UNIVERSITY OF ESSEX

SCHOOL OF LAW

LL.M in INTERNET LAW

2012/2013

Supervisor: Prof. Steve Peers

DISSERTATION

DATA PROTECTION LEGISLATION IN ELECTRONIC COMMUNICATIONS SECTOR: COMPARISON OF TURKISH AND EUROPEAN UNION LEGISLATION

Name	**:**	**Onur GENCER**
Registration Number	**:**	**1200930**
Number of Words	**:**	**18032**
Date Submitted	**:**	**12.09.2013**

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

Article 29 Working Party	WP
By-Law on Processing of Personal Data and Protection of Privacy in Electronic Communications Sector	By-Law on Privacy
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	Convention
Council of Europe	CoE
Data Protection Directive	DPD
Draft Law on the Protection of Personal Data	Draft Law
E-Privacy Directive	EPD
Electronic Communications Law	ECL
European Commission	EC
European Convention on Human Rights	ECHR
European Court of Justice	ECJ
European Union	EU
Information and Communications Technology Authority	ICTA
Internet Access Providers	IAP
Internet Service Providers	ISP
Organisation for Economic Cooperation and Development	OECD
Treaty on the Functioning of the European Union	TFEU
Turkish Criminal Code	TCC
United Kingdom	UK
United Nations	UN
United States	US

1. INTRODUCTION

In some respects, the current era is called as information age owing to the fact that the recent developments in the technology have changed our daily lives and cyberspace has become indispensable part of our life. People have become able to make banking transactions, read newspapers even follow breaking news, track public buses and arrange themselves for the next bus service where they wish to go and find nearest hospital, pharmacy or shopping centre to them with the help of the applications installed in their mobile devices. However, while those applications or services give users valuable information, they sometimes need additional information which belongs to them. Hence, intangible information is more valuable than ever and personal data is probably the most crucial one[1] and in order to benefit easiness of such services users share their personal data either being aware or not with telecom operators or other companies which serve those services. Therefore; while presence of such precious asset strikes business organizations' fancy, individuals need to protect their personal information and to prevent disclosure of it. So, that situation gave rise emergence of data protection laws and decision makers have adopted regulations in order to determine the circumstances of processing personal data and to protect privacy of individuals.

According to Ferrers; *collection of personal data is as old as society and one of the oldest habits* of humanity and since the existence of mankind, information has been collected and processed[2]. In the past, personal data was collected probably mostly for the purpose of intelligence and was collected without consent, however in present personal information is collected for being used in several areas; our health data is stored for forming our health history and sometimes it is collected to learn our habits in order to use for marketing etc. Therefore, personal data is very valuable and collection of such a value is important. On the other hand, for the individuals protection of their own personal data is as important as the collection of personal data. Because, as Edwards says, data protection is protecting *informational privacy* and *the right to control what is known about you*[3]. In spite of that, although almost all countries and international legal bodies have pointed out the importance of data protection and have put into force regulations, there is no common definition or legal regime of data protection in a global scale. In the United States (US), there is not a literally

[1] Reed C. (Ed.), 2011, Computer Law, Oxford University Press, 7th Edition, p.573
[2] Rowland D., Kohl U., Charlesworth A., 2012, Information Technology Law, Routledge, 4th Edition, p.147
[3] Edwards L. & Waelde C., 2009, Law and the Internet, Hart Publishing, 3rd Edition, p.445

data protection law[4] and in legislative texts data protection refers to privacy. However, a sectoral approach which suggests enacting more specific rules according to the substance of the sector, is adopted in order to protect privacy in each sector. On the other hand, that caused some sectors to remain not regulated[5]. On the other side of the ocean, at European Union (EU) level, personal data protection law which can be regarded as the most comprehensive form is still in effect. In 1995, European Commission (EC) adopted Directive 95/46/EC Data Protection Directive (DPD)[6] as a mandatory law and therefore 28[7] countries adopted that Directive into their national legislation. DPD determines the general framework of data protection and can be applied to all areas appertaining to processing of personal data.

Although protection of personal data and privacy is a very old concern for individuals, it has emerged in the law field from the beginning of 1970s and the factor triggered was the development of technologies in particular beginning of computers being involved thoroughly in the business sector[8]. Thereupon, first data protection law in national level enacted in Sweden in 1973 and the underlying reason of that law was the development of large mainframes that can only be used in the business sector for complicated transactions[9]. Although those machines were awkward and had a capability of processing limited transactions, it was sufficient to scare decision makers in order to worry about processing personal data. For the next decades, the technology in the computer industry has made a dramatic progress and according to the improvement of microcomputers personal computers were invented and those smart machines have been started to be used not only in business but also at home[10]. However, the actual progress has been experienced in the electronic communications sector by the invention of internet and World Wide Web. Because, internet is a decentralised, borderless, geographical independent and portable structure; people thus can easily gain information on any topic. Beyond accessing the information required, people use internet for communication or carrying out electronic transactions regarding online banking, e-government or online shopping. For the last few years, the Web 2.0 technology has risen which allows creating user-generated contents and provides that websites are transformed

[4] Jorgensen R. F., 2006, Human Rights in the Global Information Society, MIT Press, p.140
[5] Lloyd, I. J., 2011, Information Technology Law, 6th Edition, Oxford University Press, p.21
[6] EC, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data
[7] As of 08.08.2013 EU has 28 member countries
[8] Birnhack M. D., 2008, 'The EU Data Protection Directive: An Engine Of A Global Regime', Computer Law & Security Report 24, p.511
[9] Supra n.1, p.626
[10] Supra n.2, p.148

from static to dynamic[11]. The well known examples of websites that are generated with that technology are social media applications (Facebook, Twitter), video or image sharing sites (YouTube, Instagram) and blog sites etc. Almost each internet user uses at least one of those applications every day without being aware or being aware of the fact that they share their personal data via them. Furthermore, every transaction made in the internet can be tracked, stored and used for some purposes by internet service providers (ISP) or internet access providers (IAP). While reading news on the internet, a user can face an advertisement on the side of the website that related to his/her previous search on search engine or related with the product he/she looked for in any online shopping website. This situation occurs because some information is stored about users' personal behaviours via cookies in order to be used for marketing purposes. While we are not aware, we share our personal data with the third parties and that is a serious threat to our privacy.

