AN ASSESSMENT OF THE TURKISH DRAFT LAW ON PROTECTION OF PERSONAL DATA IN LIGHT OF THE EU DATA PROTECTION DIRECTIVE

Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi

Nurullah TEKİN *

ABSTRACT

The protection of personal data is recognized as a fundamental right in several European and international treaties, closely linked to but different from the right to respect for private and family life. Various directives deal with personal data usage in the European Union, but the most inclusive is the EU Data Protection Directive which protects individuals' privacy and personal data use. Despite such gradually increasing sensitivity on protection of personal data, there is not yet a specific law governing personal data privacy in Turkey, though other pieces of legislation refer to the protection of personal data. There is also a draft Law on Protection of Personal Data, which was prepared and developed by the Turkish Ministry of Justice for several years without success. In this the EU Data Protection Directive will be explained in detail. Thereafter, the state of play of this issue in Turkey and the question of why it needs a specific data protection law will be clarified. Finally, the Draft Law on Protection of Personal Data will be comparatively assessed and criticised.

Key Words: Personal Data, Information, Privacy, EU Data Protection Directive, Draft Law on Protection of Personal Data

ÖZET

Kişisel verilerin korunması, birçok uluslararası anlaşmalarda özel hayata ve aile hayatına saygı hakkı ile yakından ilgili ancak ondan farklı olarak, temel hak şeklinde düzenlenmiştir. Avrupa Birliği içerisinde çeşitli direktifler kişisel verilerin kullanımını düzenlemektedir, ancak bunlardan en kapsamlı olanı, bireyin mahremiyetini ve kişisel

* Judge, Ministry of Justice, Directorate General for EU Affairs, LL.M in University of Essex/the United Kingdom, PhD student in Istanbul University/Turkey, nurullah.tekin@adalet.gov.tr

verilerin kullanımını koruyan 'AB Veri Koruma Direktifi'dir. Kişisel verilerin korunmasına ilişkin giderek fazlalaşan bu hassasiyete rağmen, Türkiye'de kişisel veri gizliliğini düzenleyen bir kanun henüz, bazı mevzuat bölümleri kişisel verilerin korunması ile ilgili olmasına rağmen, yoktur. Adalet Bakanlığı tarafından birkaç yıldır hazırlanan ve geliştirilen ancak başarıya ulaşmamış bir "Kişisel Verilerin Korunmasına Dair Kanun Taslağı" vardır. Bu çalışmamızda, AB Veri Koruma Direktifi ayrıntılı bir şekilde anlatılmakta, Türkiye'deki mevcut durum ve bağımsız bir kişisel verilerin korunması kanununa neden gereksinim duyulduğu açıklığa kavuşturulmaya çalışılmaktadır. Son olarak da, Türkiye'deki 'Kişisel Verilerin Korunmasına Dair Kanun Tasarısı' karşılaştırmalı olarak incelenmekte ve buna göre kritiği yapılmaktadır.

Anahtar Kelimeler: Kişisel Veri, Bilgi, Mahremiyet, AB Veri Koruma Direktifi, Kişisel Verilerin Korunmasına Dair Kanun Tasarısı

♦♦♦♦

SECTION I

I. INTRODUCTION

We live in a complex, 'information age'. The digitalization of information, coupled with incredible technological development, has increased the volume of data exponentially. The application of information has changed too, since most information is now shared internationally, much of it related to individuals. Indeed, personal information and data is essential to everyday life. Our wallets are filled with credit and debit cards, phone cards and store cards which can all be used to record where we are and what we do. Each day, incredible quantities of information are processed by an equally incredible array of machines for an almost limitless amount of purposes. Data protection law aims to protect individual right to privacy by regulating the collection, use and dissemination of such personal information.

The protection of personal data is recognized as a fundamental right in several European and international treaties, closely linked to but different from the right to respect for private and family life. The development of new information technologies and most particularly the Internet over the past few decades has engendered concerns about the security of personal data. The storage and

transfer of personal data had never been easier than today. In Europe, where this issue receives the most concerted attention in the world, the response is found in 'data protection law'. This term refers to the legal structures that attempt to regulate knowledge and concealment of personal information. Various directives deal with personal data usage in the European Union (EU), but the most inclusive is the EU Data Protection Directive 95/46/EC which protects individuals' privacy and personal data use. The EU Directive represents the most sweeping and influential legislative framework concerning this issue. Although the provisions of the Directive have not been able to keep pace with the technological developments and new emerging threats to privacy, the Directive, which is currently under revision, still constitutes one of the most advanced legal frameworks in the field of data protection worldwide.

In many countries around the world, there is a data protection law which broadly governs the collection, use and dissemination of personal information by both the public and private sectors. There is an upward trend towards the enactment of comprehensive privacy and data protection laws around the world. Despite such gradually increasing sensitivity on protection of personal data, there is not yet a specific law governing personal data privacy in Turkey, though other pieces of legislation refer to the protection of personal data. There is also a draft Law on Protection of Personal Data, which was prepared and developed by the Turkish Ministry of Justice for several years without success.

This study will be organised into three sections. The first section illustrates the terminology regarding the protection of personal data and retails the situation of this concept in international instruments giving its historical background. In the second section, the EU Data Protection Directive, its scope and principles will be explained in detail, with a general overview of the protection of personal data in the EU. Thereafter, the proposed EU Data Protection Regulation will be described in general terms. Finally, in the last section, the state of play of this issue in Turkey and the question of why it needs a specific data protection law will be clarified. Finally, the Draft Law on Protection of Personal Data will be comparatively assessed and criticised.

II. PROTECTION OF PERSONAL DATA

A. TERMINOLOGY

1. DATA AND INFORMATION

It should be noted at the beginning that it is really necessary to distinguish between the concept of data and information. The development of a unified and coherent model that defines data and information is far from a straightforward task. Attempts to resolve this issue in the general case, e.g. to answer questions such as 'What is knowledge?' and 'What is information?' has been a great problem for philosophers and scientists for a long time[1].

Data and information are related to each other but they differ in many ways especially in their meanings. Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized. But when data is processed, organized, structured or presented in a given context so as to make it useful, it is called 'information'[2]. For example; while each student's test score is one piece of data, the school's average score is the information that can be concluded from the given data. Data is unprocessed instructions, once processed it becomes information. Similarly, the depth of Lake Van is generally considered to be 'data', but a book on its geological characteristics is 'information'. It should be clear from these examples that 'information' is factual and reliable since it is backed by research from experts such as scientists and researchers[3].

2. PRIVACY AND DATA PROTECTION

Before beginning, it should be stated that while privacy and data protection might seem synonymous at first sight, actually, they are twins[4]. Privacy has al-

---

1 Aamodt Agnar and Nygard Mads, *Different roles and mutual dependencies of data, information, and knowledge - an AI perspective on their integration*, Data and Knowledge Engineering, Volume:16, Issue:3, 1995, p.193

2 Morley Deborah and Parker Charles, *Understanding Computer: Today and Tomorrow*, 14th Edition, 2013, p.11

3 Zins Chaim, *Conceptual Approaches for Defining Data, Information, and Knowledge*, Journal of the American Society for Information Science and Technology, Volume:58, Issue:4, 2007, p.486

4 Kuner Christopher, *European Data Privacy Law and Online Business*, Oxford University

ways been an important issue of research and analysis. The idea of what should be kept private and what kind of regulation is reasonable to overcome threats to privacy have been at the centre of debate for many decades. However, as we transfer from an industrial to an information society, the status of privacy as a right of great importance for individuals is further highlighted[5].

Privacy is perhaps one of the most difficult notions to determine a framework and define of all the human rights in the international catalogue. There is no consensus on a uniform definition of privacy that encompasses all attributes of the term amongst scholars and courts. Privacy definitions have focused on autonomy rights, information control, or control over intimate information[6]. Other attempts define privacy through a set of interrelated features or through a personal perspective. Several privacy explanations have opened debates as to whether privacy is a value in itself or solely a means of achieving other ends[7].

The term privacy is defined as "the state in which one is not watched or disturbed by others". As far as the origin of the word is concerned, it stems from the Latin word privatus, which means "withdrawn from public life"[8]. Privacy is a concern that obviously precedes modern technology. It is like freedom: we don't appreciate its dignity and importance until it is threatened, or until we lose it[9].

The right to privacy can be seen in many European national constitutions. For instance, Germany embedded the right to what it defines as 'dignity and freedom of personality' in its constitution. Spain's constitution went a step

Press, 2003, p.3

5 Koutsias Marios, *Privacy and Data Protection in an Information Society: How Reconciled are the English with the European Union Privacy Norms?* Computer and Telecommunications Law Review, Volume:18, Issue:8, 2012, p.261

6 Bygrave Lee, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, London, Kluwer Law International, 2002, p.129

7 Rempell Scott, Privacy, *Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant V Financial Services Authority as a Paradigm of Data Protection Nuances And Emerging Dilemmas*, Florida Journal of International Law, Volume:18, 2006, p.811-812

8 *Compact Oxford Thesaurus*, Oxford University Press, 2009, p.704

9 Flaherty David H, *On the Utility of Constitutional Rights to Privacy and Data Protection*, Case Western Reserve Law Review, Volume:41 Issue:3, 1991, p.831

further to include a right to privacy in electronically stored data[10]. Privacy is recognised as a fundamental human right by several legal instruments, including the Universal Declaration of Human Rights and the European Convention on Human Rights (ECHR). Privacy regulations aimed at governing how personal data is processed were introduced in the 1970s and 1980s, and the EU Directive[11].

As for data protection, it is easier to define than privacy because data protection focuses on informational rights. It is often assumed to be a technical term relating to specific information management practices. In contrast is more likely to be considered as a fundamental right and accorded specific protection under human rights conventions and constitutions[12]. Although definition of data protection is easier than that of privacy, setting forth the appropriate purposes for data protection provokes an equally wide-ranging discussion as seen with the given purposes for protecting privacy. Many European data protection initiatives have a human rights grounding, which include the right to privacy and other conventional fundamental freedoms such as freedom of thought, protection of liberty and the right to self-determination[13].

This is further complicated by the fact that literature and academic sources use the terms interchangeably. In US legal theory, 'informational privacy' refers to 'data protection' or 'privacy', which clearly fails to clarify the distinction. In Europe meanwhile, 'data protection' is a term separate from 'privacy', as it is concerned with the control of gathering and use of personal data to protect privacy itself. Indeed, privacy, in this regard, is a larger concept, with data protection merely a specific subset[14].

"The protection of privacy is a fundamental right that is primarily protected

---

10 Monahan P. Amy, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, Law & Policy in International Business, Volume:29, p.283

11 Robinson Neil and others, *Review of the European Data Protection Directive*, RAND Corporation, sponsored by Information Commissioner's Office, May 2009, p.1

12 Rowland Diane and Macdonald Elizabeth, *Information Technology Law*, Routledge-Cavendish, Third Edition, 2005, p.303

13 Supra note 7, p.813

14 Supra note 5, p.266

by Article 8 [ECHR] and subsequent provisions within the framework of the [EU]. The concept of protection of personal data contains basic principles to protect the data subject. On the one hand, the concept of personal data protection is narrower than privacy since privacy encompasses more than personal data. On the other hand it encompasses a wider area, since personal data are protected not only to enhance the privacy of the subject but also to guarantee other fundamental rights such as the right not to be discriminated[15]."

The European Court of Human Rights (ECtHR) plays an essential role concerning the protection of the right to privacy in Europe. During the last few decades the ECtHR, which has the power to make rulings about violations of Article 8 of the ECHR, has developed a vast and relevant but not unequivocal body of case-law about privacy[16].

B. HISTORICAL BACKGROUND IN CONTEXT OF SOME INTERNATIONAL REGULATIONS

Data protection has been a primary concern for fifty years. The first significant international discussion of data protection law took place in 1968 at the United Nations (UN) International Conference on Human Rights. In the aftermath of that conference, data protection and privacy have attracted widespread domestic and international debate and legislative action, particularly in Europe[17]. The first general data protection statute was enacted by the West German state of Hesse in 1970, and then Sweden followed in 1973 with the first national statute. Other European countries followed their example, and in North America both the United States (US) and Canada developed general and quite comprehensive data protection legislation. It became apparent to those

15 European Data Protection Supervisor, *Public Access to Documents and Data Protection*, Background Paper Series No.1, July 2005, p.15, http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Papers/BackgroundP/05-07_BP_accesstodocuments_EN.pdf, accessed on: 15.06.2013

16 De Hert Paul and Gutwirth Serge, *Privacy, Data Protection and Law Enforcement, Opacity of the Individual and Transparency of Power,* in Privacy and the Criminal Law, Claes Erik, Duff R. Antony and Gutwirth Serge (editors), Oxford, 2006, p.61-62

17 Cate Fred, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, Iowa Law Review, Volume:80, 1995, p.431

concerned with data protection, however, that it could not be achieved merely with national legislation[18].

There was an essential requirement of the efforts of a universal organisation which could coordinate and organize the drafting of international legal instruments. In this regard, the two organisations which initiated transnational legal instruments in the area of data protection were the Council of Europe (CoE) and the Organization for Economic Cooperation and Development (OECD). These organisations are well suited to deal with legal issues with regard to national policies or international trade, although not equipped to discuss technical standards or other problems directly related to telecommunications technology. The CoE and OECD approached the issue from very different perspectives, reflecting the different purposes of the two organizations[19]. Finally, the UN published Guidelines for the Regulation of Computerized Personal Data in 1990.

