental rights and freedoms of individuals, resulting e.g. from contractual clauses agreed upon by the European Commission.

The 'Contractual' standard clauses

Contractual provisions binding the receiver of the data are one of the ways of providing the safeguards. It makes a transfer possible whenever the legislative or self-regulatory provisions of a non-EU country cannot themselves ensure an adequate protection.

Due to the development of such initiatives, the Article 29 Group published a list of standard contract clauses that would be integrated into contracts for the transfer of data to third countries. The Working Group reached the following conclusions:

- Contracts with third countries should provide a division of responsibility for data protection compliance between the data controller and the processor;
- Contractual solutions must accept all the basic principles and provide enforcement measures, as is the case for assessing the general level of adequacy in a third country;
- Contractual clauses should detail the purposes, means and conditions of the transfer, limiting the scope of actions for the data recipient in the third country;
- Contracts should ensure that the EU transferring party should be held partially responsible for any damage occurred by the processing of data in the third country;

- The contract must bind bodies and organisations to respect the same data principles;
- Contracts should ensure that recipients of data transfers are subjected to external verification; and
- Contracts should ensure that any complaints experienced are properly investigated.

The Working Group suggested that contractual solutions are probably best suited to large international networks, such as credit cards and airline reservation, characterised by large quantities of respective data transfers of a similar nature, and by a relatively small number of large operators in industries already subject to significant public scrutiny and regulation. Intra-company data transfer between different branches of the same company group is another area in which there is considerable potential for the use of contracts.

In June 2001, the Commission adopted a decision setting out standard contractual clauses ensuring adequate safeguards for personal data transferred from the EU to a non-EU country. The use of standards will be voluntary but will offer companies a straightforward means of complying with their obligations. Clauses contain a legally enforceable declaration whereby both data exporter and data importer undertake to process the data in accordance with basic rules and agree that individuals may enforce their rights under the contract. Standard clauses are neither compulsory for businesses, nor are they the only way to transfer data to third countries. They add simply a new possibility to those already existing in the directive, and analysed above.

Under the decision, supervisory authorities are not allowed to refuse data transfers made under the contractual clauses approved by the Commission.

Appendix 1 of the decision refers to obligations of the data exporter which agrees and warrants that the processing (including the transfer) of data is carried out in accordance with the national law of its establishment. The subject must be informed in case of sensitive data transfers. The exporter must make available to the data subject upon request a copy of the clauses and to respond in a reasonable length of time to any enquiry from the supervisory authority.

On the other hand, the obligations of the data importer are specified as follows:

- S/He has no reason to believe that the legislation applying to him prevents him from fulfilling his obligation under the contract. In the unlikely event of major legal modifications, s/he will notify the data exporter and the supervisory authority.
- He must process the personal data in accordance with the mandatory data protection principles set out in Appendix 2 of the Decision.
- He must deal promptly and properly with the data exporter and the data subject's inquiries and cooperate with the supervisory authority.
- S/He must submit, upon the request of the exporter, his data processing facilities for audit.
- S/He must make available upon request of the data subject a copy of the clauses and indicate the office that handles complaints.

In relation to any data subject damages, the decision establishes a common joint liability between the exporter and importer, and entitles the subject to receive compensation. In case of litigation with the data subject, the exporter and importer agree that the dispute could be submitted to mediation or to courts in the member state in which the exporter is established.

Appendices 2 and 3 to the standard contractual clauses set out mandatory data protection principles, very close to those referred in the directive 95/46.

Finally, with regard to the scope, this decision covers transfers of personal data from a controller established in the EU (data exporter) to a controller established in a third country (data importer), called "controller-to-controller decision".

The Commission prepared another draft decision covering cases of data transfers carried out by a controller established in the EU (data exporter) to a processor (data importer) established in a third country who merely processes personal data as a subcontractor, on behalf of a controller established inside the EU, known as "controller-to-processor decision". The draft decision is awaiting scrutiny by the EP.

Contractual clauses are not necessary for Switzerland and Hungary, which have their own data protection regimes recognised by the Commission as providing an adequate level of protection. At the time of drafting this report, the European Commission recognised the adequacy of the Canadian regime. Negotiations are being carried out with Japan and Australia.

For the United States, specific rules apply.

The Safe Harbour Agreement

In contrast to the EU legislative framework, the US authorities consider that privacy protection is sufficiently ensured by self-regulation, as indicated by the full title of the Safe Harbour Agreement: Elements of Effective Self-Regulation for Privacy Protection.

In order to bridge these different approaches, the EU and the US have been discussing data protection issues and privacy prior to the entry into force of the EU directive. So that the US would not be seen as a 'data haven', the approach has been to attempt to define a 'safe harbour' for personal data. After years of intensive debate, the Safe Harbour Agreement was signed by the EU with the United States in June 2000. The principal motivation was to prevent the possible widespread blocking of data flows to the US following the entry into force of the EU directive.

However, the major gap of the agreement remains the exclusion of data related to financial services. The reason is that the finance sector is not controlled by the US Federal Trade Commission which negotiated the agreement. US financial services firms are facing huge extra costs and bureaucratic burdens to comply with the EU law, whenever they care to do so which in fact is in a minority of the cases.