In addition to the invention of the internet, there has been another dramatic development in the electronic telecommunications sector: the invention of mobile phones. At first; mobile phones were used as alternative communication devices to fixed phones, but they evolved so much that they have become tools that threaten the market share of personal computers at present[12]. Besides providing a traditional voice communication, those devices so-called smart phones provide some advantages such as allowing internet access and installing applications for the purposes of entertainment to e-government transactions. However, in order to benefit those advantages users have to share some personal information with the third parties and ISPs. However, those data are not used only for the billing services or purpose of giving a high standard service but also for some commercial purposes like marketing. As a result, the concerns about data protection in the electronic communications sector vary and continue to vary.

EC noticed the insufficiency of DPD to address the concerns about data protection in electronic communications sector and enacted a new and specific Directive in 2002 without overriding DPD. Finally, Directive 02/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector which is called as E-Privacy

[11] Supra n.3, p.48

[12] According to the Gartner report in June 2013 traditional pc shipments declined 10.6% in 2013, while tablet shipments increased 67.9%, See: Gartner Says Worldwide PC, Tablet and Mobile Phone Shipments to Grow 5.9 Percent in 2013 as Anytime-Anywhere-Computing Drives Buyer Behaviour, http://www.gartner.com/newsroom/id/2525515

Directive (EPD)[13] in some respects took in force to fill the gaps of DPD. In context of EPD, the obligations of data processors are identified and specific issues related to electronic communications sector, in particular internet, such as processing traffic and location data, public directories, unsolicited commercial communication and cookies are regulated regarding the use of personal data in electronic communications sector. Furthermore, in order to keep pace with the technology, Article 29 Working Party 29 (WP) which was set up under Article 29 of DPD has published some documents stating the opinions on new issues which are not referred directly in EU data protection legislation. Although its opinions and recommendations have no binding force and do not reflect EC's opinions; they provide for Member States and data controllers to get expert advices regarding data protection. Moreover, harmonization of national data protection legislation in all EU State Members has been provided. .

Turkey is one of the most important emerging markets in the world and is a candidate country for full membership to EU. Furthermore, Turkish electronic communications sector is growing considerably like all over the world. That growth and progress are able to relate with the EU candidateship, because Turkey has made a great effort at last decade regarding the adaptation of EU acquis communautaire and thereupon, an independent regulatory authority was established and telecommunication sector in Turkey was liberalized. After the establishment of regulatory authority new regulations have been adopted and although remarkable progress has been reached in the field of electronic communications, further efforts are required to bring the legislation into line with the acquis. Data protection legislation is one of the main fields even there is still no enacted Data Protection Law in Turkey. Nevertheless, privacy is protected by the provisions of Turkish Constitution and with respect to electronic communications sector; regulatory authority has adopted some secondary regulations regarding the processing and protection of personal data.

In this study, data protection legislation in electronic communications sector will be analyzed comparing the legislation in Turkey and EU. Following this chapter, data protection and privacy notions and the relation between them will be examined and the issue 'how data protection law emerged and has been perceived' will be explained. In the third chapter; EU

[13] EC, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector (Directive On Privacy And Electronic Communications)

data protection legislation will be mentioned. Key features and the definitions of the DPD which are also applicable to the electronic communications sector will be given and then main Directive EPD will be explained and the extent of applicability of it to electronic communications sector will be discussed. In the fourth chapter, legislation in Turkey regarding protection of privacy and processing of personal data in electronic communications sector will be given. Also, a short examination will be made about the draft data protection law. In the final chapter, there will be a comparison analysis of EU and Turkish data protection legislation regarding electronic communications sector and some remarks will be made.

2. DATA PROTECTION AND PRIVACY

2.1 Privacy and Relation with Data Protection

Privacy has always been an important concern for individuals and it is admitted as a basic human right in almost all countries. However, privacy is perhaps the most difficult human right to describe[14], because the value of privacy differs according to the cultural and social values so people from different cultures may have a different expectation of privacy[15]. Perhaps the first and the most known definition of privacy was made over a century ago by Warren and Brandeis; "*the right to be alone"*[16]. Alan Westin stated the freedom of individual in his definition of privacy. According to Westin, privacy is "*the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others*"[17]. Miller supported Westin stating; privacy is "*the individual's ability to control the circulation of information relating to him*"[18]. Although there is not a consensus on definition of privacy on a global scale, almost all countries consider privacy as a fundamental human right and include protection of privacy in their constitution[19]. In Europe, privacy is protected by European Convention on Human Rights (ECHR) which has been

[14] Banisar D. & Davies S., 1999, 'Global Trends in Privacy Protection: An International Survey Of Privacy, Data Protection, And Surveillance Laws And Developments', Journal Of Computer & Information Law, Vol. 18, p.6
[15] O'Beirne B., 2009, 'The European Court of Human Rights' recent expansion of the right of privacy: a positive development?', Coventry Law Journal, p.1
[16] Warren S.D., Brandeis L.D., 1890, 'The Right to Privacy', Harvard Law Review, Vol.4 No.5, p.193
[17] Supra n.14, p.7
[18] Cited at supra n.2, p.150
[19] Tan D. R., 1999, "Personal Privacy In The Information Age: Comparison Of Internet Data Protection Regulations In The United States And The European Union", Loyola of Los Angeles International and Comparative Law Journal 21, p.662

signed by 47 Member States that all EU Members and Turkey are included. ECHR guarantees the right to respect for private and family life, one's home and correspondence.