1. OECD

In the 1980s, intergovernmental organizations proposed omnibus guidelines that provided minimum standards for their member nations' data privacy regulatory schemes; because they realized the need for harmonization of international privacy legislation[20]. The OECD promulgated Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data in 1980[21], thus becoming the first intergovernmental organization to publish guidelines in the privacy field. It was clear that the increasing penetration of information technology into economic and social life necessitated such an approach.[22]

---

18 Bing Jon, *The Council of Europe Convention and the OECD Guidelines on Data Protection*, Michigan Yearbook of International Legal Studies, Volume:5, 1984, p.271

19 Supra note 18, p.271-272

20 Barnes Morey Elizabeth, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive,* Northwestern Journal of International Law & Business, Volume:27, 2006, p.174

21 See the full text of the guidelines at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, accessed on: 17.06.2013

22 Godbey Briana N, *Data Protection in the European Union: Current Status and Future Implications*, A Journal of Law and Policy, Volume:2, Isuue:3, 2006, p.818

By formulating basic principles, the guidelines play a key role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data, and in preventing undesirable barriers to trans-border data flows, both on and off line. The guidelines, however, have no binding power and allow broad variation in national implementation[23]. There is no formal process for member states to ratify or adopt and were intended as a response to the danger that discrepancies in national legislation could prevent the free flow of personal data across boundaries. The principles of the Guidelines are meant to reflect the three main goals of the OECD including: pluralistic democracy, respect for human rights and open market economies[24].

The objectives of the OECD Guidelines are to attain a minimum standard of privacy protection among the parties and individual liberties with regard to personal data, to reduce the differences between the domestic laws and practices of Member States to a minimum, to avoid hampering the free flow of information, and finally to reduce the restrictions on international information transfers due to individual privacy risks these restrictions might cause[25].

The OECD guidelines do raise the possibility of a principled framework serving to both protect privacy and yet ensure the trans-border flow of personal data. The principles can be summarized as: collection limitation; data quality; purpose specification, use limitation, security safeguards, openness, individual participation, and finally accountability. The OECD principles are largely mirrored in the EU Directive's principles and formed its foundation. The EU Directive incorporates but also further refines and translates them[26].

2. THE COUNCIL OF EUROPE

In another attempt at establishing data-protection guidelines, the CoE, an

---

23 Cate Fred, *The Changing Face of Privacy Protection in the European Union and the United States*, Indiana Law Review, Volume:33, 1999, p.180

24 Bond Robert, *International Transfers of Personal Data - an Update*, Business Law International, Volume:5, No:3, 2004, p.423

25 Supra note 22, p.819

26 Knoppers Bartha Maria and Fecteau Claudine, *Human Genomic Databases: A Global Public Good?* European Journal of Health Law, Volume:10, 2003, p.28

international organization of forty-seven countries that focuses on strengthening democracy, human rights, and the rule of law throughout its member states, issued a Convention on Personal Data. It is an intergovernmental organization, established in 1949, that promotes cooperation between all European countries. In 1981, the CoE negotiated the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which obliged the Contracting States parties to enact legislation concerning the automatic processing of personal data[27].

Throughout the 1980s, this Convention was the most important European-wide consensus as regards the processing of personal information. The Convention is like a 'non-self-executing treaty'; its standards do not directly enforce binding norms on signatories. However, it required signatory nations to establish domestic data protection legislation that both promulgated the Convention's principles and provided a common core of safeguards for the processing of personal information. Like the subsequently published the EU Data Protection Directive, the Convention intended to provide a central point of reference for domestic legislative efforts [28].

However, the Convention has been the subject of some criticism. European critics have pointed out the diversity of national interpretations of the Convention's requirements. For example, some Member States have decided to follow Article 6 of the Convention and create specific protection for certain kinds of special categories of data while others have not. Similarly, substantial differences also exist in domestic data protection law concerning the extent of information disclosed to individuals about their files[29].

The Convention is generally based on comparatively ambiguous and broad formulations, and it is not necessarily directly applicable, but requires that signatory states adopt implementation measures: therefore it may not be invoked

[27] See the Convention at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, accessed on: 19.06.2013

[28] Schwartz Paul, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, Harvard Law Review, Volume:126, 2013, p.1970

[29] Schwartz Paul, *European Data Protection Law and Restrictions on International Data Flows*, Iowa Law Review, Volume:80, 1995, p.478

directly by individuals before courts. Besides, the Convention includes blanket exceptions, comprising the possibility for the Contracting parties to derogate from the rules with respect to data protection when such derogation is provided for by national law and constitutes a necessary measure in a democratic society[30].

3. THE UNITED NATIONS

The UN is another international body involved in those efforts. It needs to be emphasized beforehand that no human rights convention addresses this issue in a specific provision. Some protection for data is deduced from the right to privacy[31].

The fundamental right to protection of personal data is recognized at the universal level in various human rights instruments adopted under the auspices of the UN, mostly as an extension of the right to privacy. The UN Guidelines for the Regulation of Computerized Personal Data Files[32] set out certain principles regarding the minimum guarantees that should be provided in national legislation for the protection of personal data. The Guidelines provide for the principle of lawfulness and fairness of the collection and processing of personal data, accuracy, purpose-specification, interested-person access, non-discrimination and security of the data files[33].

According to the UN Guidelines, they apply to personal data files kept by governmental international organizations, subject to any adjustments required to take account of any differences that might exist between files for internal purposes such as those that concern personnel management and files for external purposes concerning third parties having relations with the organization.

---

30 *Data Protection in the European Union: the Role of National Data Protection Authorities*, 2010, p.12, available at: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf, accessed on: 18.06.2013

31 McGoldric Dominic, *The Charter and United Nations Human Rights Treaties, in the European Union Charter of Fundamental Rights: Politics, Law and Policy*, Steve Peers and Angela Ward (editors), 2004, p.112

32 See the Guidelines at: http://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=3ddcafaac, accessed on: 19.06.2013

33 Supra note 30, p.11

Each organization should designate the authority statutorily competent to supervise the observance of these guidelines.

SECTION II

I. PROTECTION OF PERSONAL DATA IN THE EU

Throughout the twentieth century, the EU became familiar with the dangers posed by unlimited access to personal data. Authoritarian regimes collected and used personal information to subversive effect across Europe. These experiences, therefore, animated new efforts to prevent the unchecked use of personal data, both at an international and at a national level[34]. The Second World War witnessed the arrival of some momentous declarations and conventions, all of which recognised privacy as a fundamental human right and focused principally on shielding the individual against abuse by protecting their personal data.

For example, the ECHR symbolised one of the first efforts to broaden protection to personal data. Article 8 of the ECHR provides that "everyone has the right to respect for his private and family life, his home and his correspondence." It further emphasized that interference with the right by governments is prohibited except where necessary for the proper function of a democratic society. "This Convention had become reference point for 47 European Countries affecting the legislation beyond European borders regarding with the Protection of Personal Data more than 30 consecutive years, until the rendering of the EU Directive, as secondary legislation of the EU, with the task force, being lying in the member states legislation, in a mandatory way to the EU member states"[35].

Beginning in the 1970s, some European countries adopted comprehensive data protection laws governing both public and private sectors, and established formal data protection authorities (DPA) to monitor and to uphold the laws.

---

[34] Kaplan Harvey L, Cowing Mark W, Egli Gabriel P, *A Primer for Data-Protection Principles in the European Union*, Defense Research Institute, Munich, 2009, p.39

[35] Jashari Ruzhdi, *Personal Data Protection: A European Value in the EU Integration Process*, Law & Justice Review, Volume:4, Issue:1, June 2013, p.245

For instance, the German state of Hesse adopted the first data processing regulation in 1970 due to concerns that sophisticated technologies were increasing the risk that an individual's personal data could be improperly manipulated. Sweden followed in 1973 by passing the first national data protection law. Similarly, France enacted the Law Concerning Data Processing, Files and Liberty in 1978, which granted individuals some measure of privacy protection[36].

It should be kept in mind that Europe has a long, proud history of adopting data protection standards and legislation. Some of which have been amended in the course of time and some will remain under review. Legislation always follows societal and technological advances and it is a challenge for DPAs to comply with these advancements and apply legislation and develop policy in rapidly changing conditions. While the various standards and legislation that now exist may differ in certain areas, they all have the ultimate objective of protecting personal information and freedoms of individuals[37].

In this context, the cornerstone of the EU regulatory scheme is the EU Directive, introduced in 1995. This was followed in 1997 by Directive 97/66/EC for the telecommunications sector, which was another primary piece of EU legislation. It was replaced in 2002 by Directive 2002/58/EC which updated the data protection rules for this sector.

II. EU DATA PROTECTION DIRECTIVE 95/46

A. GENERAL INFORMATION

During the 1980s, it had become obvious that the development of technology able to process personal data had led to European citizens becoming increasingly concerned about the data they entrusted to information networks. Moreover, the European Commission had realised that personal data was being utilised for commercial reasons, and was, thus, subject to Community regulation with respect to the Single Market. The Commission deemed that, through

---

36 Schriver Robert, *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*, Fordham Law Review, Volume:70, Issue:6, 2002, p.2782

37 Supra note 11, p.4

harmonisation of applicable legislation, individuals within the EU could be protected to a basic degree. This was to be implemented alongside measures aimed at eliminating lenient regulatory regimes employed by Member States.[38] Neither the OECD Guidelines nor the Convention offered specific data protection procedures, nor enabled even application and standardisation among national laws. It was with these factors in mind that, the Commission published a draft Directive in July 1990[39].

The European Parliament, on 11 March 1992, amended the Commission's proposal to remove the discrepancies in the 1990 draft between public and private sector data protection and then predominantly approved the draft directive. The Commission then issued its amended proposal and the Council of Ministers adopted a 'Common Position with a View to Adopting Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' on 20 February 1995. The directive was formally approved on 24 October 1995 and took effect three years later. On 25 October 1998, data protection law became markedly stronger throughout Europe[40].

It is clear that the primary objective of the EU Directive is to establish a common, high level of protection for personal data in all Member States in order to remove barriers to flows of personal data within the EU. This is accordant with the EU's aims of abolishing internal frontiers and of establishing an economic and monetary union. In other words, this objective reflects the reality that the need to protect the individual must be balanced with the need to foster the Single Market[41].

Directives, as a common tool of EU lawmaking, are generally not directly binding but are harmonizing instruments; they require Member States to estab-

---

38 Kuilwijk Kees Jan, *Recent Developments in EU Privacy Protection Regulation*, International Trade Law & Regulation, Volume:6, Issue:6, 2000, p.200-201

39 Jay Rosemary and Hamilton Angus, *Data Protection Law and Practice*, Second Edition, 2003, p.10

40 See the Directive at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX-:31995L0046:en:HTML, accessed on: 18.06.2013

41 See Article 1 and in particular Recital 1 and 3 of the Directive

lish national legislation that reflect their principles. In this context, following adoption of the EU Directive, each Member State was charged with the task of bringing its domestic data protection laws into line with the Directive, either by amending its existing laws or by introducing new legislation to implement the Directive[42].

B. SCOPE OF DIRECTIVE 95/46

The EU Directive is divided into seven chapters and thirty four Articles, dealing with general provisions, general rules on the lawfulness of the processing of personal data, judicial remedies and liability and sanctions, transfers of personal data to third countries, codes of conduct, the supervisory authority and working party and finally community implementing measures.

The level of protection is essentially the same in both the public and private sectors, with no formal distinction made between the rules applying in the two sectors. Article 3(1) of the Directive provides that there is no distinction between processing "wholly or partly by automatic means, and ... otherwise than by automatic means of personal data which form part of a file or is intended to form part of a file." Manual data processing is covered only if it is part of the personal data filing system[43]. This provides a safe position for personal data collected at random prior to some other information-collecting activity, so long as the principal data collecting is not computerized.

The Directive's protection is limited to 'personal data', described as any information regarding a natural person, identified or identifiable, even if through sounds and images. The Preamble to the Directive makes the only reference to sounds and images[44]; no mention is made in its operative provisions. Consequently, there is no specific exception or guidance (of the type that a prior

---

42 Ilana Saltzman, *The Status of National Implementation of Directive 95/46/EC on the Processing and Free Movement of Personal Data*, European Intellectual Property Review, Volume:18, Issue:6, 1996, p.680

43 Mell Patricia, *A Hitchhiker's Guide to Trans-border Data Exchanges Between EU Member States and the United States under the European Union Directive on the Protection of Personal Information*, Pace International Law Review, Volume:9, Issue:1, 1997, p.160

44 See the Recital 14, 16 and 17 of the Directive

data subject's consent provision would provide) for personal data identification techniques such as surveillance cameras installed by banks, digitized signatures or recording systems[45].

Although the Directive reflects an expansive approach to governing the use of personal data, it does not apply in two quite narrow contexts. First, according to Article 3(2) of the Directive, it does not apply to activities that are outside the scope of EU law. These activities include "processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law". While these examples provide some guidance as to what kinds of personal data the Commission intended to cover with this exemption, the Directive does not strictly determine the scope of EU law in this context, thereby leaving the exemption open to potentially different interpretations by the Member States[46].

Second, the Directive does not apply to processing by an individual engaged in 'purely personal or household activity'. Such activities include, for example, the use of a computerized spreadsheet to create a mailing list for graduation-party invitations. The existence of only two exceptions indicates the Directive's apparent scope[47]. The statement 'purely personal or household activity' must not make it possible to exclude from the scope of the Directive the processing of personal data by a natural person, where such data are disclosed not to one or more persons but to an indeterminate number of persons[48].