Nevertheless, according to the London Investment Banking Association (LIBA), personal data handled in the US are: "subject to extensive federal and state legislation concerning confidentiality and security of personal information. In this context, financial data processing is also subject to close examination and regulation by national authorities such as the SEC, the Securities & Exchange Commission". [8]

Despite the high level of processing of personal data in the US, discussions are still being carried out between the Commission (Article 29 Committee) and US counterparts to integrate financial services into the scope of the agreement. In the case where the enlargement of the Safe Harbour Agreement's scope is not possible, the EU officials have already announced that a model contract could be developed. Any company using it is automatically deemed to have met the terms of the EU's strict data privacy code.

In any case, even if financial services continue to be excluded, the current negotiations justify a full explanation of the content of the Safe Harbour Agreement.

The Safe Harbour Agreement:

- provides legal certainty for data controllers in the EU about the directive compliance whenever data are being exported to 'safe harbour' participants in the US;

[8] See LIBA Position Paper submitted to the European Commission in the context of the data protection revision.

- creates a less administratively burdensome framework, ensuring high data protection standards for data transfers to the US; and
- provides guidance to companies and other organisations in the US that want to provide the 'adequate level of protection'.

The Safe Harbour Agreement contains a list of US firms that are self-certified under the Safe Harbour framework. Companies voluntarily join the Safe Harbour by an annual certification to the US Department of Commerce. To qualify, a company can either join a self-regulatory privacy programme that adheres to the Agreement's requirements or develop its own self regulatory privacy policy that conforms to the Safe Harbour Agreement. Companies can therefore implement requirements in a wider contract and add specific clauses. Once certified, companies have to comply with the full list of requirements.

The agreement contains seven major principles with which companies must comply:

- Notice. Companies must notify data subjects of the purpose and use of data collection. Information about the company should also be provided in case of complaints. They must also disclose the identity of third parties having access to data.
- Choice. Companies should allow the subject to choose to op-out in case of disclosure to third parties or in case the use is incompatible with the announced purpose.
- Onward transfer (referring to transfers to third parties). If third parties are acting as an agent, the company that has made a transfer should make sure that the agent subscribes to Safe Harbour principles, or is subject to the directive, or is providing adequate protection.
- Access. Subjects must have access to personal information about them that a company holds and must be able to correct, amend or delete the information whenever it is inaccurate.
- Security. Companies must take appropriate measures to protect personal data from loss, misuse and unauthorised access, disclosure, alteration and destruction.
- Data integrity. Personal information must be relevant for the purposes for which it is to be used. A company should be sure that information is reliable for the intended use and that it is accurate, complete and current.
- Enforcement. Each company has to set up a dispute resolution system, in charge of investigating and resolving complaints. Commitments by companies to adhere to the Safe Harbour Agreement should be assessed. Obligations to repair damage are set up. Sanctions must be sufficiently rigorous to ensure compliance by the company, such as publicity of non-compliance, deletion of data or even suspension of the membership to the Safe Harbour Agreement. Enforcement is taking place in the US and according to the US law. It is carried out, primarily, by the private sector. Individuals have also the option to bring the US company to US courts, e.g. in cases of misrepresentation of a specific statute, such as the Fair Credit Reporting Act, covering situations where financial loss might occur (e.g. refusal of a loan).

Consumer representatives criticised negotiations of the agreement on grounds that it lacked an adequate level of protection and a respective means of enforcement. Amongst several examples, one can mention:

- Restrictive right for consumers to access data held in the US;
- No right to require the deletion of data wrongfully gathered;
- The Safe Harbour Agreement rules disregard the principle of legitimate purpose. Moreover, no clear remedy or effective sanctions for abuse of personal data or privacy;

- US companies are not required to make a public declaration of their commitment to the Safe Harbour principles;
- In the case of takeovers and mergers, the new company is not bound by previous commitments;
- The US based the Safe Harbour Agreement on current US law on data protection, even if there are strong domestic pressures to strengthen it; and
- The enforcement of compliance with the agreement depends on complicated mechanisms, some of which are of doubtful quality.

To summarise the transfer of data to a country outside the EU:

❶ The effort required to verify the presence of an appropriate level of data protection is **incommensurate**. Moreover, in case of inappropriate level, the sanction consisting in preventing the transfer appears to be **utopian, in comparison to actual IT tools**.

❷ The corresponding EU model contracts drafted by the European Commission are **far too complicated** and are only **partially relevant** to the specific characteristics of the credit bureau market.

❸ The Safe Harbour Agreement is based on self-regulation, which is precisely the opposite of the EU approach. Moreover, **financial services are still excluded** from the agreement, even if national authorities and industry consider the US protection level as adequate.

3.2 The EU directive on data protection and telecommunications

Telecommunications and all related recent developments also present serious risks to the privacy of users, despite the fact that the success of such new technology depends on gaining the trust of the consumer.

In this context, and amongst other measures, the EU adopted Directive 97/66 on the processing of personal data and the protection of privacy in the telecommunications sector, with the aim to complete the data protection directive 95/46, as a subsidiary set of rules. This directive applies to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks within the EU. Member states are allowed to take measures to restrict the scope of the rights and obligations of the directive, regarding for example security, phone bills and digital networks whenever such exceptions are necessary for security, defence, public security, criminal offences and investigative reasons.

Telecommunications service providers must take appropriate technical and organisational measures to secure their networks and inform subscribers in case of security breaches.

Member states must prohibit listening, storage, tapping and interception of communications without the consent of the users concerned. This prohibition does not apply to legally authorised recording evidence from commercial transactions or of any other business communication.

This directive had to be implemented by member states by 24 October 1998.

With online services, however, the principle of the ‘purpose limitation’ of the data processing became in practice an exception, rather the rule.