Privacy appears to be constructed at four dimensions: first one is territorial privacy which involves setting limits or boundaries on intrusion into a specific space or area such as searches and video surveillance; second one is bodily privacy which involves the integrity of an individual's body against invasive procedures; third one is data privacy which controls the collecting and processing personal data and the last one is privacy of communications which covers the confidentiality of communication made in forms of telephone, email etc[20]. The term information privacy may be used to refer to the combination of last two dimensions: communication privacy and data privacy[21].

The emergence and widespread use of information technologies have added a new dimension to information privacy, because the collection and processing of personal data have become much easier and cost efficient than ever by means of high capability computers and internet technology[22]. In particular; on Internet, our personal data can be collected and processed in milliseconds which makes our personal data a very valuable asset due to the fact that our personal data including personal behaviours, habits are all known by data processors and used for specific services, advertisements or other services[23]. From the users' point, those services make their life easier and gain plenty of time. On the other hand, possible use of personal data without the consent of the user for the purposes other than the signified purpose for collection may pose a threat to privacy. According to the surveys, concerns over privacy violations are now greater than ever due to the developments in technology[24]. This probability revealed the need for regulation of information privacy, hence data protection law emerged. The Deputy Data Protection Registrar explained the relation between the data protection and privacy after the implementation of DPD with those words: "*data protection is a form of privacy*" [25]. The relation between privacy and data protection is a bit complicated because some argue that they are incompatible notions, on the other hand they refer to same meaning both in legal and academic texts and in some countries such as US. In some respects, while privacy rules are

[20] Supra n.8, p.664
[21] Clarke R., 2006, Introduction to Dataveillance and Information Privacy, and Definitions of Terms, http://www.rogerclarke.com/DV/Intro.html
[22] Supra n.8, p.510
[23] Ibid
[24] Supra n.14, p.4
[25] Supra n.2, p.153

protecting the individuals from interference into their private life by prohibiting collecting and processing personal data, data protection rules specify the circumstances how privacy can be violated legally[26].

2.2 The Emergence of Data Protection

In accordance with the developments in information technologies the concerns on privacy increased in the late 1960s and first general data protection law was enacted in Hesse- one of the German States, in 1970, but the first data protection law in national level was enacted in Sweden in 1973[27]. However, as the relation between data protection and privacy is considered, approval of privacy as a human right is earlier.

Privacy was firstly guaranteed by Council of Europe (CoE) in 1950 at an international level. In the light of Article 8 of ECHR, privacy is a right to be respected and protected in a high level and the scope of privacy is individual's private and family life, home and communication right[28]. That approach can be considered as a milestone in the evolution of data protection[29] because the articles are still in effect and the regulations regarding protection and processing personal data in Europe are based on Article 8 of ECHR. The text of Article 8 is given below[30].

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

[26] Koenig, C., Bartosch A.,Braun J.D., Rames M., 2009, EC Competition and Telecommunications Law, Kluwer Law International, Second Edition, p.510
[27] Bing J., 1984, 'The Council of Europe Convention and the OECD Guidelines on Data Protection', 5 Michigan Yearbook of International Legal Studies, p. 271
[28] Newell B. C. , 2011, 'Rethinking Reasonable Expectations of Privacy in Online Social Networks', Richmond Journal of Law and Technology, Vol. XVII, Issue 4, p.8
[29] Supra n.26, p.514
[30] European Convention on Human Rights, 1953, Art.8

The rapid improvements in information technologies and enactment of national data protection laws in some countries turned international organizations' attention to looking for new regulations in order to determine the conditions of processing personal data[31]. Hence, CoE adopted the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (Convention) in 1980. The Convention contains basic data protection principles which are almost assimilated in the further regulations. In addition, the rules of transborder data flows were established in the Convention.

The Organisation for Economic Cooperation and Development (OECD) is the other international organization that deals with the data protection issue and in 1980 it adopted the 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data'. The importance of that guideline is that it was aimed to harmonize the different national data protection legislations. It would be an effective guideline in global scale because OECD has Members from all over the world which Members are strong economically and a great majority of data is processed by them[32]. However, that document has no binding force and it only constitutes a guideline for Members who wish to enact national data protection law.

Although, both Convention and OECD guideline have no legal forces, many countries considered those documents and adopted some of its rules in their national laws. Both documents ruled that personal data needs to be protected at every step of processing under some principles. The common points of these principles are that personal information must be[33]:

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;
- accessible to the subject;
- kept secure;
- deleted after its purpose is completed.

[31] Supra n.14, p.10
[32] Busch A., 2010, 'The Regulation of Privacy', Jerusalem Papers in Regulation & Governance Working Paper No. 26, p.6
[33] Supra n.14, p.11

Later, in the beginning of 90s, United Nations (UN) adopted its own guideline regarding regulation of personal data files bearing in mind the protection of personal data is a human right[34].

In EU, the right to personal data protection is guaranteed under Treaty on the Functioning of the European Union (TFEU) which forms the EU's constitutional basis; therefore, personal data is protected in a high level in EU. Article 16(1) TFEU states; "everyone has the right to protection of personal data concerning them". Article 16(2) obliges European Parliament and Council to determine the rules of processing personal data and to provide compliance with these rules under the control of independent authority. Hence, EU adopted a General Data Protection Directive in 1995 which lays down the basic principles of data protection and is applicable to all areas. However it remained incapable in the area of electronic communications sector and protection of personal data in electronic communications has been regulated with specific Directive named E-Privacy Directive since 2002. When it is examined the main purpose of the EU Directives, it is obviously seemed that they are based on the provisions of Charter and TFEU.