The European Court of Justice (ECJ) took a narrow approach to the interpretation of Article 3(2) as applied to the Internet. The Court held that the exception should be interpreted as relating only to activities which are carried

---

45 D'afflitto Rosario Imperiali, *European Union Directive On Personal Privacy Rights And Computerized Information*, Villanova Law Review, Volume:41, Issue:1, 1996, p.313-315

46 Oxman Stephen A, *Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?* Boston College International & Comparative Law Review, Volume:24, 2000, p.194

47 Supra note 34, p.39-40

48 Maxeiner James R, *Freedom of Information and the EU Data Protection Directive*, Federal Communications Law Journal, Volume:48, 1996, p.100

out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet[49].

The Directive protects the fundamental rights of individuals by affirmative and expanding Convention principles. After prolonged discussion throughout the EU legal persons were excluded from the scope of the Directive's protection. The Directive, however, points out that it has no effect upon existing legislation protecting legal persons regarding data processing which concerns them. Since the exemption does not apply to corporate entities, it can have little effect in protecting the free flow of business information[50].

C. KEY TERMS OF DIRECTIVE 95/46

1. PERSONAL DATA

One of the crucial ways the Directive balances competing interests of privacy and freedom of information is to limit its application to personal data. The EU's data protection law is filled with its own terminology. One of the most important terms is 'personal data' which is the information, provided by EU data protection law. This term is defined in Article 2(a) as any information relating to an identified or identifiable natural person. Allied to this, an 'identifiable person' is one who can be identified directly or indirectly, particularly by reference to an identification number or to one or more factors specific to the person's "physical, physiological, mental, economic, cultural or social identity."

The scope of personal data is quite wide but is not unlimited and contains almost any type of data that can be traced to an individual[51]. This involves not only basic factual information referring to an individual's identity, such as name, address or social security number, but also information revealing an individual's personal preferences, such as records of purchases or visits to

49 See Case C-101/01, *Bodil Lindqvist v. Jönköping*, [2003] ECR I- 12971, para 47
50 Supra note 45, p.313
51 Johnson Elizabeth H, *Data Protection Law in the European Union*, The Federal Lawyer, 2007, p.44

websites[52]. Article 2(a) means that everyone may freely collect, process, and report information about corporate bodies and groups of individuals where the individuals cannot be identified[53]. This would include not only textual information, but also photographs, audiovisual images, and sound recordings of an identified or identifiable person, whether dead or alive[54]. For example, in telephone banking, where the customer's voice giving instructions to the bank are recorded on tape, those recorded instructions should be considered as personal data. Also, images of individuals captured by a video surveillance system can be personal data to the extent that the individuals are recognizable.

Taking into account the definition in the Directive, one could ask why the EU adopted such a sweeping definition. Indeed, this definition was not new to the EU Directive, but could be already found in substantially similar form in the CoE Convention and in the OECD Guidelines. The Directive and its predecessors likely adopted such a broad definition because of their public-law rather than private-law orientation. The explanatory memorandum to the 1992 Commission Draft stated that the "amended proposal meets Parliament's wish that the definition of 'personal data' should be as general as possible, so as to include all information concerning an identifiable individual" [55].

2. DATA PROCESSING

The term 'data processing' is also remarkable and further extends the scope of EU data protection law. The Directive defines it as "any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction". This definition encapsulates almost any use of personal data, in-

[52] Supra note 46, p.191
[53] Supra note 48, p.100
[54] Cate Fred, *The European Data Protection Directive and European-US Trade*, Currents: International Trade Law, Volume:7, 1998, p.62
[55] Maxeiner James R, *Business Information and Personal Data: Some Common-Law Observations about the EU Draft Data Protection Directive*, Iowa Law Review, Volume:80, 1995, p.626-627

cluding mere collection and reaches essentially every task a party or its counsel undertakes to process data in the course of litigation. Actually, the mere act of storing personal data implicates the requirements of the Directive[56].

This definition of processing certainly covers such things as opening and reading a manual file and even extends to merely calling up or reading a piece of information on a computer screen. The EJC pointed out in this regard that placing names and telephone numbers, for instance, on an internet home page constitute the processing of personal data[57]. In that vein, the recording of CCTV images of people's faces or other identifying characteristics also constitutes processing[58].

3. DATA CONTROLLER

Article 2(d) of the Directive defines a data controller as the person which alone or jointly with others determines the purposes and means of the processing of personal data. In this context, a data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files. This definition has been shaped during the negotiations about the draft proposal for the Directive in the early 1990's and the scope of controller was essentially taken from the CoE Convention.

Data controllers can be either individuals or legal persons such as companies, government departments or voluntary organisations. Examples of cases where the data controller is an individual include general practitioners, politicians or sole traders, where these individuals keep personal information about their patients, constituents and clients. Even if an individual is given responsibility for data protection in an organisation, they act on behalf of the organisation, which are the data controller[59].

---

56 Supra note 34, p.40

57 *Lindqvist* Case, para 24

58 Carey Peter, *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Second Edition, 2004, p.20

59 *Key definitions of the Data Protection Act,* online at: http://www.ico.org.uk/for_organisations/data_protection/the_guide/key_definitions, accessed on: 26.06.2013

The data controller is governed by the laws of the Member State in which it is established. The notion of establishment is not defined in the Directive. But it is generally accepted that it means the data controller physically exists within the territory of a Member State[60] and "implies the effective and real exercise of activity through stable arrangements". However, the Directive continues to afford protection even if the data controller is established in a third country. In such an occasion, the "processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice"[61].

4. DATA PROCESSOR

According to Article 2(e) of the Directive, data processor is a natural or legal person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment.

In practice, data controllers often use third party companies to process their data due to the time and cost savings involved. As long as the third party merely acts on the order of the data controller but does not itself determine the purposes for the processing of the data, it will be a data processor. Examples of data processors include payroll companies, accountants or market research companies, all of which could hold or process personal information on behalf of someone else[62].

It should be noted that it is possible for one company or person to be both a data controller and a data processor, as regards distinct sets of personal data. For example, a payroll company would be the data controller regarding the data about its own staff, but would be the data processor concerning the staff payroll data it is processing for its client companies.

---

60 Bauchner Joshua S, *State Sovereignty And The Globalizing Effects of the Internet: A Case Study of the Privacy Debate*, Brooklyn Journal of International Law, Volume:26, Issue:2, 2000, p.701

61 See the Recital 19 and 20 of the Directive

62 Supra note 58, p.19

It is useful to give an example to clarify the key terms involved. Mayflowers Ltd advertises kitchen products in a national newspaper. Robert sees the advertisement and telephones the company for a brochure. He gives his name, telephone number, date of birth and address. The telephone operator enters this information into the company's computer database as Robert is speaking. In this example, the terminology of the Directive applies as follows;

Personal data: information about Robert's name, telephone number, date of birth and address.

Processing: this occurs where the personal data is entered into the computer system, stored in electronic media, read on screen or used in printed material.

Data subject: Robert.

Data controller: Mayflowers Ltd.

D. THE DATA PROTECTION PRINCIPLES

The data protection principles form the backbone of the legislation. Most of the principles are linked to the need to protect privacy, and to prevent undue interference with the private life of individuals. They consist of a number of obligations, with which European data controllers must comply when processing personal data. These principles can be said to be key in the mediatory role of the Directive in balancing the competing interests between data controllers and data subjects with regard the processing of personal data[63].

1. PRINCIPLES RELATING TO DATA QUALITY

a. Fairness and Legality

According to Article 6(1) (a) of the Directive, personal data must be processed fairly and lawfully. Although the lawfulness requirement is relatively straightforward, the requirement of fairness is somewhat ambiguous. In fact, the requirement that data processing be fair is a rudimentary legal generalisa-

[63] Wong Rebecca and Savirimuthu Joseph, *All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet*, Journal of Computer & Information Law, Volume:25, 2008, p.243

tion. While some countries have taken steps to define the fairness requirement, others leave it to the discretion of the DPAs[64].

b. Limited Purpose

Article 6(1) (b) indicates that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". It is clear from the Article 'specified' and 'explicit' purpose must also be 'legitimate'. This is not the same as lawful - certain activities may be technically within the law but nevertheless not legitimate, e.g., if they have unfair or disproportionately negative effects on the data subjects. This works in concert with the requirement of fairness. The Article also allows for the use of personal data for uses other than the original, specified, primary purpose, to the extent that the further processing is not incompatible with the primary purpose[65]. According to a public survey, 70% of Europeans are concerned that personal data kept by companies may be used for a purpose other than that for which it was collected[66].

c. Relevancy

The third principle concerning data quality is the proportionality or adequacy principle as stated in Article 6(1) (c). The EU Directive limits the nature and amount of data that can be collected by stipulating that the personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". It essentially obliges data controllers to obtain from data subjects only those pieces of information necessary for the data controller's purpose for processing such data. However, it does not provide a concrete and enforceable right to demand deletion of an individual's personal data automatically after a certain time period or immediately at the

64 Korff Douwe, *Data Protection Laws in the European Union*, the Direct Marketing Association, 2005, p.37-38

65 Korff Douwe, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*, 2010, p.65-66, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf, accessed on: 28.06.2013

66 *Attitudes on Data Protection and Electronic Identity in the European Union*, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, accessed on: 29.06.2013

request of the data subject.

For example; Magdalen Recruiting Ltd requires job applicants to state their driving licence number on its standard client details form. David, who intends to apply for a job that does not involve driving, fills in the form including details of his driving licence. On this occasion, the company breaches this principle by processing details of David's driving licence.

d. Accuracy

The term accuracy is one of the basic qualities of data, inaccuracy of the simplest kind, such as the case of mistaken identity, is conceptually the easiest to deal with[67]. Article 6(1) (d) indicates that personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data that are inaccurate or incomplete, having regard for the purposes for which they were collected or for which they are further processed, are erased or rectified".

A practical weakness of the provision is that it fails to recognize adequately the nature of data collection. It postulates a focused aim that data collectors may not always have. Business and science professionals sometimes obtain information before being certain of its accuracy or expediency. Only after using such information may the user determine its accuracy or utility[68]. This term is so important that whatever we do today to restrict access to personal data, subsequent decision-makers will probably discard. The same cannot be said of efforts to make the files accurate[69].

e. Limited Time

According to Article 6(1) (e), personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further pro-

67 Karst Kenneth L, *The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 *L*aw and *C*ontemporary *Pr*oblems, 1966, p.353

68 Supra note 55, p.634

69 Supra note 67, p.376

cessed". Information that is no longer required should be destroyed. If this doesn't occur, or if the information is kept for longer than necessary given the purpose the information was initially collected or processed for, then this principle will have been violated. It is also necessary for the data controller to review all data, the purpose(s) it was processed for and evaluate how long such material should be retained[70].

2. CRITERIA FOR LEGITIMATE DATA PROCESSING

a. Consent

It is stated that personal data may be processed when "the data subject has unambiguously given his consent"[71]. The Directive further specifies, in Article 2(h), that consent must be both informed and voluntary. Even though this condition seems straightforward, it may prove problematic in practice[72]. Certain types of personal data may require the consent of multiple people. For example, e-mail includes the identity of at least two people, the sender and receiver. Furthermore, certain Member States may have different criteria for what constitutes 'unambiguous' consent. German authorities, for instance, have suggested that "it is doubtful as to whether consent can be granted voluntarily in an employment relationship"[73].

b. Contract

According to Article 7(b), personal data may be processed when "necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". This applies to processing of data necessary to achieve the specified purpose of a contract. The problem lies in situations, where, for instance, processing is required within a non-negotiable contract, but is not strictly necessary to meet the purpose of that contract. Indeed, in these cases, enforcement of the

70 Supra note 58, p.58
71 See Article 7(a) of the Directive
72 Kosta Eleni, *Consent in European Data Protection Law*, 2013, p.110
73 *Report of the Ad-Hoc Working Group on Employee Data Protection of the Düsseldorfer Kreis*, p.4, available at: http://www.globalcompliance.com/pdf/german-guidelines-summation-5-24.pdf, accessed on: 29.06.2013

provisions may rely upon situationally specific data protection law[74]. It should be emphasized in this regard that this condition refers a contract to which the data subject is a party. It is therefore not necessary for the data controller to be a party to the contract with the data subject[75].

c. Legal Obligations

It is noted in Article 7(c) that personal data may be processed when "necessary for compliance with a legal obligation to which the controller is subject". Although this provision is clearly expressed, it is possible that some legal obligations may not justify processing of personal data. Despite the provision certainly applying to legal obligations arising within the EU, it is not completely explicit that it applies to legal obligations arising elsewhere[76].

d. Vital Interest

This criterion is indicated in Article 7(d) that it may be processed when "necessary in order to protect the vital interests of the data subject". The statement 'vital' is the key to this condition and is likely to be interpreted narrowly due to the reference in Recital 31 of the Directive to the protection of an interest that is essential for the data subject's life. An emergency situation would therefore be covered. It is likely that 'vital interests' only applies in cases of life or death circumstances[77].

For example, Susan goes to Austria for a skiing holiday. She is caught in an avalanche while skiing off-piste and requires emergency hospital treatment. The Austrian hospital asks Susan's medical records to be transferred from Spain, but Susan is unable to consent to such transfer, as she is unconscious. On this occasion, the processing by Susan's doctor is legitimate for this provision's purposes because of the fact it is necessary to Susan's physical well-being.