In this context, the European Commission launched in 1999 a communication aiming at a general review of the existing legal framework for telecommunications at EU level.

Furthermore, the EU adopted Directive 2002/58/EC on the processing of personal data and the protection of privacy in electronic communications services with the aim to harmonise the provisions of the member states, required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of such data and of electronic communications equipment and services in the European Community.

With this directive, the EU found a solution to spamming, as it creates an opt-in system for e-mail, faxes and automated calling systems. Users must give prior permission for receiving unsolicited electronic communications for marketing purposes. Member states may adopt measures to restrict the scope of the rights and obligations when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. state security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, as referred to in Article 13(1) of directive 95/46/EC. To this end, member states may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds specified in this directive.

Member states had to transpose the directive into national law by 31 October 2003.

4. Specific EU Measures on Data Protection

We examine below some of the sector-specific EU directives, whose provisions may apply or derogate to the general regime, which often creates problems of inconsistencies.

4.1 The e-commerce directive

As noted previously, the internet is an open network processing vast quantities of personal data. It seems obvious that the processing of personal data undertaken in the context of e-commerce has to be considered in the light of the directives that have already been extensively analysed in this report.

In order to regulate certain legal aspects of e-commerce, the EU adopted Directive 2000/31. Article 14 clearly states that the protection of individuals with regard to the processing of personal data is solely governed by the data protection directives (95/46 and 97/66). Article 14 underlines the fact that the implementation and application of the directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communications and the liability of intermediaries.

The main principle of the directive is the ‘internal market clause’, enabling information society providers to supply services throughout the EU on the basis of the rules and regulations prevailing in the member state in which they are established (home country principle). Several derogations are nevertheless allowed.

The most controversial point of this directive concerns spamming, which is used for marketing reasons. The problem for EU citizens is threefold: first, the collecting of e-mail is most of the time done without their consent; second, they receive a tremendous number of junk mail and unwanted advertising; and third, they bear the cost of connection time to delete those e-mails. According to the data protection directives, personal data must be collected and processed fairly, lawfully and in line with the stated purposes. Processing must take place on legitimate grounds such as consent. Furthermore, the data subject has to be informed and has the right to object to the processing for direct marketing purposes. It thus seems obvious that spamming does not at all respect EU legislation.

In practice, enforcement of such rules is highly difficult. Consumers do not have the illusion that their inbox will be limited to true e-mails, free of spamming, basically because most of the spamming comes from outside the EU, where companies do not care about the EU and are not really prevented from acting due to poor enforcement of EU legislation.

4.2 The e-signature directive

On the internet, and particularly in the context of e-commerce, several ways of entering a signature are possible, such as the insertion of a scanned image of a handwritten signature or a digital signature using public key cryptography. The EU has adopted directive 1999/93, which is technologically neutral, in that it does not privilege any particular type of e-signature. Signatures allow recipients of electronic data to verify their origin and to check that they are complete and unaltered. The aim of the directive is to offer both consumers and businesses new opportunities to exchange information and to trade electronically in a secure way, regardless of borders.

Article 8 enacts some specific data protection rules, requiring that certification service providers and national bodies responsible for accreditation or supervision comply with the requirements of the general data protection directive. Certification service providers may collect private information only directly from the subject and only in so far as it is necessary for the purpose of issuing a certificate.

4.3 The distance marketing directive

In 1997, the EU published Directive 97/7 on the protection of consumers in respect of distance contracts. Article 10 of the directive states that consumers have the right to object to distance communication. However, Article 14 allows member states to introduce or maintain more stringent provisions to ensure a higher level of consumer protection. Curiously, the directive does not mention internet technologies and e-contracts and, moreover, it clearly excludes financial services from the scope of its application.

In order to cover this gap in legislation and to harmonise national regulations, the EU adopted Directive 2002/65 of 23 September 2002 concerning the distance marketing of consumer financial services. This directive aims at setting up common rules on the offer, request, negotiation and conclusion of such contracts, while establishing the fundamental rights of the consumer in this area.

In the context of any distance contract, the directive confers to the consumer:

- A right of information. Before they enter into any contract, consumers must be provided with various information about the supplier, the service, the price and the payment, the delivery and its costs, the formalities of the contract (applicable law, competent court, duration, rights, …);
- a right of reflection, known as “a presale disclosure requirement”, before the conclusion of the contract, for a period of 14 days. Terms and conditions must be communicated to consumers in writing and by durable medium to allow him to take this decision;
- a right of withdrawal for 14 days without incurring any penalty and without the obligation to indicate the grounds for withdrawal;
- a right to be reimbursed, in the event of unavailability of the services, even where sums of money have already been paid; and
- a prohibition on inertia selling (abusive marketing practices seeking to oblige consumers to buy a service they have not solicited).

Regarding the use of spamming and cold calling, member states are called upon to lay down in their legislation one of the following options: under the first option ('opt-in') cold calling and spamming are prohibited unless the consumer has expressly consented; under the second option ('opt-out') this is prohibited only if the consumer has signalled his/her objection, e.g. by entering his/her name on a registry set up for this purpose.

4.4 The Investment Services directive

In 1993, the EU adopted an Investment Services Directive 93/22 aiming to achieve a major step forward on the way to integration of European financial securities markets, through a European passport for investment firms. Based on the mutual recognition of supervision by its home member state, a company could operate EU-wide. However, numerous provisions of the ISD allow host country intervention in the "interest of the general goods", such as the implementation of local code of conducts.