Turkey is one of the signatory countries of ECHR and is a member of both OECD and UN and is a candidate for full EU membership, however there is still no specific data protection law. Although there are some provisions regarding protection of privacy in constitutional level, they are inadequate for protection of personal data. However, there is a substantial legislation regarding the processing of personal data in electronic communications sector.

3. EU LEGISLATION ON DATA PROTECTION

3.1 General Data Protection Directive

As mentioned above, EU was the last international organization putting legislation regarding data protection.. Even, some of the Member States such as Germany and United Kingdom (UK) had national data protection laws before they are obliged to adapt DPD. One of the reasons of that fact was the Convention, because all EU Member States has signed the Convention and EU recommended Member States to ratify it. However, Member States did

[34] United Nations, 45/95 Guidelines For The Regulation Of Computerized Personal Data Files, http://www.un.org/documents/ga/res/45/a45r095.htm

not make much effort to consider the Convention and only six[35] of them ratified it[36]. The inconsistency caused from the existing laws in some Member States that enacted before Convention and the inadequate adaptation of Convention necessitated the EU to concern on data protection issue. In order to have a harmonized legislation in data protection area, DPD was put in force in 1995 requiring adoption by Member States until 1998.

The main idea of the Directive is stated in the first Article by referring the right to privacy as it is stated both in the TFEU and ECHR. Member States are obliged to take measures in order to protect the fundamental rights and freedoms of natural persons, however those measures shall not prohibit the processing of personal data[37]. The essential aim of DPD is to determine the limits and the conditions under which personal data can be processed and provide the free movement of such data under certain circumstances.

The substantial feature of that Directive is to be a general directive establishing a general framework on data protection; therefore, its provisions can be applied to all forms of data without making discrimination between sectors[38].

3.1.1 Essential Definitions in DPD

3.1.1.1 Personal Data

The key terms in Article 1(1) DPD specify the scope of the data protection. "*Processing personal data*" expression obviously shows that DPD deals with only processing personal data[39]. Personal data is described under Article 2 DPD as: '*any information relating to an identified or identifiable natural person*'; ... , in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. It can be deduced from the definition that the content of the information is irrelevant[40]. According to that description, name, surname, social security number or contact details are regarded as personal information. Indeed, data that can be

[35] Denmark, France, Germany, Luxembourg, Spain, UK
[36] Supra n.5, p.33
[37] Supra n.26, p.516
[38] Dolin R.A., 2010, 'Search Query Privacy: The Problem of Anonymization', Hastings Science & Techonology Law Journal, Vol. 2, No. 2, p.140, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1620198
[39] Lipton J. D., 2010, 'Digital Multi-Media and the Limits of Privacy Law', Case Western Reserve University Case Research Paper Series in Legal Studies Working Paper 2010-16, p.4 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1584737
[40] Supra n.26, p.517

correlated with individual is in the scope of personal data. However, the data can be correlated with legal persons is not regarded as a personal data in the scope of DPD[41].

Although in some cases deciding certain information is whether personal data or not is peremptorily obvious, in some cases the decision may be given relatively. While a person's image with additional information which helps to identify a specific person is considered as personal data, a sole image is not regarded a personal data. In a similar manner, a sound of individual may be considered to be personal data if it identifies a specific person[42]. In addition to those, some information special to electronic communications need additional interpretation in order to decide whether it is personal data or not. IP addresses are one of those. On Internet, IP addresses are unique and identify computers connected to the Internet. IP addresses are assigned to computers by ISPs dynamically or statically depending on the users' choice of connection[43]. It is easy to determine the individual who uses static IP address but if a person uses dynamic assignment it is not possible to identify the person from sole IP address. However, a user's approximate geographical location can be deduced from his IP address and even a person can be identified by additional information which ISPs have. Due to this debate, while Google which uses IP addresses to improve the ability of its services claims IP addresses are not personal data, EU has opinion in the opposite direction and declared; IP addresses should generally be regarded as personal information[44]. Moreover, WP clarifies this debate in its WP 136; *"unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side*", stating that these considerations will apply equally to search engine operators[45]. The other debate is whether email address of individual is a personal data or not because the person's name, political or ideological view or working place may be guessed from the prefix or domain name[46]. However, considering the latter Directives, EU qualifies email address as a personal data[47]. Also, cookies which are small text files and used for several purposes on Internet such

[41] Bell R. & Neil R., 2004, EU Electronic Communications Law, Richmond Law & Tax Ltd., p.114
[42] Bergkamp L. & Dhont J., 2000, 'Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web', EDI Law Review 7, p.74
[43] Kuner C., 2003, European Data Privacy Law and Online Business, Oxford University Press, p.53
[44] EU: IP Addresses Are Personal Information, 2009, http://www.cbsnews.com/2100-205_162-3734904.html
[45] Article 29 - Data Protection Working Party, 2008, 'Opinion 1/2008 On Data Protection Issues Related To Search Engines', p.8
[46] Magee J., 2002-2003, 'The Law Regulating Unsolicited Commercial E-Mail: An International Perspective', 19 Santa Clara Computer & High Tech. Law Journal, p. 364
[47] Supra n.16, p. 366

as storing information for authentication to website or habits of users; are the subject of a debate whether they are considered to be personal data[48]. Those debates will be explained in the following chapter in detail.

3.1.1.2 Consent

Owing to the main objective of DPD is the protection of informational privacy; the data subject has a crucial role, because the consent of him is prerequisite for processing personal data[49]. Consent is defined in Article 2(h) DPD as; "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*"[50]. WP clarified the concept of consent as*; it may be a handwritten signature or oral statement or share his name and address with the third parties to obtain information. Even, dropping a business card in a bowl indicates the consent of data subject and is adequate to constitute a processing of personal data*[51].