---

74 Supra note 34, p.41
75 Supra note 58, p.74
76 Kinton John D, *Managing the EU-US Discovery Conflict*, Law 360, 2008, available at: http://www.law360.com/articles/72082/managing-the-eu-us-discovery-conflict, accessed on: 29.06.2013
77 Supra note 58, p.75

e. Public Interest

Personal data may be processed when "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed"[78]. The term of 'public interest' is vague and interpretation is likely to be varied across the EU. In Belgium, for example, processing for epidemiological purposes is assumed to be in the public interest and therefore may proceed without prior consent. Likewise, the wording 'exercise of an official authority' is likely be interpreted differently between the Member States. Domestic legislation is to determine whether only public agencies or natural or legal persons governed by public law or by private law, such as professional associations, may qualify under this exception[79].

f. Legitimate Interest

Personal data may be processed when "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)"[80]. The type of balancing of interests introduced by this provision bestows Member States remarkable flexibility in determining when processing is permitted. In this respect, individual data protection laws outline the precise scope of when such processing is 'necessary'[81].

The Directive does not define the term legitimate interests. However, Recital 30 of the Directive refers to "the legitimate ordinary business activities of companies and other bodies". As a result, legitimate interests probably cover 'legitimate business interests', which may include direct marketing[82]. "It must

78 See Article 7(e) and also Recital 32 of the Directive

79 Bergkamp Lucas and Dhont Jan, *Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web*, The EDI Law Review, Volume:7, 2000, p.82

80 See Article 7(f) of the Directive

81 Supra note 34, p.42

82 Supra note 79, p.81

suffice to note that this provision reflects the structure of the main substantive articles in the ECHR, which allow for restrictions on, or interferences with, such rights for a legitimate purpose, provided that the restrictions or interferences are necessary in a democratic society. The ECtHR has developed detailed tests on the basis of this approach, which therefore also apply under the Directive, in the application of these criteria"[83].

3. SENSITIVE DATA

The EU Directive, in Article 8(1), adds an additional layer of protection to personal data considered uniquely sensitive. Certain personal data merits higher if it includes "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and ...health or sex life". Accordingly, the Directive forces Member States to flatly prohibit the processing all sensitive data, except in a limited set of circumstances[84]. Those circumstances exist where:

- a data subject has given explicit consent,
- it is necessary for a controller to meet legal obligations with respect to employment law,
- it is necessary to protect the vital interests of a data subject (or another person), and the data subject is physically or legally incapable of giving consent,
- it is carried out by a non-profit organization whose aim is to advance an agenda related to one of the categories of sensitive data,
- the data are manifestly made public by the data subject,
- it is necessary to establish or defend legal claims, and
- it is required under health grounds

In practical terms, the processing of sensitive data almost invariably requires the explicit consent of the data subject as all other circumstances listed are rarely present in a commercial setting. The requirement of explicit consent

83 Supra note 65, p.68
84 Supra note 45, p.314

implies that the individual must have clearly indicated his assent to the processing[85]. This means opt-in consent and opt-out consent, which are explained below, is not sufficient. Since non-sensitive data can sometimes be linked to sensitive data, the implications of the consent requirement may go beyond the scope of pure sensitive data[86].

It should be kept in mind that meeting these criteria does not mean that the other requirements introduced by the Directive do not apply. In some Member States, the processing of personal data for marketing purposes may pass the legitimacy test, even if no consent is gained. However, consent is always required for processing of sensitive data for these aims. Accordingly, an opt-out arrangement for direct marketing purposes offered to data subjects visiting a web site offering medical or pharmaceutical products or services, would not be assumed sufficient. Only an opt-in formula is adequate when health data is processed for direct marketing goals[87].

The most common way of establishing consent in the EU is by the use of an opt-out or opt-in method. Such a clause comprises a statement of intended uses for data together with a box that enables a user to remark, by ticking, that he does not wish his data to be used for a particular specified purpose (opt-out) or a box that allows a user to indicate that he admits to particular specified processing (opt-in)[88].

For example, a company sends information on sports products to Michael. If a clause stating 'please tick the box if you do not wish to be contacted in this way' is present, then this is an opt-out clause. Conversely, if the company would like to make his data available to a chosen business partner, and a clause is present that states 'please tick the box if you wish your information to be used in this way', then this is an opt-in clause.

While the definition of sensitive data in the Directive is quite broad to be-

85 Supra note 4, p.70
86 Corien Prins, *When Personal Data, Behaviour and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?* SCRIPT-ed, Volume:3, Issue:4, 2006, p.291
87 Supra note 79, p.82-83
88 Supra note 58, p.254

gin with, some Member States define sensitive data more widely than others. For example, Portugal includes data about the 'private life' of the individual within the definition, thereby requiring express consent for collection of data on consumer and household habits, whereas in the UK such data would almost certainly be treated as 'non-sensitive' personal data and would require an accordingly lower degree of protection[89].

When Article 8(1) is applied to the internet; it is debatable whether the criterion works in practice. See, for instance, the Lindqvist case. Specifically, it can be contended that any photographs of the data subject uploaded on the internet falls within Article 8 of the Directive because the picture demonstrates some of the characteristics that may be accepted as sensitive data[90]. The ECJ took the view that the expression 'data concerning health' used in Article 8(1) must be given a broad interpretation so as to include information regarding all aspects, both physical and mental, of the health of an individual[91]. Hence, reference to the fact that an individual has injured her foot and is on half-time on medical grounds constituted personal data concerning health within the meaning of Article 8(1) of the Directive.

E. THE RIGHTS OF DATA SUBJECTS

The data subject rights are central to data protection; they are the primary means to assert one's right to informational self-determination. The basic rights of data subjects involved in the Directive are not new: they had already appeared in other international data protection instruments, such as the CoE Convention, the OECD and the UN Guidelines on data protection. Articles 10 to 15 of the Directive provide data subjects with rights. Subjects are bestowed a right of access, correction and objection. There are certain modifications to these rights but in general they underscore the aim of protecting the fundamental rights of individuals. The directive does not decide the complex philosoph-

89 Charlesworth Andrew, *Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?* Hastings Law Journal, Volume:54, 2003, p.940

90 Wong Rebecca, *Data Protection Online: Alternative Approaches to Sensitive Data?* Journal of International Commercial Law and Technology, Volume:2, Issue:1, 2007, p.9)

91 Case *Lindqvist*, para 50

ical question of whether the data subject owns his data, but clarify that they may not be processed if this violates privacy. Mostly, the directive protects informational privacy[92].

1. RIGHT TO ACCESS

Assurances are provided for data subjects in Article 12 of the Directive. It requires Member States to guarantee that data subjects have a right of access to data being collected by data controllers. It refers to data subjects' right to obtain the relevant data without constraint at reasonable intervals and without excessive delay or expense[93]. This does not need to be automatic. It is perfectly acceptable for data controllers to require subjects to request the data that is held about them. Nevertheless, data subjects also have the right to be told if their data is being processed, and for what purpose. There is a stipulation that this must be presented 'in an intelligible form' which indicates the source of the data. Should a situation arise where the processing of personal data is automated (though there are limits within the Directive which concern the conditions in which automated data processing can be permitted), then the data subject still has the right to be told of 'the logic involved' in the processing of their personal data[94].

The data subject access right compels European organisations to disclose a copy of all personal data to relevant individuals, upon a request being received from such an individual. It regularly constitutes an onerous burden, both administratively and financially to data controllers. It is also a powerful tool with which data subjects are able to gain access to great amounts of information held about them by organisations of all kinds[95]. Beside, Article 13

---

92 Blume Peter, *Trans-border Data Flow: Is There a Solution in Sight?* International Journal of Law and Information Technology, Volume:8, No:1, 2000, p.66

93 It differs from country to country. In Finland, for example, reasonable intervals, without excessive expense means the controller must provide access once a year without charge. If requested more often, the controller may charge up to the maximum of actual costs incurred; and that without excessive delay means within three months.(Supra note 107, p.395)

94 Salbu Steven R, *The European Union Data Privacy Directive and International Relations*, Vanderbilt Journal of Transnational Law, Volume:35, 2002, p.672

95 Supra note 58, p.24

allows Member States to make exceptions to those rights of access, such as defence, national or public security.

To give a pertinent but simple example regarding this right; Robert receives a brochure from Mayflowers Ltd but notices something odd about the address label on the packaging. His name appears as Mr Robert H. Murray. He feels sure that he did not give his middle name to the telephone operator. He writes a letter to the company asking for a copy of all the information it holds on his and details of the source of that information. In this case, the company must supply Robert with the information he has requested.

2. RIGHT TO CORRECT

One of the important provisions of the data protection regulation is the ability of the subject to correct any erroneous data. According to Article 12(b), data subjects have the right to rectify, erase or block any data processing not in compliance with the Directive, especially if incompatibility is a function of the incompleteness or inaccuracy of the data. Besides, if third parties have received the data prior to such erasure or blocking, the data subject has the right to notification of the rectification to third parties[96].

In this context, Member States must grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller[97].

3. RIGHT TO OBJECT

The Directive also creates another main right of the data subject. Article 14(a) requires Member States to give data subjects the right to object to the processing of data relating to him or her at any time 'on compelling legitimate grounds'. Moreover, the Directive states that the data subject has the right to

[96] Supra note 94, p.673
[97] See Article 32(2) of the Directive

object to the processing of personal data used in direct marketing[98]. Direct marketing is subject to a right, exercisable by the data subject, to prevent processing for this purpose. This right allows individuals to stop the delivery of 'junk mail'.

The second provision for data subject objection is set out in Article 15(1). This right contains the related data subject's right 'not to be subject to a decision which produces legal effects concerning him' and 'which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him'[99]. "Where a decision significantly affecting that individual is taken wholly by automated means and the data controller has not received a notice from the data subject requiring him to refrain from taking such decisions, the data controller must, as soon as is reasonably practicable, inform the individual that such a decision has been taken"[100].

F. OBLIGATIONS OF CONTROLLERS

1. NOTICE TO SUBJECTS

Articles 10 and 11(1) of the Directive require data controllers or his representative to inform data subjects of a data processing related to them and also of the main features of the data collecting operations. Except where a data subject already knows such information, controllers must provide the data subject with the following information: the identity of the controller, the purpose of the processing, the recipients or categories of recipients of the data, whether providing information is obligatory or voluntary and the existence of the right to access and correct personal data[101].

Where data is collected from data subjects, such details must be given to them at the time of collection, except if they are already familiar with them. Where the data has not been obtained from the data subjects, the details must be given to them at the time of the recording of the data, or at the latest when

98 See 14(b) of the Directive
99 Supra note 45, p.319
100 Supra note 58, p.41
101 Supra note 34, p.43

the data is disclosed to third parties for the first time, unless the data subjects are already familiar with such details[102].

Where data has not been collected from the data subjects, the requirement that information must be given to the data subjects does not apply in the following instances; in the case of processing for statistical purposes or for the purposes of historical or scientific research, in the event the provision of such information proves impossible or would involve a disproportionate effort and if recording or disclosure is expressly required by law[103]. Member States may restrict the rights and obligations concerning the obligation to inform the data subjects, when such a restriction constitutes a necessary measure to guard certain public interests, or protect the data subjects or the interests of others[104].

2. NOTICE TO DATA PROTECTION AUTHORITIES

In conformity with the Directive, it is generally unlawful to process personal data anywhere in the EU unless the data controller maintains an appropriate entry in the relevant national register of data controllers. Article 18 of the Directive compels Member States to include in their laws an obligation to notify a supervisory authority before carrying out any automatic processing or set of processing operations intended to serve a single or several related purposes[105].

Furthermore, Article 19 of the Directive stipulates in detail what facts must be stated in the notification. With the exception of providing an exemption by national law, the data controllers must at least supply the following information to the concerned DPAs prior to performing any automatic processing operation: the name and address of the controller and any relevant representative, the purposes of the processing; a description of the category or categories of persons affected, and of the data relating to them, the recipients or 'categories of recipients' to whom the data may be disclosed, any proposed transfers to third countries and a general description of measures taken to ensure the secu-

102 See Article 11(1)
103 See Article 11(2)
104 Roos Anneliese, *The Law of Data (privacy) Protection: A Comparative and Theoretical Study*, University of South Africa, 2003, p.210
105 Supra note 55, p.637

rity of processing[106]. Controllers must also notify the supervisory authority of changes in any of the above information.

Notification processes may be simplified or exempted by individual Member States in a few cases only in order to avoid unnecessary administrative formalities. In this regard, Article 18(2) provides for situations in which Member States may simplify or exempt categories of processing which "are unlikely... to affect adversely the rights and freedoms of data subjects", or where the controller "appoints a personal data protection official" in compliance with national legal requirements. Certain minimum information must still, however, be supplied[107]. The notification obligation is intended to enhance transparency for data subjects, raise awareness for data controllers and give DPAs a useful monitoring tool in the form of registers.

G. SUPERVISORY AUTHORITIES

The Directive requires all EU Member States to establish independent public authorities to monitor the application of the Directive within its territory. The supervisory authorities, in this context, have, at minimum, broad competence to investigate data protection issues, to provide guidance, to engage in legal proceedings where national laws have been violated and to bring violations to the attention of judicial authorities. They must be also consulted when regulations with a potential data protection impact are drafted. This emphasis on independent supervision is a vital characteristic of the European approach to data protection[108]. The Directive also established what has become known as the Article 29 Working Party. It is partly comprised of representatives of the supervisory authorities designated by each Member State[109].

The EJC noted that the independence of the Supervisory Authority pre-

106 Supra note 34, p.43

107 Shaffer Gregory, *Globalization And Social Protection: The Impact of EU And International Rules in The Ratcheting up of US Data Privacy Standards*, Yale Journal of International Law, Volume:25, 2000, p.220

108 Supra note 11, p.21

109 Garrie Daniel, Duffy-Lewis Maureen and Wong Rebecca, *Data Protection: The Challenges Facing Social Networking*, International Law & Management Review, Volume:6, 2010, p.130

cludes any influence being exercised by supervised bodies. It also prohibits any external influence, whether direct or indirect, which could call into question the performance of authorities tasked with establishing a fair balance between the protection of the right to private life and the free movement of personal data. The Court also took the view that for the purposes of the role adopted by those authorities as guardians of the right to private life, it is necessary that their decisions, and therefore the authorities themselves, remain above any suspicion of partiality[110].