As occurred with the data protection directives, however, the transposition of the ISD into national legislation has not always served and has sometimes seriously undermined the achievement of the express aims of the directive. The major problems with the ISD have been indeed caused by poor implementation and inconsistent interpretation of legislation by member states. In addition to the multiplicity of member state regulatory regimes, certain new technological and economic developments have either frustrated the original purpose of the directive or rendered it outdated.

As a remedy, the Commission proposed in 2000 a Communication aiming at the extension and revision of the ISD to resolve problems in both areas. It suggested that the revision might also be used as an opportunity for the elimination of certain failings in the original text. Further to a consultation process, the Commission proposed a revised document that took into consideration industry's comments.

Two main areas are concerned:

- Making the single passport for investment firms work better: taking in account new forms of services formats based on electronic communications, as well as new king of service providers; and
- Supporting orderly and efficient trading in a world of competing infrastructures.

The Commission is undoubtedly concerned with retail investor protection, namely the provision of complete information, the management of conflicts of interest and the reputation of market participants in sustaining investor confidence. A high level of protection is crucial in its own right, but it is also a pre-condition for the effective operation of the ISD passport.

Until now, no special provision addresses the issue of protecting investor data. Due to the importance of the forthcoming proposal of ISD revision, however, this matter should be closely followed to see whether any specific rule is being drafted or if the proposal simply refers to the general regime.

4.5 The consumer credit directive

As occurred with the data protection directives and the ISD, the consumer credit directive 87/102 is based on minimum harmonisation standards, therefore allowing member states to use and abuse a broad margin of manoeuvre. Obviously, this situation results in 15 different sets of rules.

In the meantime, since the adoption of the directive, the market has had a tremendous evolution at all levels, products and services. Moreover, the EU has adopted other directives, such as e-commerce and distance selling, which are relevant to aspects of consumer credit.

As a consequence, the European Commission presented in September 2002 a proposal for a directive to update the current consumer credit directive.

This time, the Commission defends the maximum harmonisation. As far as data protection is concerned, the proposal aims at the improvement of the circulation of solvency data across borders. This is especially important once related to the concept of 'responsible lending', requiring that credit companies carry out an honest assessment of the consumers' ability to make payments. This concept forces lenders to be more careful when granting loans, as they are simply the best placed to appreciate the risks involved.

The Article 29 Working Group has already delivered an opinion according to which they would in principle prefer either a simple reference to the provisions of directive 95/46 or more elaborate data protection proposals. The proposal in itself does not contain additional provisions to the current data protection regime.

> e.g. The proposal prevents the abuse of data gathered in the context of a judgement of the creditworthiness of a consumer. If collected for that purpose, the data could not be used for marketing reasons. Those data are considered as sensitive from a privacy point of view. The borrower is obliged to disclose all the information when requested by the lender, which has a 'right of access' to solvency data. This last professional must adapt the information and the products according to the client's profile.

Further to this sector-specific analysis, this report draws the following conclusions:

❶ Most of the regulations analysed in this section seems to be **concerned** at least **with the safety and security of consumers' data**. In general, they do not lay down extensive specific rules for privacy and leave, most of the time, the regulation of this matter to the general data protection directives. Nevertheless, some recent legislation derogates to the general framework, creating inconsistencies and new barriers.

❷ UNICE has highlighted this problem. Each of the directives analysed in this section of the report 'may come into play in a single business transaction or each one may be applicable in separate but almost identical business operations that leads to inconsistencies (e.g. opt-on solution for commercial communication as opposed to opt-out in the e-commerce directive)'.

❸ Sector-specific legislation is **burdensome**: a single data protection directive should cover all data protection issues in a consistent manner.

5. The Current Revision of the Data Protection Directive

Article 33 of the directive on data protection requires the European Commission to make regular reports on implementation at national level. This first report has been postponed until now as a result of the delays in the implementation of the directive.

Finally, in 2002, the European Commission launched a broad open consultation on the implementation of data protection legislation consisting of several components: a questionnaire to member states on the transposition of the directive, another questionnaire to national data protection authorities on the practical application of the directive, a call for comments to

stakeholders (public and private sector) and finally, an on-line survey addressed to data controllers and subjects. Based on this consultation process, the European Commission published in May 2003 its first report attesting that the 1995 data protection directive has broadly achieved its aim of ensuring strong protection for privacy while making it easier for personal data to be moved around the EU. However, late implementation by member states and differences in the ways the directive is applied at national level have prevented Europe's economy from getting the full benefit of the directive.

The Commission's id report does not imply that the text of the directive will be modified in any way. The Commission indeed recognised that it is premature to initiate a new legislative process, as there is a lack of sufficient experience in the implementation from Members States. Rather than modifications to the current regime, the Commission would prefer a correct implementation in all member states. The report proposes a work plan to reduce those differences, based on cooperation among member states and between member states and the Commission, followed by a review in 2005 of whether amendments to the directive are necessary.

The analysis of our paper has demonstrated several problems in applying the directive. The report published by the European Commission sums up and systematises them.

5.1 The late transposition of the EU directive

Although the directive set the deadline of October 1998 for its implementation, most of the member states were late in transposing it, and most national legislation only came into force in 2000 or even 2001.

In two countries (France and Ireland), the process of implementation is not even finished, while Luxembourg's new legislation entered into force by 2003!

The European Commission took several member states to court for non-compliance with the obligation to transpose the directive (France, Luxembourg, the Netherlands, Germany and Ireland).