Consent must be a clear and unambiguous indicator of the data subjects' wishes[52]. Although unambiguous consent is not defined precisely, the term "freely given" is interpreted as there should not be any doubt or any pressure about the consent of data subject. For instance, if any hierarchical relationship exists between data controller and data subject, therefore if data subject feels obliged to give his consent or in case of refusal of giving his consent is penalized, that consent may not be regarded as freely given[53].

Besides, consent must be specific for the purpose of processing personal data which means given consent will be invalid if personal data is used for other purposes which are not stated at the time consent given[54]. That fact necessitates that the data subject must be informed properly regarding the purpose of collection his data and the details and scope of processing. Because he must understand the facts and be able to evaluate the risks to his privacy in order

[48] Supra n.43, p.53
[49] Blume P., 2012, 'The Inherent Contradictions in Data Protection Law', International Data Privacy Law, Vol. 2, No. 1, p.29
[50] Supra n.6, Art.2
[51] Article 29 - Data Protection Working Party, 2011, 'Opinion 15/2011 On The Definition Of Consent', p.11,
[52] Supra n.26, p.542
[53] Supra n.42, p.77
[54] Supra n.26, p.543

to be able to decide freely whether giving his consent[55]. Moreover, consent must be revocable which means that data subject has an opportunity to withdraw his consent if he changes his opinion on sharing his personal data[56].

EC used the term "explicit consent" in Article 8 which determines the circumstances of processing special categories of data. However, like the unambiguous consent that term needs additional interpretation too[57]. The term explicit is stricter than the unambiguous and therefore some Member States require that explicit consent must be given written[58]. In order to differentiate the terms explicit and unambiguous WP helped us in the official papers: "*meaning an active response, oral or in writing, whereby the individual expresses his/her wish to have his/her data processed for certain purposes. Therefore, express consent cannot be obtained by the presence of a pre-ticked box. The data subject must take some positive action to signify consent and must be free not to consent*"[59].

The definition of consent is assimilated in EPD and the same criteria shall be applied in the context of EPD to determine the validity of the given consent[60].

3.1.1.3 Sensitive Data

Although any information related to a person can be considered as a personal data, which of them should be classed as a sensitive data is more significant in order to provide a special protection[61]. Sensitive data can be processed if and only if the explicit consent of the data subject exists. Article 8 DPD describes which information should be considered as sensitive data and should be processed specially as below:[62]

- racial or ethnic origin,

[55] Borghi M., Ferretti F. & Karapapa S., 2013, 'Online Data Processing Consent Under Eu Law: A Theoretical Framework And Empirical Evidence From The UK', International Journal of Law and Information Technology, Vol. 21, No. 2, p.122
[56] Supra n.26, p.543
[57] Supra n.55, p.119
[58] Supra n.26, p.537
[59] Altheim M., 2011, 'The Meaning of "Consent" in the EU Data Protection Framework: A New Article 29 Working Party Opinion', http://ediscoverymap.com/2011/07/the-meaning-of-%E2%80%9Cconsent%E2%80%9D-in-the-eu-data-protection-framework-a-new-article-29-working-party-opinion/
[60] Supra n.55, p.119
[61] Supra n.5, p.41
[62] Supra n.6, Art.8

- political opinions,
- religious or philosophical beliefs,
- trade-union membership,
- health information
- sexual life.

In Lindqvist case, the European Court of Justice (ECJ) was asked to give an opinion to Swedish Courts about Mrs. Lindqvist's website where some personal information including full names, telephone numbers and references to hobbies and jobs of her colleagues were published without obtaining their consent. The case was discussed in many ways and one of the rulings of the ECJ was related to publishing health information of individual without being authorized by data supervisory authority[63]. Because, Mrs. Lindqvist mentioned on her website how one of her colleagues got an injured leg and for that reason she was working part-time. The ECJ held that; "*in the light of the purpose of the Data Protection Directive 95/46/EC, the expression "data concerning health" used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual"*[64]. Consequently, ECJ interpreted the sensitive data widely and information about foot injury of individual was considered in the scope of Article 8(1) DPD[65].

3.1.2 Data Protection Actors

3.1.2.1 Data Controller and Processor

Data controller is a natural or legal person, public authority, agency or any other body which determines the purposes and means of the processing of personal data. Under the provisions of DPD, controller must notify the national supervisory authority for its purpose(s) to process personal data before carrying out operation. In this context, it is obvious that data controller is the part which has most obligations under DPD[66]. In some conditions, personal data can be

[63] Supra n.5, p.43
[64] Case C-101/01, 2003, Criminal proceedings against Bodil Lindqvist, http://curia.europa.eu/juris/liste.jsf?language=en&num=C-101/01
[65] Wong R., 2007, 'Data Protection Online: Alternative Approaches to Sensitive Data?', Journal of International Commercial Law and Technology Vol. 2, Issue 1, p.11
[66] Supra n.3, p.456

processed by data processor on behalf of data controller under circumstances that are indicated by DPD[67].

Recent developments in electronic communications sector have caused an increase in the diversity of services given and users are aware or not their personal data is collected, stored and processed for several purposes by those services. Therefore, number of data controllers has increased and sometimes that constitutes a question of debate whether the third party has an obligation as a data controller under the provisions of DPD. As that issue will be examined in detail in the following of this paper; telecommunication operators, internet service providers, search engines, social network providers, email service providers and online shopping sites etc. are all considered data controllers and have some obligations under certain circumstances.

3.1.2.2 Data Subjects

Data subject means an individual who is the subject of personal data. The DPD text points to identified or identifiable natural person while referring data subject. Identifiable person is defined as one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. It is obvious from the above definition, DPD deals with only natural persons and companies or legal persons are not in the scope of DPD. However, DPD does not prohibit the covering of legal persons and in some Member States[68] legal persons are included in the scope of national data protection laws thereof[69].