The functions of a supervisory authority should also include hearing complaints from data subjects and issuing a public report at regular intervals concerning the state of data protection in the country. The directive requires each supervisory authority to investigate data processing that "poses specific risks to the rights and freedoms of individuals." Each supervisory authority is required to keep and make available to the public a "register of notified processing operations"[111]. A supervisory authority provides accordance with the Directive's principles. "When the data subject seeks to challenge the decisions of the Authority or pursue an asserted violation of the right to privacy by third parties, the data subject may always seek recourse in an ordinary jurisdiction"[112].

Each Member States' supervisory authority is competent to exercise the powers conferred on it within the territory of the Member States, even though a different national law may apply. The authority of one Member State may approach that of another with a request to apply its power. The supervisory bodies are instructed to cooperate generally with one another, to the extent necessary for the performance of their duties, in particular by exchanging all useful information[113].

Specific institutional arrangements vary. The Netherlands has a DPA with general responsibility alongside other sector-specific bodies in areas such as health and telecommunications. Federal states with decentralized regional

110 See Case C-518/07, *Commission v Germany*, [2010] ECR I-1885
111 Supra note 23, p.183-184
112 Supra note 45, p.320
113 See Article 28(6) of the Directive

institutions, such as Germany, adopt national bodies with attendant sub-state agencies operating at the regional level. Other states, such as Romania, operate Ombudsman bodies responsible for monitoring privacy rights, while equivalent bodies in Finland protect personal data[114].

H. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Perhaps the most controversial provisions of the EU Directive are those concerning the transfer of personal data to third countries. Article 25 in this regard formed the basis for a large variety of disputes because it represented one of the very few occasions where the EU broadened its scope of regulation to external legal orders[115]. It should be reiterated that the EU system seeks to realize the dual aims of the Directive, namely, free flow of information and effective data protection[116]. However, the variation in levels of data protection in EU Member States may prevent transfer of personal data from one country to another. This difference may further create an obstacle to the pursuit of a number of economic activities at the Union level. Therefore, the Directive first sets a strong standard for protection among Member States and removes obstacles to trans-border data flow within the Union[117].

The Directive also regulates the transfer of data out of the EU and expressly prohibits this transfer to third countries (non Member States) except under limited circumstances. But, it should be underscored here that outside of the EU, the Directive has no such effect and the level of protection varies more dramatically by nation. According to article 25(1) of the Directive, such a transfer is only admissible if an adequate level of data protection is secured in the recipient country[118].

---

114 Supra note 30, p.19

115 Koutsias Marios, *The International Reach of European Union Data Protection Law and the United States: is International Trade in a Safe Harbour?* International Trade Law & Regulation, Volume:18, Issue:2, 2012, p.32

116 Bainbridge David, *Processing Personal Data and the Data Protection Directive*, Information & Communications Technology Law, Volume:6, Issue:1, 1997, p.17

117 Kong Lingjie, *Data Protection and Trans-Border Data Flow in the European and Global Context,* European Journal of International Law, Volume:21, 2010, p.443

118 Swire Peter and Litan Robert, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press, 1998, p.31

The above restrictions provide de facto extraterritorial effect to the Directive. For instance, many transnational companies are obliged to ensure that all of their data processing activities are performed in conformity with the terms of the Directive because of the difficulty or impossibility of separating personal data collected within the EU from personal data collected elsewhere. It can be divided the exceptions to the general prohibition against transferring personal data outside of the EU into following three categories[119].

1. CIRCUMSTANCE-SPECIFIC EXCEPTIONS

The circumstance-specific exceptions to the general prohibition against transferring personal data outside of the EU are similar to the circumstances that determine when such personal data may be processed. The Directive, in Article 26(1), provides for derogations from the prohibition of transfer of data to third countries without adequate protection for privacy. Those exceptions are consent, contract, public, vital and legitimate interest - identical to criteria for legitimate data processing explained before.

2. COUNTRY-SPECIFIC EXCEPTIONS

a. Adequate Level of Protection

Article 25 of the Directive indicates that data may be transferred to a third country if it ensures an 'adequate level of protection'. However, the Directive does not provide much guidance on how adequacy is to be defined or determined, other than to remark that it should be "assessed in the light of all the circumstances surrounding the data transfer" on a case-by-case basis[120]. Due to the fact that it is not clear what is meant by the principle 'adequate level of protection', there is the risk that various applications appear within the EU Member States.

The data controller could potentially choose, for the export of data, the country with the lowest level of data protection. It is for this reason that the

[119] Supra note 34, p.43

[120] Hobby Seth, *The EU Data Protection Directive: Implementing A Worldwide Data Protection Regime and How The U.S. Position Has Progressed*, International Law & Management Review, Issue:1, 2005, p.173

Directive provides for a harmonized practice of decision making[121].

The European Commission is entitled, however, to determine particular countries as providing 'an adequate level of protection'. Most states have their own data protection laws but, to date, few have been designated by the EU as having adequate laws[122]. Among the countries that do are the three non-EU members of the European Economic Area (EEA); Norway, Liechtenstein, and Iceland. Besides, the only additional countries that the Commission has determined provide an adequate level of protection such as Switzerland, Canada, Argentina, Israel and Australia[123].

The Data Protection Working Party has carefully considered the question of adequacy in a working document. In this paper, it is deemed that a minimum of six basic principles must be included in an acceptable regulation. These are the purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle, rights of access, rectification and opposition, and finally there must be restrictions on onward transfers[124].

b. Safe Harbor

EU Directive prohibits the transfer of personal data to non-EU countries that do not meet the EU adequacy standard for privacy protection. Such protection can either be at a country level or at an organizational level. While the US and the EU share the aim of enhancing privacy protection for their citizens, the US takes a different approach to privacy from that taken by the EU. In order to bridge these differences in approach and provide a streamlined means for US organizations to comply with the Directive, the US Department of Commerce, in consultation with the European Commission, developed a

---

121 Zinser Alexander, *European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers*, Tulane Journal of Technology & Intellectual Property, Volume:6, p.172-173

122 Supra note 24, p.424

123 See all list of countries who have adequacy of the protection of personal data, at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm, accessed on: 07.07.2013

124 Supra note 92, p.69

Safe Harbor framework[125].

The EU and the US Department of Commerce entered into negotiations in 2000 that provided provisions to allow the transfer of personal data from the EU to organizations in the US that publicly certify themselves to be a Safe Harbor. This process enables a US company or affiliate to receive personal data from the EU if it agrees to treat the data as if the Directive applied. Personal data transferred to a Safe Harbor organization may, for example, include payroll data, employee evaluations, customer lists, billing information, and documents collected for production in litigation within the US as part of the Safe Harbor process, an organization must comply with the following seven principles that mirror principles outlined in the Directive:

Notice refers to the requirement that the company inform data subjects about the purposes of its data collection and use, the types of disclosure, and the options for limiting use and disclosure. Notice must be clear and conspicuous, and must be provided on the front end of any data transaction where reasonably practicable[126].

Choice refers to the requirement that data subjects be offered the opportunity to determine whether and how their data will be used and disclosed. To facilitate this option, organizations must provide to individuals clear and readily available information and mechanisms[127].

Access is directed to the requirement that data subjects must be granted access to the information that an organization holds about them, and must be endowed with the ability to delete, correct, or amend such data, provided that the expense of maintaining such an operation is not unreasonably disproportionate to the rights of the individual and does not affect the rights of persons other than the individual[128].

---

125 See the US and EU Safe Harbor at: http://export.gov/safeharbor/eu/index.asp, accessed on: 07.07.2013

126 Supra note 120, p.181

127 Bender David and Ponemon Larry, *Binding Corporate Rules for Cross-Border Data Transfer*, Rutgers Journal of Law & Urban Policy, Volume:3, Issue:2, 2006, p.157

128 Supra note 24, p.425

Security relates to the requirement that the company take reasonable steps to protect the data from loss, misuse, unauthorized access, disclosure, alteration and destruction[129].

Enforcement concerns the requirement that the company provide to the data subject some affordable, readily available mechanism for assuring compliance with the Safe Harbor Principles[130].

Onward Transfer is the requirement that once in the US, the data will only be disclosed to third parties, consistent with the principles of notice and choice, or pursuant to an agreement imposing a level of protection at least as high as that required by the Safe Harbor Principles[131].

Data Integrity refers to the requirement that personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current[132].

In conclusion, The Safe Harbor Agreement was necessary in order for the requirements of the Directive (regarding an 'adequate' level of protection offered by third countries to recipients of data transfers) to be satisfied.

3. BUSINESS-SPECIFIC EXCEPTIONS

There are currently two methods that companies can employ to avoid the prohibition against transferring personal data outside of the EU. These methods, Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), are likely to become increasingly important as DPAs institute stricter enforcement regimes for cross-border transfers of personal data.

a. Standard Contractual Clauses

The Commission has the power to decide that certain SCCs offer sufficient safeguards as required by Article 26(2) of the EU Directive. They provide

129 Supra note 39, p.225
130 Supra note 36, p.2791
131 Supra note 39, p.224
132 Supra note 120, p.183

adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. The effect of such a decision is that by incorporating the SCCs into a contract, personal data can flow from a data controller established in any of the EU Member States and three EEA member countries to a data controller established in a country not ensuring an adequate level of data protection. Except in very specific circumstances, national DPAs cannot block such transfer[133].

Historically, The Commission has approved three sets of contractual clauses. Two of these sets of contractual clauses apply to transfers from data controllers in the EU/EEA to controllers in third countries. The third set applies to transfers from data controllers in the EU/EEA to processors in third countries. Accordingly, businesses will either have the possibility to choose between two sets of SCCs or only have the opportunity to use the last set of contractual clauses. It is important to stress that this does not prevent companies relying on different contracts approved at national level by DPAs[134].

b. Binding Corporate Rules

The second business-specific exception relies on so-called Binding Corporate Rules. This exception is available to multinational corporations that enact codes of conduct that comply with the Directive, and that apply company-wide. Once the BCRs are approved, they allow a corporation to freely transfer personal data throughout its organization[135].

"The approval process for BCRs begins with an application to the most appropriate DPA. The application must detail the applicant's efforts to protect and process personal data worldwide. In addition, the application must demon-

133 *Model Contracts for the transfer of personal data to third countries*, at: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm, accessed on: 07.07.2013

134 *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*, p.24, http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf, accessed on: 07.07.2013

135 Lambert Paul, *A User's Guide to Data Protection*, Bloomsbury Professional Ltd, 2013, p.401

strate that the systems necessary to protect and process the data are already functional and effective. After the first DPA provisionally approves the application, the application is sent to every other relevant DPA for approval"[136].

III. THE PROPOSED EU DATA PROTECTION REGULATION

It should be admitted, however, that the current Data Protection Directive was introduced in the pre-internet age. But, 250 million people now use the internet daily in Europe. It is therefore deemed not to be fit for the challenges of the 21st century. Fast technological advancements and globalisation have brought new challenges with significant effect on the data protection debate, and people thus need to invest in more efficient protection of their fundamental rights and freedoms[137].

EU Member States have applied the existing rules in different ways, resulting in considerable differences in practice and interpretation, as well as causing much legal uncertainty. This means undue costs, but also a loss of protection for citizens in cross-border situations. There needs to be more consistency across the EU. Finally, the Lisbon Treaty emphasised the importance of data protection as a fundamental right and brought a legal basis for horizontal rules in all EU policy fields. This required a review of current rules and called for a more sweeping approach[138].

As a consequence, The European Commission published a proposal for Data Protection Regulation on 25 January 2012. The proposed Regulation will replace the 1995 Directive and focuses on the protection of individuals' privacy in relation to the use of personal data. Once adopted, the regulation will take direct effect in all EU Member States. Although the Proposed Regulation itself requires a substantial study, this study will discuss the key aspects of the Regulation.

- The replacement of the Directive with a Regulation in itself constitutes a

[136] Supra note 34, p.45
[137] Kuschewsky Monika, *Sweeping Reform for EU Data Protection*, European Lawyer, Volume:112, 2012, p.12
[138] Hustinx Peter, *Streamlining Data Protection*, European Lawyer, Volume:112, 2012, p.4

great novelty, perhaps the most important. Since Regulations are directly applicable, the EU's data protection rules will be exactly the same in all Member States. A Regulation can be both vertically and horizontally directly effective, so that its provisions may be relied upon in court proceedings against public institutions as well as private parties[139].

- The rights of the data subjects have been clarified and particular importance has been given to 'the right to erasure or the right to be forgotten', especially for social networks and other services in the online environment. When people no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted[140].
- Whenever consent is required for data processing, it should not only be freely given, specific and informed, but also explicit, namely it should be based on a statement or a clear affirmative action. The Regulation adds the elements that consent has to be explicit in the definition of consent, so the provisions of the Regulation concerning the processing of sensitive data do not refer to 'explicit' consent any more[141].
- The Regulation also introduces 'the right to data portability' which gives individuals the right to obtain an electronic copy of their data from organisations or request that an organisation transfer their data to another organisation. This right is intended to empower consumers, enabling them to easily switch services.
- 'Data breach notification' refers to an obligation of controllers to quickly provide information on data breaches, such as unauthorised access or other data leaks. Article 31 compels controllers to notify all such breaches to the supervisory authority without undue delay and where feasible within 24 hours of discovery of a breach. Late notifications have to be accompanied by a reasoned justification for the delay.
- Individuals will have the right to refer all cases to their home nation-

139 De Waele Henri, *Implications of Replacing the Data Protection Directive with a Regulation - a Legal Perspective*, Privacy & Data Protection, Volume:12, Issue:4, 2012, p.4

140 See Article 17 of the Proposed Regulation

141 Supra note 72, p.147

al DPA even when their personal data is processed outside their home country. "National DPAs will be significantly strengthened, in terms of independence, resources and powers. In particular, they will be empowered to issue orders, engage in legal proceedings and fine companies that violate EU data protection rules"[142].