The Article 29 Working Party recalled that "not all member states have implemented the directive in time. The consequence of this delay is the continuation of the existence of divergent regimes that maintains legal uncertainty as regards the obligations of controllers of personal data such as business and administration, as well as the rights of individuals".[9]

It should be recalled that the Stockholm European Council (spring 2001) set a maximum target of 1.5% for the implementation deficit of member states regarding Internal Market legislation. The last scoreboard reached the conclusions that the EU is still far from this target and put the spotlight on technical barriers that persist, holding back the overall economic performance.

5.2 The diverging national implementation

Article 8 states that "the level of protection must be equivalent in all member states". However, the next article provides member states with a margin of manoeuvre, recognising that "within the limits of this margin of manoeuvre and in accordance with EU law, disparities could arise in the implementation of the directive, and this could have an effect on the movement of data within the member state as well as within the Community".

One of the major concerns of the directive is precisely the lack of uniformity in the implementation by member states. Member states have failed to adopt consistent implementing

[9] Article 29 Working Party, Fifth Annual Report (2000), March 2002.

legislation for the directive, which has resulted in legal uncertainty and unnecessary extra costs and burdens for business operating across the Single Market.[10]

The present paper has tried to elucidate the issues surrounding the wrongful or divergent implementation carried out by national legislation, such as the processing of categories not requiring notice to or registration with national authorities, standards and fees for access to data at the request of data subjects, difference in judicial recourse for non-compliance, differences in approval requirements for cross-border data flows, …. With so much disparities, the present situation runs against the basic principle of harmonisation.

In his closing remarks at the EU conference on the review of the directive, Commissioner Frits Bolkestein summarised the situation by stating that: "Divergences in data protection legislation and the way it is applied in the member states are in fact creating problems for the free movements of data. These difficulties damage the competitiveness of our enterprises, because they are prevented from operating effectively on a EU scale (…) it makes no sense to invest huge efforts in developing an ambitious programme to create a Single Market for financial products and services in the EU, just to discover that the idea of European products or services trips up on obstacles that prevent companies from running personal databases on a EU basis".

Once the diagnosis is done, it's time to focus on the adequate treatment. The directive has to be much clearer and stronger in order to prevent member states from over-stretching the margin of manoeuvre. The problem is endemic at EU level: a directive contains too many prescriptive rules and very little proper enforcement.

But, before thinking about amending the EU data protection directive in concrete terms, it should be first examined whether application problems might not be solved by proper implementation of existing provisions. Even if the directive is far from being perfect, all shortcomings experienced are not primarily caused by the directive itself, but mainly because of national implementation.

Therefore, the industry is of the opinion that the European Commission needs to analyse national implementation (in detail), highlighting to what extent national rules conform with the EU framework. In case of any deviation, opposition or wrong interpretation, national law should be modified and brought into line with EU provisions. "There must be a level playing field in the area of data protection legislation; companies and citizens must be able to rely on finding the same data protection standards throughout Europe".[11] The European Commission needs to exert its influence for a high EU data protection legal environment, so as to prevent EU standards from differing too much at national level.

5.3 The ever-evolving development of information society

As the internet is based on a dynamic architecture, in a perpetual movement, it appears totally unreal to regulate systematically after any new IT development. It's a race the regulator will never win.

Therefore, any recent high and effective standards of protection need to take account of the latest technological developments.

[10] The International Chamber of Commerce (ICC), Position Paper to the European Commission on the Consultation process on the Data Protection directive.

[11] Bundesverband Deutscher Banken (BDB), Position Paper to the European Commission on the Consultation process on the Data Protection directive.

In this context, the internet should be directly constructed bearing in mind data protection objectives. Although technology progress may result in lack of privacy, technology can also be used by regulators to protect personal data.

From being part of the problem, it could be used as part of the solution. The EU policy is precisely going in this direction, with measures to promote research programmes and investigations.

5.4 The unworkable international transfers system

Member states show difficulties with the interpretation of Articles 25 and 26. With cross-border operations, the problems are caused by the fact that a variety of supervisory authorities are involved. The industry suggests a more flexible regime for international data transfers, in a pragmatic and practical way, particularly in relation to transfers within multinational companies. Therefore, it makes sense to insist that the supervisory authority of the company's head office hold sole responsibility for cross-border operations within the EU territory, as an application of the country of origin principle.

Rules on the transfer of data to third countries are extremely restrictive and obstruct any form of cooperation, particularly in the case of a group of companies and subsidiaries, established all over the world.

There are a request for alternative model contracts being authorised by the Commission and new development in the field of company codes of conduct. UNICE has suggested that it should be for the data controller to determine the adequacy of the code, and that there is no need for such code to be presented for the individual approval of each member state, as is presently the case. It should be possible to transfer data from the entire EU territory once it is demonstrated that the legal requirements of a single member state have been satisfied.

Moreover, there is a lack of consistency in relation to contractual terms. Some countries, such as the Netherlands, require companies to obtain a license for data export even when the Commission's model contract is being used and is unamended.

❶ The results of this consultation were integrated into the European Commission's report on how the data protection directive is being applied.

❷ As previously stated, further to the current consultation, the Commission does not intend to modify the directive, and neither do the industry sector and the majority of member states. However, four member states (UK, Finland, Austria and Sweden) have presented a position paper requesting explicit amendments to the current regime. The aim is to cut red tape, facilitate cross-border transfers and remove bureaucratic requirements.