According to the provisions of DPD, the data subjects have rights to protect their privacy in contrast to the obligations of the data controllers and processors[70]. Undoubtedly, the most important right of data subjects is the right to their privacy. Beyond this, Article 12 sets out the rights of data subject in order to accessing data[71].

> *Member States shall guarantee every data subject the right to obtain from the controller:*

[67] Ibid
[68] Austria, Denmark, Italy, Luxemburg
[69] Supra n.43, p.55
[70] Supra n.5, p.56
[71] Supra n.6, Art.12

a) without constraint at reasonable intervals and without excessive delay or expense:

- *confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,*
- *communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,*
- *knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);*

b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

3.1.2.3 Supervisory Agencies

One of the most important provisions of DPD is which imposes an obligation to Member States to set up an independent supervisory authority. This authority is responsible for monitoring the appliance of national data protection law in the Member State, giving advice to the government about administrative measures and regulations and starting legal proceedings in case of violation of data protection regulation. They can receive complaints from individual concerning the protection of his rights and freedoms in regard to the processing of personal data. Therefore, they have power to investigate the complaint and access to data and obtain all information relating to the complaint. Also they have power to impose sanctions to data controllers. However, they are not in a replacement condition to courts, individual has a right to open a lawsuit in the courts without lodging complaint to supervisory authority.

Perhaps, the most important role of supervisory authority is ruled under Article 18 DPD. Hereunder, data controller must notify the supervisory authority before carrying out any operation. This notification must involve at least these information: the name and address of the controller, the purpose or purposes of data processing, a description of the category or categories of data subject, the recipients or categories of recipient to whom the data might be

disclosed, possible data flows to third countries, brief description of measures taken in order to ensure secure processing.

3.1.3 Data Protection Principles

DPD sets out five principles for qualified data management and processing which are stated under Article 6 as below[72]:

a) Personal data must be processed fairly and lawfully,
b) Personal data must be collected for specified purposes and processed for only certain purposes.
c) Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected.
d) Personal data must be accurate and kept up to date.
e) Personal data must not be kept longer than is necessary.

'The purpose specification' which is mentioned under Article 6(b) is the first and also prerequisite principle in applying data protection laws and processing personal data[73]. According to the provision, the purpose of the processing personal data must be notified before the collection of data in order to ensure data subject is aware of the extent of processing his personal data[74]. Thus, he can give his consent for the specific purpose. However, it is not sufficient only to specify the purpose before the collection of personal data; also it must not be further processed in an incompatible way[75]. Otherwise, the consent of the data subject would not be valid anymore.

The extensive interpretation of the lawfulness and fairness principle is stated under Article 7. To legitimise the data, there should be a clearly and freely given consent of data subject or where processing of personal data is for one of the five circumstances[76]. Furthermore, under the provisions of Section IV of DPD, data subjects should be given information about the extent of information that will be collected and purpose of collecting or processing in order to

[72] Supra n.6, Art.6
[73] Article 29 Working Party, 2013,' Opinion 03/2013 On Purpose Limitation', p.4
[74] Supra n.26, p.560
[75] Supra n.73, p.4
[76] Supra n.2, p.160

decide whether the data is collected fairly or whether the information they give is not excessive for certain purpose[77].

Proportionality principle which refers to the third principle determines the limits of the data can be collected[78]. Data controller shall not collect data more than needed for the specified purpose of processing. In other words, there must be a rational relation between the collected personal data and purpose of processing.

According to the fifth principle the data must be kept no longer than it is needed. This principle has a crucial role in electronic communications sector. Because some data including call detail records and location data are regarded as personal data and keeping them for longer terms constitute a threat to privacy. Moreover, the retention of data in publicly available electronic communications services and public communications networks is regulated under Data Retention Directive[79] in detail.

3.2 E-Privacy Directive

The rapid improvement in the electronic communications sector, in particular Internet and commencing of mobile phones taking a serious place in our lives were the most striking developments in the beginning of millennium. These developments caused a change of the informational privacy in negative side, because individuals concern on privacy has increased. On the other side, EC took notice of these concerns and decided that current general Directive is not sufficient to cover the specific issues in electronic communications sector[80]. As a result, Directive 2002/58 (mentioned as EPD above) adopted as a sectoral approach in order to deal with the privacy concerns only in electronic communications sector. EPD was prepared in a technology independent manner in order to involve current and future communication types[81]. However, some new technologies and issues need additional interpretation and at that point WP has published its opinions on these specific concerns such as search engines and social networks.

---

[77] Kirsch M., 2011-2012, 'Do-Not-Track: Revising The EU's Data Protection Framework To Require Meaningful Consent For Behavioural Advertising', Richmond Journal of Law & Technology, Vol.18 Is.1, p.4
[78] Supra n.26, p.560
[79] EC, Directive 2006/24/EC of the European Parliament and of the Council Of 15 March 2006 On The Retention Of Data Generated Or Processed In Connection With The Provision Of Publicly Available Electronic Communications Services Or Of Public Communications Networks And Amending Directive 2002/58/EC
[80] Supra n.1, p.622
[81] Supra n.46, p.370

However, EPD does not replace DPD and the general rules of DPD are always effective. Besides that, the provisions of EPD override the provisions of DPD if there is any rule regarding the processing of personal data in electronic communications sector. It is explained in legal theory; while EPD can be considered as a lex specialis, DPD can be considered as lex generalis[82]. For instance, EPD refers to DPD for some definitions such as personal data and consent, on the other hand traffic data is explained within EPD due to be sector specific[83]. So, EPD complements DPD regarding electronic communications sector.

Main objective of EPD is stated under the first article as to protect of fundamental rights and freedoms, in particular right to privacy with respect to the processing of personal data in the electronic communications sector. EPD extends the scope of protection to legal persons and therefore legal persons have almost same protection level as well as individuals[84]. Because, EC preferred to use the term 'subscriber' in Article 2 which covers both natural and legal persons.