- The international scope of EU data protection law will be broadened. It will not only apply to processing of personal data in the context of an establishment of a controller in the EU, but also to processing related to the offering of goods or services to data subjects in the EU, or to the monitoring of their behaviour[143].
- Provisions on data transfer to third countries have also been further developed and streamlined, including a provision on BCRs with need for approval by a single DPA. In other words, the Proposed Regulation consolidates many of the policies negotiated post-directives. Notably, it acknowledges the validity of the Safe Harbor Agreement, BCRs, and contractual clauses[144].
- The Proposed Regulation creates a new institution; the European Data Protection Board. It upgrades the status of the Article 29 Working Party, the panel of national supervisory authorities. It states that the Commission is not a member of this Board, but has the right to participate in the activities and to be represented. The Board provides a useful forum in which national supervisory authorities can come to an agreement on important issues. The role of these national officials is a long-established one[145].

These reforms are intended to address the issue of responsibility and accountability which lies at the heart of issues concerning the processing of personal data. The replacement of a Directive with a Regulation clearly provides a substantial step towards standardised, accessible and transparent rules and

142 Supra note 137, p.13
143 Supra note 138, p.14
144 Supra note 28, p.2006
145 See Article 64 of the Proposed Regulation

procedures which can be applied across the EU, regardless of the eventful form of the Regulation[146].

SECTION III

I. PROTECTION OF PERSONAL DATA IN TURKEY

A. GENERAL OVERVIEW

From an international perspective, Turkey, as a member of the Council of Europe, has ratified the ECHR, signed both the CoE Convention on the Protection of Personal Data in 1981, and the Additional Protocol to the Convention regarding supervisory authorities and trans-border data flows in 2001, but has not yet ratified them. Therefore, they are not of the status of 'law' for the purposes of Turkey's domestic law.

It is important to stress that the right to protection of personal data is a fundamental right. It is different from, but closely linked to, the right to respect for private and family life. Domestically, this right is referred to in the Turkish Constitution and in various pieces of legislation such as the Criminal and Civil laws, but it is not defined. In fact, before 2010 the term 'personal data or protection of personal data' was not explicitly stated though it was postulated within the scope of the protection of private life in the Constitution. Thereafter, on 12 September 2010, a referendum was held on a reform package which introduced amendments to the last Constitution adopted in 1982. As a result of the amendment, the right to protection of personal data detailed in Article 20 of the Constitution has been bolstered, increasing the scope of accountability and introducing more stringent requirements for protection of personal data. The following paragraph has been added to the Article 20 of the Turkish Constitution:

"Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data and to be informed whether these are used in consistency with envisaged objectives. Personal data shall only be

[146] Supra note 139, p.5

processed in accordance with the conditions anticipated by law or with the express consent of the person. Principles and procedures on the protection of personal data shall be regulated by law."

Indeed, it was the first time personal data has been codified and protected as a standalone legal concept apart from privacy through 2005 Turkish Criminal Law and Criminal Procedure Law. In contrast to the OECD, CoE and EU who adopted protection to personal data to eliminate possible restrictions to global trade, the first protection in Turkish legislation was provided for personal data in the criminal code.

In Criminal Law, Articles 135-140 contain provisions concerning data protection. The new articles made it a criminal offence to collect and process data unlawfully or without consent with a maximum prison sentence. It is considered a criminal offence to cause the data to be seized by others, to deteriorate, or to be damaged as a result of failure to take the necessary security measures. According to Article 135(2), any person who records the political, philosophical or religious concepts of individuals, or personal data relating to their racial origins, ethical tendencies, health conditions, sexual lives or union relationships is punished with imprisonment. The Criminal Law also considers disclosure and delivery of personal data to unauthorized persons. Moreover, in case of failure to destroy the data within a defined system despite the expiry of legally prescribed period, the persons responsible for this failure should be sentenced to imprisonment. Finally, it states that such criminal offences are applicable to all systems in which data is held and emphasizes the liability of legal entities.

Regarding Criminal Procedure Law, it should be stated at the outset that criminal science is of great importance in order to achieve material in order to initiate criminal proceedings. In this context blood, fingerprints, voice and smell are all considered to be personal data. Turkish Criminal Procedure Law provides protection for the examination of samples obtained from the body or crime scene and addressed them for the first time as personal data. Information obtained from the analysis of such samples is also considered to be personal

data and should not be used for any other purposes. Further, individuals who have access to the files should not disclose the information to unauthorized persons[147].

Prior to these main laws, definitions regarding the processing of personal data were detailed in a Regulation called 'Processing of Personal Information and Protection of Privacy Regulation on Telecommunications Sector' (2004). Here, personal data meant any information concerning an identified or identifiable natural and/or legal person; an identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, health, genetic, ethnic, religious and political information in accordance with the relevant Regulation. This definition is very close to the EU Directive.

In the field of Civil Law, there are some provisions which are originally related to protection of personal rights, particularly in the Civil Code and the Code of Obligation. The rights of individuals may be protected through these provisions in the case of unlawful processing of personal data. Pursuant to Article 24 of the Civil Code, an individual whose personal rights are unjustly violated may bring a civil action to protect against such violation and/or the compensation of damages arising from such violation. Disclosing or misuse of personal and/or confidential data can be considered to be an infringement of personal rights according to these general rules for the protection of personal rights. An aggrieved party may file a lawsuit and receive indemnity of its material and immaterial damages under Article 49 of the Code of Obligations.

Provisions regarding personal data and its protection can also be found in the text of other laws, such as in Labour Law, the Right to Information Act and the Population Services Law. According to Labour Law, for instance, "the employer shall arrange a personal file for each employee working in his establishment. In addition to the information about the employee's identity, the employ-

[147] See Article 80 of the Criminal Procedure Code of the Republic of Turkey, available at: http://legislationline.org/documents/section/criminal-codes, accessed on: 16.07.2013

er is obliged to keep all the documents and records which he has to arrange in accordance with this Act and other legislation and to show them to authorised persons and authorities when requested. The employer is under the obligation to use the information he has obtained about the employee in accordance with the principles of honesty and law and not to disclose the information for which the employee has a justifiable interest in keeping as a secret"[148].

B. THE NEED FOR A DATA PROTECTION LAW

There is a need to answer a more general question, before the assessment of the Draft Law: Is it necessary to adopt such a law in Turkey? It should be borne in mind that Turkey is a democratic state that respects human rights. Indeed, this is enshrined in its Constitution.

Turkey is a member of many international organisations such as the CoE, UN and OECD. However, Turkey has failed to incorporate the principles adopted by these organisations in the field of data protection into its domestic law. Turkey still lacks a clear, adequate legal arrangement concerning the processing of personal data.

Protection of personal data has been a part of the legal system in a majority of European Countries for nearly forty years. Indeed, the longest established arrangements in this field are in Europe. If one leaves aside the US, almost all modern democratic States have adopted regulations in this regard[149].

The processing of personal data without safeguards violates fundamental rights. In Turkey, the public are fully aware that there are archives where private and sensitive data has been recorded with no legal basis. Nor is there any institution to control and supervise the processing of personal data.

In Articles 135 et al of the Turkish Criminal Code, the processing of personal data unlawfully has been deemed an offence. However, there are no regulations which clarify in which conditions it is contrary to law and in which

[148] See Article 75 of the Labour Law, available at: http://www.iskanunu.com/5510-social-insurance-and-universal-health-insurance-law/243-4857-labo-law-english-by-article, accessed on:16.07.2013

[149] Kuzeci Elif, *Kişisel Verilerin Korunması*, Turhan Kitabevi, Ankara, 2010, p.351

conditions it is not. In 2010, with the amendment made in the Constitution, protection of personal data was secured as a fundamental right, and it was stated that other details should be regulated by law.

It is also important to state here that making a legal arrangement about protection of personal data and establishment of regulatory and supervisory institution is pertinent to 4 of the 'Acquis Chapters'. These Chapters are 23rd Chapter (Judiciary and Fundamental Rights), 24th Chapter (Justice, Freedom and Security), 10th Chapter (Information Society and Media) and 28th Chapter (Consumer and Health Protection). Accordingly, it is also a requirement for Turkey to adopt such a law in the accession process.

The fact that such a Law has not been implemented is described as an important deficiency in the Progress Reports, the Accession Partnership Documents, and in the 23rd Chapter Post Screening Reports. The 2012 progress report stated that "Turkey needs to align its legislation with the data protection *acquis* and set up a fully independent data protection supervisory authority. Turkey also needs to ratify both the CoE Convention for the protection of individuals with regard to automatic processing of personal data and the additional protocol to it on supervisory authorities and trans-border data flow. The absence of data protection legislation hampers operational cooperation between police and judicial authorities and on counter-terrorism[150]."

Furthermore, operational cooperation agreements cannot be made with the European Police Office (EUROPOL) on the grounds that personal data is not protected in Turkey. The current cooperation and exchange of information and documents cannot be made via electronic transmission and for this reason, delays and failures are experienced. Furthermore, Turkey cannot benefit from the opportunities provided by the Schengen Information System and Supplementary Information Request at the National Entry (SIRENE) Office[151].

---

150 *Turkey 2012 Progress Report*, p.74, available at: http://ec.europa.eu/enlargement/pdf/key_documents/2012/package/tr_rapport_2012_en.pdf, accessed on: 18.07.2013

151 This system allows important information about stolen cars, passports, European arrest warrants, wanted persons and persona non grata to be shared.

In addition, security cooperation agreements cannot be made with countries such as France and Belgium. Information sharing within the Turkish Ministry of Foreign Affairs on issues such as military service, identity, and citizenship is severely hindered. Data of this type cannot be taken from foreign countries. Similarly, operational cooperation with EUROJUST, the EU's judicial cooperation unit for trans-border organized crimes, is impossible. For this reason, problems are invariably encountered in extradition cases and regarding the sharing of information and documents in the judicial field.

Finally, foreign capital cannot be easily invested in Turkey. Legislation does not permit the applicable data to be transferred to the relevant organisations in Turkey. Turkish businessmen cannot take data from their partners in foreign countries and problems are experienced. The pre-condition of effective protection of personal data is necessary before participation in some tenders can be authorized. Hence, Turkey is characterized as 'unreliable country' on data security.

Taking into consideration all the issues mentioned above, there is clearly an unequivocal requirement for the entry into force of an independent and inclusive law as immediately as possible.

II. DRAFT LAW ON DATA PROTECTION

A. BACKGROUND

The Turkish Government is committed to harmonizing its legislation in compliance with the National Program for the Harmonization of Turkish Legislation with EU Law. Accordingly, the Draft Law on the Protection of Personal Data mainly follows the CoE Convention, the EU Directive and the Commission Decision 2001/497/EC of 15 June 2001 on SCCs for the transfer of personal data to third countries[152].

The first studies about a Draft Law date back to the late 1980s. Even in the 2000s various drafts were still being prepared by the Ministry of Justice,

[152] See the Commission Decision at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:en:NOT, accessed on: 19.07.2013

but studies could not be finalized. A new Commission, established in 2004, canvassed 53 institutions, including public sector institutions, universities and non-governmental organisations for their opinions. The Ministry of Justice sent the Draft to the Prime Ministry in 2006. Thereafter it was referred to Turkish Grand National Assembly (TGNA) by the Prime Ministry in 2008. The Draft was sent to Justice Commission on 2 May 2008 and was referred by the National Assembly Justice Commission on 7 May 2008 to a sub-commission. After several meetings about the Draft, the sub-commission suspended its studies due to its busy agenda. Eventually, when the draft before the Justice Sub-Commission could not become law owing to TGNA elections, it was annulled pursuant to Article 77 of Internal Regulation of the National Assembly. It was then returned to the Prime Ministry.

The Ministry of Justice, however, continued studies related to the subject when the Draft Law was returned to the Prime Ministry. One particular project, entitled 'the Project on Personal Data Protection' was begun in early 2011[153]. The aim of the project is to support the Draft Law to be enacted in line with the EU Acquis. Consequently, in co-operation with a Dutch Project partner Considerati, workshops were held in 2011. The programme began with the participation of various public institutions in Ankara and was completed with a workshop in Istanbul including representatives from the private sector on 7 October 2011.

In March 2012, in a meeting held in the Prime Ministry with the authorities, the Draft Law was again discussed. The Ministry concluded that the Draft Law should not be referred to the Assembly again in its current shape and instead, be referred to the Prime Ministry in a more understandable manner after renewal.

Thereupon, a working group under the aegis of the Ministry of Justice was formed. This working group was drawn up in line with the criticisms and sug-

[153] See the Project called "*Support to Better Introduction of the Data Protection System in Turkey*" available at: http://ec.europa.eu/enlargement/pdf/turkey/ipa/2011/part2/tr2011.0123.13_data_protection_system.pdf, accessed on: 20.07.2013

gestions regarding the current Draft law. As a result of all the assessments made of the Draft, it was finalized and referred to the Prime Ministry under the name of 'Draft Law on Protection of Personal Data[154]' on 8 June 2012. The Draft remains in the Prime Ministry on the grounds that a change is required to the structure of the DPA.