6. Overall Conclusions

In its Consumer Policy Action Plan for 1999-2001, the European Commission stated that "of all developments in the information society, e-commerce has the potential to most profoundly change the relationship between business and consumers and the nature of consumption itself". More and more firms and bank retailers are offering their services on the internet, attracting an ever-increasing number of clients to experience the advantages of a borderless environment. Consumers are offered convenience, speed and global choice in services, goods and more importantly, prices. The relationship between consumers and business will never be the same again.

Simultaneously, however, enhanced possibilities to communicate and to do business give rise to concerns as to the protection of consumers, such as in the areas of marketing, privacy and payment.

In this context, data protection is a precondition for the development of e-commerce. All surveys carried out recently agree on the importance attached by consumers to the protection of personal data. Users would make greater use of the internet if confidentiality were protected more effectively.

In regards to the EU data protection directives, the major difficulties were to find the appropriate balance between, on one side, measures to promote the implementation of the Single Market through the free movement of information and, on the other hand, the protection of fundamental rights and freedoms belonging to human persons. In this context, IT became the real hobby-horse of the EU as the information society is precisely the "*carrefour*" of two major concerns: the need to bring all citizens into an integrated union and the necessity for its industry to compete in a world-scale economy.

Previous to any adaptation of familiar solutions to on-line services, it is important to consider the level of regulation with which the new rules can be best shaped: either through new legislation or self-regulation. Indeed, the redaction of codes of conduct must not be underestimated as a solution for data protection in the context of the internet. More flexible and closer to the US approach, codes of conduct could play a crucial role.

From a normative point of view, the report offers evidence that the EU legislative framework on data protection provides EU consumers with a reasonable level of security, either inside and outside the European area. directives reinforce consumer confidence by stipulating rights to be observed by providers, under the control of supervisory authorities. In this context, "this regulation is facilitating the development of the internet, as providing a sufficient degree of public confidence in the legal protection of privacy and security of on-line consumers" (see LÜDI case – Judgment of the ECJ – 1992). In parallel, it also appears that numerous rules of the traditional legal framework are still equipped to function properly in the on-line world and that the well-known guiding principles of the European Court of Justice are apt to protect consumer interests in the internet environment.

Unfortunately, considerable obstacles remain to an effective implementation and harmonisation of data protection law in the EU.

First, many member state transposed the EU directives clearly after the deadline. In some of them, the legislative process is still in progress.

Secondly, once implemented (in due time or not), harmonisation is missing. National legislation differs so much from one member state to another that new additional obstacles to the internal market are emerging. Those disparities between national laws are explained by the differences in how member states approach privacy, but mainly by the room of manoeuvre allowed to them regarding the implementation of several important provisions, such as the treatment of sensitive data and the transfer of data, inside and outside the EU territory. This situation leads directly to a lack of transparency and legal certainty. According to ACCIS, the Association of Consumers Credit Information Supplier, "we remain firmly convinced that the EU data protection directive allows the individual countries sufficient freedom to apply the directive in accordance with the practical requirements posed by their specific national situations". Variations in national practices and traditions, coupled with derogations and exceptions to the current regime, are inhibiting efforts of harmonisation.

Further to the EU directive, multinational companies are still obliged to comply with several national laws in place of one single regime. It's clearly evidence that the aim of the EU norm is

far from being achieved. From all the discrepancies, the notification procedure is the most unacceptable for industry. As applied by member states the regime results in an increase of costs and administrative red tape.

Third, the possibility to grant an effective enforcement of the data subject's rights. This lacunae seems to be confirmed by the powers granted to the Commission to make proposals for amendments with regard to the implementation of the directive.

Fourth, data transfers to third countries' regimes are not appropriate and are not easily enforceable. As an alternative, contractual clauses remain too complicated. Finally, the Safe Harbour Agreement simply excludes financial services. In a word, the directive does not provide full protection all over the world. The directive grants people protected by the directive with the guarantee to maintain an adequate level of protection for transfers not covered.

Fifth, a number of loopholes are also left by the directive with regard to the protection of personal data in open networks. If most of the regulation applying to data protection in the traditional market are not efficiently implemented and enforced, the situation in the e-market could become even worse. The report, therefore, concludes that several provisions introduced by the directives appear even less effective in an internet environment. Online consumers do not, in practice, have the same degree of privacy protection as offline consumers. Regulation can be especially ineffective in the virtual world. The internet spans the globe, and regulation by single country, or even a group of nations, is often less effective because there are alternative geographic channels for information and technology. The EU directive is indeed limited to an EU level, but even if EU standards are harmonised, it is unlikely that the same standards will be adopted around the world. The EU still has to persuade third countries that the EU model of legislation is the most appropriate to protect private data.

Sixth, the multiplication of sector-specific legislation derogating to the general framework creates, once again, additional inconsistencies in efforts to complete the Internal Market.

In the context of the current revision process, if the Commission takes the initiative to amend the actual regime, member states will take again a couple of years for the transposition and the subsequent implementation. In the meantime, however, the inadequacies are still present and demand an immediate solution.

In sum, whilst moderate progress has been made at regulatory level, tremendous advances in technology and continuing variations in national responses remain major obstacles to achieving data protection equivalence, both within the EU and in third countries.

7. Recommendations

This report concludes that the vulnerabilities of information systems are growing faster than our ability and willingness to respond to them. Cyber security today is far worse than what known-best practices can provide.