3.2.1 Obligations Under the EPD

3.2.1.1 Security of Services

EPD ensures security of services in electronic communications by obliging providers of services to take appropriate security measures in order to prevent disclosure of personal data. In Article 4(1a), the risks that may occur and the scope of the measures which providers are shall take are listed. According to the provisions, providers are obliged for not only purposely or unlawfully but also accidentally processing, access or disclosure of personal data. In order to provide security of services given by provider of a publicly available telecommunications services, providers take measures including but not limited to ensure only authorized personnel could access to data for only legitimate purposes and ensure having a sufficient security policy.

Perhaps, the vital point of the Article 4 is that providers are obliged to inform their subscribers if there has been any risk of a breach to network security. Providers shall also inform the

[82] Supra n.26, p.520
[83] Ibid
[84] Supra n.1, p.623

responsible data supervisory agency about this risk[85]. The reason of the importance of this provision is the providers are not pleased with this obligation, because in the event of any risk they could lose reputation. On the other hand, the purpose and opinion of the EC is exactly to incite providers to implement appropriate and effective security policy and to invest in further measures to provide security of services.

3.2.1.2 Confidentiality of Communication

The other obligation under EPD, contrary to the Article 5 of obliging providers, obliges Member States to take appropriate measures by adopting national laws in order to ensure confidentiality of communications. According to the provision, Member States shall prohibit all electronic interception or surveillance such as listening, taping, storage or other kind of activities unless subscriber has given his consent[86]. However, these measures shall not affect the nature of the operation needed for electronic communication service providing that these operations are carried out lawfully and for the purpose of providing evidence of a commercial transaction or of any other business communication.

Although the confidentiality provision seems very strict, there is an exception under certain circumstances. These exceptions are ruled by Article 15 and they are applicable to safeguard "*national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system"*[87]. However, these measures must be necessary, appropriate and proportionate measure within a democratic society and in accordance with the general principles of Community Law[88] such as the right of privacy, of protection of personal data and of freedom of expression and information which are set out by the Charter of Fundamental Rights of the European Union[89].

[85] Nihoul P. & Rodford P., 2011, EU Electronic Communications Law Competition and Regulation in the European Telecommunications Market, Second Edition, Oxford University Press, p.412
[86] Farr S. & Oakley V., 2006, EU Communications Law, Second Edition, Sweet & Maxwell, p.337
[87] Supra n.13 , Art.15
[88] Supra n.85, p.416
[89] Goemans C. & Dumortier J., 2003, 'Enforcement Issues–Mandatory Retention Of Traffic Data In The Eu: Possible Impact On Privacy And On-Line Anonymity', Digital Anonymity and the Law, Series IT & Law, p.9 http://www.law.kuleuven.be/icri/publications/440Retention_of_traffic_data_Dumortier_Goemans.pdf

3.2.1.3 Traffic Data

Traffic data is inherent data type which is generated automatically during the communication[90]. For instance when subscriber originates a call, sends email or does something on Internet, he leaves some data behind him which are collected by ISPs, IAPs or by other relevant service providers for billing or other operational processes[91]. All these data which arise from the nature of communication can be considered as traffic data. Traffic data is described under the Article 2(b) EPD as; "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*"[92].

Processing of traffic data is set out under Article 6 EPD. Traffic data can be collected, processed or stored only if it is necessary for the transmission of communication and even this condition is met, traffic data must not be kept no longer than for the required purpose, so it must be immediately erased or anonymised[93]. Nevertheless, traffic data may only be processed under certain circumstances which are listed under Article 6 EPD[94].

Service providers are allowed to process traffic data for billing purposes and interconnection payments[95]. However, this allowance is limited for only certain time period which should be sufficient for preparing invoice. The decision of determining this time period is left to the Member States[96]. But, there is an exception to the limitation of retention of traffic data for purposes of law enforcement[97] which are described under Article 13(1) of DPD[98]. This rule has caused debate within the European Parliament and in order to strike a balance between national security and privacy; strict conditions are set out which data may be retained only for a limited period and where necessary, appropriate and proportionate in a democratic society[99].

---

[90] Supra n.3, p.516
[91] Ibid
[92] Supra n.13, Art.2(b)
[93] Supra n.26, p.527
[94] Supra n.86, p.337
[95] Supra n.13, Art.6(2)
[96] Supra n.41, p.121
[97] Supra n.13, Art.15(1)
[98] Supra n.6, Art.13(1)
[99] Article 29 – Working Party, 2002, 'Opinion 5/2002 On The Statement Of The European Data Protection Commissioners At The International Conference In Cardiff (9-11 September 2002) On Mandatory Systematic Retention Of Telecommunication Traffic Data', p.3

Furthermore, the content of the data collected for the purpose of billing must be necessary for the operation[100]. For example, duration, called number, date and time can be considered reasonable for billing a phone call communication. The other data collected during the communication and will not be necessary for billing, must be erased or anonymised immediately after the communication terminates.

Moreover, traffic data may be processed for the purpose of marketing electronic communications services or for the provision of value added services[101]. But, in order to legitimate this process, user must give his consent and must be notified about the purpose and scope of processing and which data will be collected for specified purpose. Furthermore, all the principles of data subject's consent stated under DPD must be applicable[102]. As is known, some of the value added services are given by the third parties which are not also the provider of the electronic communication service. In such a condition, if third party provider will use traffic data, the main service provider must authorize it and accept the responsibility of any misuse that may cause a violation of privacy[103].