B. ASSESSMENT AND CRITICISIM

The Draft Law has been submitted for criticism to various EU institutions such as the European Commission and Eurojust. These criticisms have led to substantial changes, though it should be stressed that since the document has not had parliamentary approval it is not an official draft law. This means many provisions, such as the structure of the supervisory board, could still be altered during subsequent ministerial reviews. Nevertheless, the proposed Draft Law follows the CoE Convention and the EU Directive closely. The terms, definitions and institutions of the general data protection system have mostly been adopted by verbatim translation. However, there are also some arrangements peculiar to Turkey and its legislative system.

The purpose of this Draft Law is to protect fundamental rights and freedoms of people in the processing of personal data and to set forth principles and procedures which bind natural or legal persons who process personal data. The provisions apply to natural persons whose personal data are processed as well as to natural or legal persons who process such data fully or partially through automatic or non-automatic means.

The following critique summarises 9 major issues with the Draft Law as it currently stands. Each discussion begins with a short summary followed by suggestions of what should be done, if applicable.

1. Definitions of some concepts in the Draft are different, broader or more stringent than those of the EU Directive.

According to Article 3(g), data controller means the natural or legal per-

[154] See the Draft Law in Turkish at: http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Kanuntas/kisiselveriler.pdf, accessed on: 20.07.2013

son that is responsible for establishing and managing the data registry system. Such a definition is more stringent than the EU Directive. Further, the statement 'determines the purposes, conditions and means of the processing of personal data' should be added to the end of the sentence. Moreover, there is no definition of 'data subject's consent', 'representative', 'third party[155]' and 'recipient' in the Draft. These should be added in line with the EU Directive.

A definition of personal data was extended to cover legal persons in the previous 2008 Draft, whereas the EU Directive is limited to the protection of personal data of natural persons. Including legal persons would lead to a high administrative burden and expand the scope of the law to such an extent that effective enforcement would be difficult. Therefore, taking into account the criticism and particularly the Article 20(3) of Turkish Constitution, the Ministry of Justice took the decision to remove the term 'legal persons' from the renewed Draft.

2. Processing of personal data will be organised with a specific framework law. General principles will be determined through the Draft

According to the Draft, personal data must be processed in a way compatible with the law and rules of veracity (fairly and lawfully). They must be collected for specified, clear and legitimate purposes and they must not be reprocessed contrary to those purposes. Moreover, these data must be relevant, adequate and proportionate with the reason of collection or further processing. They must be accurate and kept up to date, when necessary. At this juncture, the term 'when necessary' is an unnecessary addition, because personal data should always be kept up to date. If no changes are necessary, then the data is up-to-date. Furthermore, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. These principles are required to be taken into consideration in all data processing.

[155] Ironically, the term 'third party' had been defined in the 2008 Draft Law.

3. Personal data will be processed only with the explicit consent of the data subject with some exceptions

First of all, it should be noted that the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal[156]. As a rule, personal data may only be processed with the explicit consent of the data subject in the conditions clearly specified under the laws. In case of an objection by the data subject, data cannot be processed except for the fulfilment of obligations foreseen in the laws. The exceptions of this rule have been indicated in Article 5(2) as follows: clear specification by laws, vital interests of a person who is incapable of explaining his/her consent, conclusion and performance of the contract, making public by the data subject and fulfilment of legal responsibilities of data controller.

Regarding this Article, it can be seen that the grounds of justification for lawful data processing are different. The Draft makes a distinction between processing on the basis of consent and other grounds. Such a distinction is not made in the Directive. Actually, this is an important category as it allows for the balancing of interest. In addition thereto, it would be appropriate to incorporate consent, not as a separate ground, but as a ground equal to the others. Apart from this, the ground of vital interest is broader in the Draft, as it also covers the protection of 'another person where a data subject is incapable of giving his consent'.

4. It introduces the prohibition of the processing of special categories of data.

The processing of special categories of data (sensitive data) is prohibited. This consists of information relating to race, ethnic origins, political views, philosophical beliefs, religion, sect or other beliefs, membership to certain associations, foundations or trade-unions, health or sexual life[157]. The limited exceptions of this rule are also indicated in Article 6.

---

156 Supra note 135, p.98

157 In 2008 Draft, 'sexual life' was not regarded as sensitive data, it was covered under private life.

According to Article 6(2) (a), special categories of data may be processed if the data subject has given his 'unambiguous' consent. Such consent should be changed to 'explicit consent' since this is stronger than unambiguous consent in the EU[158]. An exemption also applies to data which has been made public by the data subject. In this case, 'manifestly' should be inserted between 'made' and 'public' in pursuant of the EU Directive. For sensitive data to be processed it must be absolutely clear that the data subject wishes the data to be public.

5. Rights such as obtaining information and correction are provided to the data subjects.

According to Article 9, data controllers shall be obliged to inform the data subject about the identity of data controller, purposes and forms of data processing and their right to obtain information and rectification. The data subject shall be entitled to apply to the data controller to learn whether personal data concerning him has been processed, request information if any personal data is processed, demand the rectification of the data content if there is incompleteness or inaccuracy and demand deletion or destruction if it is contrary to law with notification of the processes to be made to third parties to whom the data is transferred.

According to Article 7(2), personal data shall be deleted, destroyed or anonymized upon demand by the data subject provided that their preservation is required under the relevant legislation or that the liabilities under a contract have been completely fulfilled. This provision can be criticized.

Firstly, what is the difference between delete and destroy? Yet, when the terms 'rectification, erasure or blocking' are used in the EU Directive, the Draft prefers to use such terms. According to the Draft's preamble, 'delete' means, for example, deletion of personal data from documents, files, CDs and hard disks. As for 'destroy', it refers, for instance, to destruction of materials such as documents, files, CDs and hard disk data. Although such a distinction is made, it is still confusing and should be parallel with terms in the EU Directive.

[158] The 2008 Draft had required written consent for the processing of special categories of data.

Secondly, personal data should also be deleted if it is no longer necessary for the purposes of processing. In other words, it should not be solely dependent on the wishes of the data subject. Therefore, the statement 'no longer' should be added before the term 'required'.

6. Data transfer to third countries is restricted.

Transfer of personal data is set forth in Article 8 of the Draft. As a rule, personal data can be transferred to third countries in the event that there is an adequate level of protection in the foreign country from which data is requested and the conditions specified in this Draft are met. The exceptions of this rule have been indicated in Article 8(3). 'The data concerned have been made public by the data subject' is one of the derogations of the main rule. This is a somewhat strange addition. Is this for data published on the internet? This exemption does not exist in the Directive. Therefore, this statement should not be derogated and should be removed from the Article.

In Article 8(5) (a), 'the international conventions to which Turkey is a party' is one of the criteria for assessing which foreign country has an adequate level of protection. If Turkey is to ratify the CoE Convention, it would be better to explicitly mention in the Draft that one of the criteria for assessing the adequacy of the level of protection of a third country is to see if that country has both ratified and implemented the Convention and its additional protocol.

Similarly, in Article 8(5) (b), 'the state of reciprocity concerning data transfer between the country requesting the personal data and Turkey' is also accepted as one of the criteria for assessing the adequacy of the level of protection of a third country. This is by no means a data protection element and is an unnecessary addition. It should be deleted.

Moreover, personal data concerning race, ethnic origins, political views, philosophical beliefs, religion, sect or other beliefs cannot be transferred to third parties and foreign countries without 'consent' of the data subject. Instead of this usage, it would be better to say that either consent or when sufficient guarantees are in place, taking into account the necessity and proportionality

of such transfer. Again, it is important to emphasise that when dealing with sensitive data, it should always be 'explicit consent'.

Finally, 'health and sexual life' has not been specified in the section dealing with the transfer of sensitive data to third countries. It is inexplicable why there no distinction between personal data concerning 'health and sexual life' and others in the Draft. In order to achieve coherency with the other provisions regarding sensitive data in the Draft, this data should be incorporated here.

7. Administrative and criminal sanctions have been provided.

According to the EU Directive, Member States must lay down the sanctions to be imposed in case of infringement of the national provisions adopted pursuant to this Directive. In this regard, with the Draft, in case of actions contrary to the obligations determined in the Draft, judicial and administrative sanctions have been introduced in parallel with the Turkish Criminal Code. For instance, according to Article 26(3), a data controller who fails to delete or anonymise personal data in breach of Article 7 of the Draft shall be sentenced to a term of imprisonment from six months to one year. The term 'destroy' is not included. In order to achieve harmony with other relevant provisions, this term should be incorporated here.

8. An independent Data Protection Board will be established.

DPAs operate as one of the key actors in the field of privacy regulation, ensuring civil liberties and consumer rights by supervising and enforcing compliance with data protection policies. When it comes to effective regulation the issue of 'complete independence' of the DPA is of vital importance in terms of protection of personal data[159]. It is generally accepted that the presence of three elements is primarily required: Institutional, Functional (fulfilling its duties without taking orders and instructions) and Financial (budget and budget planning) Independence.

[159] Indeed, although the term 'complete independence' is used in the EU Directive, as one might expect there is no institution, organisation or individual who claim to be completely independent. Nevertheless, the wording refers to the increased relevance the EU put on the autonomous status of DPAs.

It is inconceivable that the DPA will be an institution affiliated functionally to a Ministry or a public institution, acting under their supervision and according to their instruction. When DPAs in European practice are examined, it is clear that they are institutions with an independent budget, secretariat and regular personnel with administrative and financial autonomy. In a case opened by EU Commission against Germany, the ECJ declared that Germany had breached Article 28(1) of the Directive because the authorities had established a process to monitor the processing of personal data which was subject to State scrutiny. Thus, it was not completely independent as required by that provision[160].

Regarding the abovementioned criteria and the EJC' decisions, the previous 2008 Draft Law did not provide full independence as stated in the CoE Convention and the EU Directive. The EU Commission therefore cited the issues stated above in its criticisms regarding the current draft and expressed the view that any supervisory authority formed must be established with full independence.

The legal and political realities within EU Member States indicate that extremely diverse interpretations of the term 'complete independence' are prevalent. Although the aims provided in the Directive are supposed to be binding, Member States are allowed some latitude in working out the details of the national legislation that is finally implemented[161]. This is why the legal structures and the status of DPAs differ from country to country. These legal details determine what kind of powers and duties are delegated and whether or not DPAs are able to work independently and effectively.

In the EU, the members of DPAs are appointed by special procedures, often involving Parliament. Some are appointed by the Government, such as in Ireland, Luxembourg and the UK, while some are appointed by the Minister of

[160] See Case C-518/07 *Commission v. Germany*, para 56. The EJC also took a similar view about Austria in 2012. (See Case C-614/10 *Commission v. Austria*, 16 October 2012)

[161] Simitis Spiros, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, Iowa Law Review, Volume:80, 1995, p.452

Justice, such as in Denmark and the Netherlands[162]. Alternatively, representatives of the DPAs are elected and can only be dismissed by Parliament with the consent of the Senate, as in Poland[163].

Despite all these criticisms, the Draft is nevertheless remarkably close to meeting the appropriate criteria. According to the Draft, a Data Protection Agency has been established as a public organization with administrative and financial autonomy to carry out tasks delegated under this Law. The Agency is affiliated with the Ministry of Justice but shall exercise its powers independently. No body, authority, institution or person can give instructions or orders to influence its decisions. The Agency consists of the Data Protection Board and the Secretariat General. The Data Protection Board is composed of seven members. Four members of the Board are elected by the Council of Ministers, two members by the General Assemblies of the Court of Cassation and Council of State from among their own members, and one member by the General Assembly of the Higher Education Board from among lecturers. The Council of Ministers shall elect one of the members of the Board as the Chairperson of the Board[164].

One could argue that there is no Parliamentary involvement in those procedures, most obviously in appointment and dismissal of the members. Such involvement would be a major step towards the provision of independence. Another criticism concerns the process of selecting the Chairperson of the Board by Government (the Council of Ministers). Ideally, the members of the Board should elect their chairperson from amongst themselves.

9. In relation to the implementation of the Law, there are exceptions for areas such as intelligence and judicial activities.

In the Draft, some major exceptions concerning the implementation of the Law have been introduced. Data processing for purely personal purposes, data

[162] Supra note 65, p.104
[163] See relevant Polish Act, available at: http://www.giodo.gov.pl/144/id_art/171/j/en/, accessed on: 25.07.2013
[164] See Article 12 of the Draft

processing within the scope of press freedom, judicial activities by judicial authorities, intelligence activity of the National Intelligence Service and Police Office, and anonymous data processing have been excluded from the scope of the Law. Articles 9, 10 and 25 of the Draft will not be implemented in cases of data processing for the purposes of the prevention of crime and disciplinary proceedings or where data processing is necessary for the State to function, or where supervision acts are required.

III. CONCLUSION

We live in an information community. Information exists in an often bewildering array of forms. It can be printed or written on paper, stored electronically, transmitted by post or electronic means, shared online, or exchanged verbally. There are ways of storing data and transmitting information that many citizens of the world cannot begin to comprehend. Undeniably, this information has changed – and is continuing to change - the way we see the world and how we interact with it. Crucially, it is changing the way we live, and the way we work. Whatever forms the information takes, or the means by which it is shared or stored, it is important that we understand its potential, but also the risks associated with it. This obligation is not just for governments to understand – it is for business, academia and even private individuals. The information community is not going to disappear.

This is why data protection legislation is essential to protect the interests, privacy and identity of individuals who cannot control the use made of their personal information. International expectations increasingly put pressure on countries without data protection legislation to adopt such legislation if they wish to remain part of the international information community. Despite differences in language, legal traditions and cultural and social values, there has been a concerted approach to codify the basic principles that should be involved in data protection legislation.