Much improved security would be possible today if technology producers, operators of critical systems, and users took appropriate steps. Therefore, all on-line actors are strongly recommended to take measures to increase the level of data protection. To take the maximum advantage of the Internal Market, these challenges to the protection of data privacy raise two sets of options.

First of all, there is technological approach to integrate the privacy directly into the new IT developments with the consequence of minimising any obstacles. Alternatively, there is the regulatory approach to implementing and updating current legislation.

From the consumers' point of view, each user should:

- ensure that adequate security tools are available, to train in their use and to dedicate enough time to security concerns;
- use systematically encryption programmes;
- test frequently the current security systems;
- communicate any vulnerability noticed to supervisory authorities when using systems or programmes; and
- make pressure on industry to turn available more safety products;

From the IT industry point of view, the sector should:

- create and adapt products according to the need and the development of risks (e.g. warning information whenever transmitting information in an insecure environment);
- develop easy-using products being able to be used for all king of public;
- incorporate privacy preferences into the internet browser technologies which, combined with labelling and filtering of website information practices, can assure respect for data protection;
- limit the use of cookies by asking the prior consent of consumers;
- build encryption solutions that could be easily implemented.

Finally, from the regulators point of view, the EU legislator should:

- use voluntary Codes of Conducts to assess on technical issues;
- legislate “quality labels” for on-line service, which should be considered to restore the confidence of the consumers;
- allow member states to grant certain legal and tax advantages to web sites voluntary accredited to quality labels;
- speed up the legislative process to follow closely IT developments;
- reduce margin of manoeuvre to implement differently EU provisions;
- set up effective infringement procedures in case of non-compliance and non implementation of EU rules by member states;
- launch advertisement campaigns to aware EU consumers on privacy issues.

Therefore, for the on-line environment, the most effective approach for fair information practices will combine substantive data protection rules and principles with technical arrangements that allow the most efficient and least intrusive compliance.

Selected References

Articles

Bischoff, Pierre (1998), "L'Union Européenne et la protection des données: la société de l'information à l'épreuve des droits de l'homme", *Revue du Marché Commun et de l'Union Européenne*, No. 421, September, pp. 537–552.

Boulanger, Marie-Hélène, Cécile Terwangne, Thierry Leonard, Sophie Louveaux, Damien Moreau and Yves Poullet (1997), "La protection des données à caractère personnel en droit communautaire", *JTDE*, June, pp. 121–127, 145–155, 173–179.

Brühann, Ulf (1999), "La protection des données à caractère personnel et la Communauté Européenne", *Revue du Marché Commun et de l'Union Européenne*, No. 428, May, pp. 328–341.

Carey, Peter (2000), "E-commerce: does the Data Protection Act 1998 apply to offshore e-business?", *Computers & Law*, August/September, Vol. 11, pp. 23–25.

France, Elisabeth (1997), "Can Data Protection survive in cyberspace?", *Computers & Law*, June, pp. 20–24.

Hadfield, Gillian K., Robert Howse and Michael J. Trebilcock (1998), "Information-based principles for rethinking consumer protection policy", *Journal of Consumer Policy*, June, pp. 131–169.

Kelleher, Denis and Karen Murray (1999), "IT law in the European Union", *Sweet & Maxwell*, London.

Kronke, Herbert (1998), "Applicable law in torts and contracts in cyberspace", in Boele-Woelki, Katharina and Catherine Kessedjian, *Internet Which court decides? Which law applies? Quel tribunal décide? Quel droit s'applique?*, Kluwer Law International, Cambridge, pp.65–87.

McBride, Jeremy (2001), "Disclosure of crime prevention data: specific European and international standards", *European Law Review*, pp.86–102.

Millard, Christopher (1999), "Data Protection and the internet", *Computers & Law*, February/March, Vol. 9, pp. 29–35.

Monti, Mario (1998), "The Internet and privacy: what regulation?", Rome, 9 May.

Osborne, Dawn (2000), "Jurisdiction on the internet – not such a barrel of laughs for Euromarket", *Computers & Laws*, August/September, Vol. 11, pp. 26–27.

Pearce, Graham and Nicholas Platten (1998), "Achieving Personal Data Protection in the European Union", *Journal of Common Market Studies*, Vol. 36, No. 4, December, pp. 529–547.

Rothchild, John (1998), "Making the market work: enhancing consumer sovereignty through the telemarketing sale rule and the distance selling directive", *Journal of Consumer Policy*, September, pp. 279–313.

Rowland, Diane and Elizabeth MacDonald (1997), *Information Technology Law*, 2nd edition, London: Cavendish Publishing.

Seaman, Adrienne (1999-2000), "E-commerce, jurisdiction and choice of the law", *Computers & Law*, December/January, Vol. 10, pp. 28–30.

Singleton, Susan (1995), "The Data Protection directive", *Europe Bulletin*, Croner CCH, October, pp 3–16.

Singleton, Susan (1998), "The database and Data Protection directives", *Europe Bulletin*, Croner CCH, March, pp 3–15.

Singleton, Susan (2000), "Distance selling Regulations", *Europe Bulletin*, Croner CCH, May, pp. 3–15.

Swetenham, Richard (2000), "Le plan d'action pour une utilisation plus sûre d'Internet", *Revue du Marché Commun et de l'Union Européenne*, No. 436, March, pp. 160–167.

Swire, Peter P. and Robert E. Litan (1998), *None of your business – World Data Flows, Electronic Commerce, and the European Privacy directive*, Brookings Institution Press, Washington, D.C.