The EU Directive on data processing practices has been incredibly influential. Its principles have provided the basis for international regulatory responses. It has set the standard for legal definitions of personal data. Moreo-

ver, it successfully harmonized existing regulations, safeguarding individual rights to informational privacy, but also creating a common European system where data could be freely and safely exchanged. Nevertheless, it has flaws. Importantly, it has failed to create a robust legal framework suitable for future data processing and privacy needs. It fails conspicuously to address the rapid changes in how information is collected, stored, transmitted, used, reused, exchanged and sold.

In Turkey, there is currently no specific law regarding personal data protection. Instead, data protection is governed by a variety of general provisions derived from a number of other laws and regulations. This situation cannot continue indefinitely. Though there is a Draft Law on Protection of Personal Data pending before the Office of the Prime Ministry, this Draft Law closely follows the EU Directive. Its strengths and weaknesses are evident in the Turkish Draft Law.

Turkey's motivation to adopt the Draft Law stems from the desire to become a member of the EU. Turkey has introduced the Draft, but it has not yet been accepted as Turkish legislation. This stems from internal constitutional issues which beset the Draft Law and have hindered its implementation for nearly 25 years. Nevertheless, Turkey remains committed to adopting personal data protection laws. This is due to the increasing necessity to exchange information with European institutions regarding security, immigration, military and criminal matters.

The success - or failure - of privacy and data protection in Turkey will not be decided only by the text of the legislation. Its success will also depend on the actions of those called upon to enforce the law. Turkey has an opportunity to draw on a wealth of international, European, and domestic experience, to design protection for personal data which is more than just fit for purpose, but will continue to function in a changing world. It should not be wasted.

♦♦♦♦

BIBLIOGRAPHY

Books and Articles

Aamodt Agnar and Nygard Mads, *Different roles and mutual dependencies of data, information, and knowledge - an AI perspective on their integration*, Data and Knowledge Engineering, Volume: 16, Issue: 3, 1995, (pp.191-222)

Barnes Morey Elizabeth, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive*, Northwestern Journal of International Law & Business, Volume: 27, 2006, (pp.171-197)

Bauchner Joshua S, *State Sovereignty and The Globalizing Effects of the Internet: A Case Study of the Privacy Debate*, Brooklyn Journal of International Law, Volume: 26, Issue: 2, 2000, (pp.689-722)

Bender David and Ponemon Larry, *Binding Corporate Rules for Cross-Border Data Transfer*, Rutgers Journal of Law & Urban Policy, Volume: 3, Issue: 2, 2006, (pp.154-171)

Bergkamp Lucas and Dhont Jan, *Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web*, The EDI Law Review, Volume: 7, 2000, (pp.71-114)

Bing Jon, *The Council of Europe Convention and the OECD Guidelines on Data Protection*, Michigan Yearbook of International Legal Studies, Volume: 5, 1984, (pp.271-304)

Blume Peter, *Trans-border Data Flow: Is There a Solution in Sight?* International Journal of Law and Information Technology, Volume: 8, No: 1, 2000, (pp.65-86)

Bond Robert, *International Transfers of Personal Data - an Update*, Business Law International, Volume: 5, No: 3, 2004, (pp.423-432)

Bainbridge David, *Processing Personal Data and the Data Protection Directive*, Information & Communications Technology Law, Volume: 6, Issue: 1, 1997, (pp.17-40)

Bygrave Lee, *Data Protection Law: Approaching Its Rationale, Logic and*

Limits, London, Kluwer Law International, 2002

Carey Peter, *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Second Edition, 2004

Cate Fred, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, Iowa Law Review, Volume: 80, 1995, (pp.431-443)

Cate Fred, *The Changing Face of Privacy Protection in the European Union and the United States*, Indiana Law Review, Volume:33, 1999, (pp.173-232)

Cate Fred, *The European Data Protection Directive and European-US Trade*, Currents: International Trade Law, Volume: 7, 1998, (pp.61-80)

Charlesworth Andrew, *Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?* Hastings Law Journal, Volume: 54, 2003, (pp.931-969)

Compact Oxford Thesaurus, Oxford University Press, 2009

Corien Prins, *When Personal Data, Behaviour and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter*? SCRIPT-ed, Volume: 3, Issue: 4, 2006

D'afflitto Rosario Imperiali, *European Union Directive On Personal Privacy Rights And Computerized Information*, Villanova Law Review, Volume: 41, Issue: 1, 1996, (pp.305-323)

De Hert Paul and Gutwirth Serge, *Privacy, Data Protection and Law Enforcement, Opacity of the Individual and Transparency of Power*, in Privacy and the criminal law, Claes Erik, Duff R. Antony and Gutwirth Serge (editors), Oxford, 2006, (pp.61-104)

De Waele Henri, *Implications of Replacing the Data Protection Directive with a Regulation - a Legal Perspective*, Privacy & Data Protection, Volume:12, Issue:4, 2012, p.3-5, (pp.3-5)

Flaherty David H., *On the Utility of Constitutional Rights to Privacy and Data Protection*, Case Western Reserve Law Review, Volume: 41 Issue: 3, 1991

Garrie Daniel, Duffy-Lewis Maureen and Wong Rebecca, *Data Protection: The Challenges Facing Social Networking*, International Law & Management Review, Volume:6, 2010, (pp.127-152)

Godbey Briana N, *Data Protection in the European Union: Current Status and Future Implications*, A Journal of Law and Policy, Volume: 2, Issue: 3, 2006, p.818, (pp.803-829)

Hobby Seth, *The EU Data Protection Directive: Implementing A Worldwide Data Protection Regime and How The U.S. Position Has Progressed*, International Law & Management Review, Issue: 1, 2005, (pp.155-190)

Hustinx Peter, *Streamlining Data Protection*, European Lawyer, Volume: 112, 2012

Ilana Saltzman, *The Status of National Implementation of Directive 95/46/EC on the Processing and Free Movement of Personal Data*, European Intellectual Property Review, Volume: 18, Issue: 6, 1996, (pp.680-683)

Jashari Ruzhdi, *Personal Data Protection: A European Value in the EU Integration Process*, Law & Justice Review, Volume: 4, Issue: 1, June 2013, p.245, (pp.241-254)

Jay Rosemary and Hamilton Angus, *Data Protection Law and Practice*, Second Edition, 2003

Johnson Elizabeth H, *Data Protection Law in the European Union*, The Federal Lawyer, 2007

Kaplan Harvey L, Cowing Mark W, Egli Gabriel P, *A Primer for Data-Protection Principles in the European Union*, Defense Research Institute, Munich, 2009

Karst Kenneth L, *The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 *L*aw and *C*ontemporary *Pr*oblems, 1966, (pp.342-376)

Kinton John D, *Managing the EU-US Discovery Conflict*, Law 360, 2008, available at: http://www.law360.com/articles/72082/managing-the-eu-us-dis-

covery-conflict, accessed on: 29.06.2013

Knoppers Bartha Maria and Fecteau Claudine, *Human Genomic Databases: A Global Public Good?* European Journal of Health Law, Volume: 10, 2003, (pp.27-41)

Kong Lingjie, *Data Protection and Trans-Border Data Flow in the European and Global Context,* European Journal of International Law, Volume: 21, 2010, (pp.441-456)

Korff Douwe, *Data Protection Laws in the European Union,* the Direct Marketing Association, 2005

Korff Douwe, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments,* 2010, available at:

http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf, accessed on: 28.06.2013

Kosta Eleni, *Consent in European Data Protection Law*, 2013

Koutsias Marios, *Privacy and data protection in an information society: how reconciled are the English with the European Union privacy norms?* Computer and Telecommunications Law Review, Volume: 18, Issue: 8, 2012, (pp.261-270)

Koutsias Marios, *The International Reach of European Union Data Protection Law and the United States: is International Trade in a Safe Harbour?* International Trade Law & Regulation, Volume: 18, Issue: 2, 2012, (pp.31-45)

Kuilwijk Kees Jan, *Recent Developments in EU Privacy Protection Regulation*, International Trade Law & Regulation, Volume: 6, Issue: 6, 2000, (pp.200-212)

Kuner Christopher, *European Data Privacy Law and Online Business*, Oxford University Press, 2003

Kuschewsky Monika, *Sweeping Reform for EU Data Protection*, European Lawyer, Volume: 112, 2012

Lambert Paul, *A User's Guide to Data Protection*, Bloomsbury Professional Ltd, 2013

Maxeiner James R, *Business Information and Personal Data: Some Common-Law Observations about the EU Draft Data Protection Directive*, Iowa Law Review, Volume: 80, 1995, (pp.619-638)

Maxeiner James R, *Freedom of Information and the EU Data Protection Directive*, Federal Communications Law Journal, Volume: 48, 1996, (pp.93-104)

McGoldric Dominic, *The Charter and United Nations Human Rights Treaties*, in the European Union Charter of Fundamental Rights: Politics, Law and Policy, Steven Peers and Angela Ward (editors), 2004

Mell Patricia, *A Hitchhiker's Guide to Trans-border Data Exchanges between EU Member States and the United States under the European Union Directive on the Protection of Personal Information*, Pace International Law Review, Volume:9, Issue:1, 1997, (pp.147-183)

Mika Raento, *The Data Subject's Right of Access and to be Informed in Finland: An Experimental Study*, International Journal of Law and Information Technology**,** Volume: 14, No: 3, 2006, (pp.390-409)

Monahan P. Amy, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, Law & Policy in International Business, Volume: 29, (pp.275-296)

Morley Deborah and Parker Charles, *Understanding Computer: Today and Tomorrow*, 14th Edition, 2013

Oxman Stephen A, *Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?* Boston College International & Comparative Law Review, Volume: 24, 2000, (pp.191-203)

Rempell Scott, *Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant V Financial Services Authority as a Paradigm of Data Protection Nuances And Emerging Dilemmas*, Florida Journal of International Law, Volume: 18, 2006, (pp.807-841)

Robinson Neil and others, *Review of the European Data Protection Directive*, RAND Corporation, sponsored by Information Commissioner's Office, May 2009

Roos Anneliese, *The Law of Data (privacy) Protection: A Comparative and Theoretical Study*, University of South Africa, 2003

Rowland Diane and Macdonald Elizabeth, *Information Technology Law*, Routledge-Cavendish, Third Edition, 2005

Salbu Steven R, *The European Union Data Privacy Directive and International Relations*, Vanderbilt Journal of Transnational Law, Volume: 35, 2002, (pp.655-695)

Schriver Robert, *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*, Fordham Law Review, Volume: 70, Issue: 6, 2002, (pp.2777-2818)

Schwartz Paul, *European Data Protection Law and Restrictions on International Data Flows*, Iowa Law Review, Volume: 80, 1995, (pp.471-496)

Schwartz Paul, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, Harvard Law Review, Volume: 126, 2013, (pp.1966-2009)

Shaffer Gregory, *Globalization And Social Protection: The Impact of EU And International Rules in The Ratcheting up of US Data Privacy Standards*, Yale Journal of International Law, Volume: 25, 2000, (pp.1-88)

Simitis Spiros, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, Iowa Law Review, Volume: 80, 1995, (pp.445-469)

Swire Peter and Litan Robert, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press, 1998

Watts Mark, *How Far Are We Protected From Ourselves?* Privacy and Data Protection, Volume: 9, Issue 4, 2009, (pp.1-8)

Wong Rebecca, *Data Protection Online: Alternative Approaches to Sensitive Data?* Journal of International Commercial Law and Technology, Volume: 2,

Issue: 1, 2007, (pp.9-16)

Wong Rebecca and Savirimuthu Joseph, *All or Nothing: This is The Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet*, Journal of Computer & Information Law, Volume: 25, 2008, (pp.241-266)

Zins Chaim, *Conceptual Approaches for Defining Data, Information, and Knowledge,* Journal of the American Society for Information Science and Technology, Volume: 58, Issue: 4, 2007, (pp.479-473)

Zinser Alexander, *European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers*, Tulane Journal of Technology & Intellectual Property, Volume: 6, (pp.171-179)

Internet Resources

Data Protection in the European Union: the Role of National Data Protection Authorities, 2010, available at: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf, accessed on: 18.06.2013

European Data Protection Supervisor, Public Access to Documents and Data Protection, Background Paper Series No.1, July 2005, available at:

http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Papers/BackgroundP/05-07_BP_accesstodocuments_EN.pdf, accessed on: 15.06.2013

Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries, p.24, at:

http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf, accessed on: 07.07.2013

Key definitions of the Data Protection Act, online at: http://www.ico.org.uk/for_organisations/data_protection/the_guide/key_definitions, accessed on: 26.06.2013

Model Contracts for the transfer of personal data to third countries, at:

http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm, accessed on: 07.07.2013

Report of the Ad-Hoc Working Group on Employee Data Protection of the Düsseldorfer Kreis, available at: http://www.globalcompliance.com/pdf/german-guidelines-summation-5-24.pdf, accessed on: 29.06.2013

http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, accessed on: 19.06.2013

http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm, accessed on: 07.07.2013

http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Kanuntas/kisisel-veriler.pdf, accessed on: 20.07.2013

http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacy-andtransborderflowsofpersonaldata.htm, accessed on: 17.06.2013

http://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=3ddcafaac, accessed on: 19.06.2013

Cases

Case C-101/01, *Bodil Lindqvist v. Jönköping*, [2003] ECR I- 12971

Case C-518/07, *Commission v Germany*, [2010] ECR I-1885

Case C-614/10 *Commission v. Austria*, 16 October 2012