Thomas, Douglas and Brian D. Loader (2000), *Cybercrime: law enforcement, security and surveillance in the information age*, Routledge, London.

Waixel, Robert (2000), "Successfully Managing the new Data Protection laws", *Computers & Law*, August/September, Vol. 11, Issue 3, pp. 34–36.

Official documents

BEUC, Bureau Européen des Unions de Consommateurs, *«Protecting the Privacy of European Consumers in a Global Environment. Comments on the EU-US Safe Harbour Negotiations»*, Brussels, February 2000.

Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, Strasbourg, 1981.

Council of Europe, Recommendation n° R(90) 19 on Protection of personal data used for payment and other related operations, Strasbourg, 13.09.90.

Council of Europe, Recommendation n° R(95) 13 on problems of criminal procedure law connected with Information technology to member states, Strasbourg, 11.09.95.

Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJCE, L. 012, 16.01.01, pp. 1–23.

Directive 87/102 of the European Parliament and of the Council of 22 December 1986 on the approximation of laws, regulations and administrative provisions of the member states on consumer credit, OJCE, L. 42, 12.02.87, pp. 48–53.

Directive 91/308 of the European Parliament and of the Council of 10 June 1991 on the prevention of the use of the financial system for the purpose of money laundering, OJCE, L. 166, 28.06.91, pp. 77–83.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJCE, L. 281, 23.11.95, pp. 31–50.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJCE, L. 077, 27.03.96, pp. 20–28.

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, OJCE, L. 144, 04.06.97, pp. 19–27.

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJCE, L. 024, 30.01.98, pp. 1–8.

Directive 99/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and guarantees, OJCE, L. 171, 07.07.99, pp. 12–16.

Directive 1999/93 of 13 December 1999 on a Community framework for electronic signatures, OJCE, L. 13, 19.01.00, pp. 12–20.

Directive 2000/12/EC of the European Parliament and of the Council of 20 March 2000 relating to the taking up and pursuit of the business of credit institutions, OJCE, L. 126, 26.05.00, p. 1–59.

Directive 2000/31 of 8 June 2000 on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market, OJCE, L. 178, 17.07.00, pp. 1–16.

Directive 2002/58 of 12 July 2002 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJCE, L 201, 31.07.02, pp. 37–47.

Directive 2002/65/EC of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council directive 90/619/EEC and directives 97/7/EC and 98/27/EC, OJCE, L 271 , 09.10.02, pp. 16–24.

European Commission, COM (1993) 700 final, White Paper on Growth, competitiveness and employment: the challenges and ways forward into the 21st century, 05.12.93.

European Commission, COM (1994) 347 final, Communication on the Europe's way forward to the Information Society, 19.07.94.

European Commission, COM (1997) 157 final, Communication on an European initiative in electronic commerce, 16.04.97.

European Commission, COM (1997) 503 final, Communication on Ensuring security and trust in electronic commerce, 18.10.97.

European Commission, COM (2000) 385 final, Proposal for a directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, 12.07.00.

European Commission, COM (2001) 497 final, Decision on Standard Contractual Clauses for the transfer of personal data to third countries under directive 95/46/EC, 15.06.01.

European Commission, Recommendation concerning transactions by electronic payment instruments and in the relationship between issuer and holder, OJCE, 30.07.97, L. 208, p. 52.

European Commission, *« On-line services and Data Protection and the protection of privacy: part one – Description of the general situation, part two – case studies »*, Annex to the Annual Report 1998 (XV D/504/98) of the Working Party established by Article 29 of directive 95/46/EC, Vol. I.; *« On-line services and Data Protection and the protection of privacy :Regulatory responses »*, Vol. II., Office for Official Publication of the EC, Luxembourg, 1999.

European Commission, *« Working document on privacy on the Internet – An Internet EU approach to on-line Data Protection »*, adopted by the article 29 Data Protection working party, 21.11.00.

European Commission, *« Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons »*, Final Report, Cambridge, Oct. 1998.

European Parliament, *«The impact of rapid technological change in information technology on the stability of world trade and international cash flows»*, WD for the STOA panel, Luxembourg, Feb. 2000.

OECD, Guidelines on protection of privacy and transborder flows of personal data, Paris, 1981.

OECD, Recommendation of the OECD Council concerning guidelines for consumer protection in the context of Electronic commerce, Paris, 09.12.99.

OECD, « Electronic Finance: Economics and Institutional Factors », Financial Affairs Division, Occasional paper, N°2, Paris, Nov. 2001.

TACD, Trans Atlantic Consumer Dialogue, *«Submission of the Trans Atlantic Consumer Dialogue (TACD) concerning the US Department of commerce draft international safe harbor privacy principles and FAQS»*, 15.03.00.

Web sites

www.privacy.fgov.be : site of the Belgium national authority on Data Protection

www.dataprotection.gov.uk : site of the British national authority on Data Protection

www.export.gov/safeharbor/sh.html : site of the US Department of Commerce

www.epic.org : site of the Electronic Privacy Information Centre

www.privacylaws.com : site of the Privacy Law & Business

www.cstb.org : site of Computer Science & Telecommunications Board

http://europa.eu.int/comm/internal_market/privacy/lawreport/paper_en.htm: site of the European Commission Revision process on the Data protection directive. All the Position Papers, comments and contributes received in the context of the revision process are present there. All the Position Papers coming from the Financial Services & Banking industry and consumer lobbies, used as arguments in the present Paper, can be red in the same place.