3.2.1.4 Location Data

Location data is a type of data which indicates the geographic position of the terminal equipment of a user of a publicly available electronic communications service[104]. Location data includes latitude, longitude and altitude of the user's terminal equipment, direction of travel, identification of the network cell with the date and time information[105]. Therefore it indicates the current location of the equipment for given time. If it is considered that terminal equipment is a mobile phone, this data set indicates where the subscriber was during certain time period; even his path might be tracked easily.

Collecting and processing location data has emerged according to the recent developments in technology and has become popular in recent years in line with the smart phones. Although it is not a new concept, the reason being more popular is the increase in usage of value added services. Location data is processed by value added services in many ways which while some

[100] Supra n.41, p.121
[101] Supra n.13, Art.6(3)
[102] Supra n.41, p.122
[103] Ibid, p.122
[104] Supra n.13, Art.2(c)
[105] Ibid, recital 14

are very useful for users, some are only for fun. For instance, location data is used to be able to get directions when driving, to be able to learn nearest locations such as hospital, pharmacy, and restaurant or for weather forecast[106]. Location data can be also used for commercial issues like marketing or advertising. Assuming, such a value added service obtains your location data, process this data with other services and finds that it is raining at your geographical location in the current time and as a result a message appears on your mobile device screen: "*Would you like a cup of our delicious coffee while it is raining outside. Coffee shop is only 50 metres far away from you. Touch for directions."* At first, it sounds good but user may face with few problems. First, user's location is tracked by third parties and user may have a feeling of following by someone. Second, it may be irritating if user has several advertisement messages during shopping. Therefore, location data may only be processed when they are made anonymous or with the data subject's given consent[107]. The consent is valid only if some conditions are met. First, user or subscribers must be informed about the extent of the data and purpose for processing[108]. Moreover, if this data is shared with or transferred to third parties, user or subscribers must also be notified about this information[109]. Second, user must be able to withdraw his consent, free of charge, whenever he wishes[110].

3.2.1.5 Relation Between Traffic Data, Location Data and Personal Data

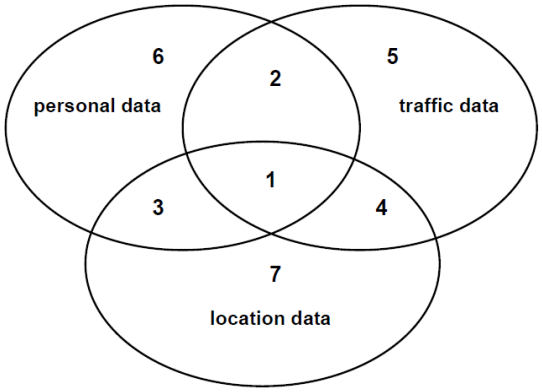
Location data may be considered as traffic data under some conditions[111]. If location of the terminal equipment is needed for the conveyance of communications and therefore for the purpose of billing, this data may also be considered as traffic data. For instance, in GSM network GSM-cell information is needed in order to begin and end the communication[112]. However, this information does not include the latitude, altitude, longitude or direction of travel which specifies the exact location of the terminal equipment[113]. If that data includes those additional information which helps to find the exact location of user, it is considered as 'location data other than traffic data'. Data controllers have to obtain data subject's prior

[106] Supra n.3, p.517
[107] Supra n.13, Art.9
[108] Supra n.26, p.528
[109] Ibid, p.528
[110] Supra n.86, p.338
[111] Supra n.26, p.528
[112] Ibid
[113] Supra n.41, p.122

consent in order to process such a location data[114]. As it seems, the relation between traffic data and location data is a quite complicated issue.

The relation between traffic data, location data and personal data is more complex than the relation between traffic data and location data. Because, if traffic data or location data is not also personal data; the provisions of DPD is not applicable. This relation is enlightened by WP in its opinions; "*since location data always relate to an identified or identifiable natural person, they are subject to the provisions on the protection of personal data laid down in Directive 95/46/EC*"[115]. However, in order to clarify this relation additional explanations are needed. To understand this relation, seven data groups can be formed as shown on the below illustration[116].

Figure 1: Relation Between Traffic Data, Location Data And Personal Data



1. Traffic data that also location data and personal data: The GSM cell-id of a mobile phone when subscriber sends a text message.
2. Traffic data that also only personal data: The date and time of a phone call made by individual.
3. Personal data and location data but not traffic data: Exact location of an individual with subscription.
4. Traffic data and location data but not personal data: The date and time of a phone call made from a certain public phone booth.

[114] Ibid
[115] Article 29 – Working Party, 2005, 'Opinion 5/2005 On the Use of Location Data With a View to Providing Value-Added Services', p.3
[116] Cuijpers C., Roosendal A., Koops B., 2007, 'D11.5 The Legal Framework for Location Based Services in Europe', Future of Identity in the Information Society Working Party Report, p.27 http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP11-del11.5-legal_framework_for_LBS.pdf

5. Only traffic data: The date and time data when a user used anonymizing service on Internet.
6. Only personal data: The account number of individual.
7. Only location data: The GSM cell-id of a mobile phone which user uses prepaid account and moreover is not subscribed to provider.

In the lights of the examples above, there are seven possibilities regarding the relation between traffic data, location data and personal data. It is obviously seen that, the opinion of WP does not cover the two of these possibilities[117]. It is an indicator of how complex is this relation and each case may need additional interpretation.

This complexity emerges another debate about which Directive even which provision is applicable. As mentioned before, EPD is lex specialis in legal theory; therefore it takes precedence of DPD[118]. For the issues that are not covered by EPD, but are in the scope of DPD, the provisions of DPD are applied. Moreover, the different provisions of EPD are applicable for traffic data and location data[119]. So provider of a location based service, should take into account of following questions in order to decide which provision is applicable[120].

- Is data personal data in the scope of Article 2(a) DPD?
- Is data traffic data in the scope of Article 2(b) EPD?
- Is data location data in the scope of Article 2(c) DPD?
- Does the data relate to users or subscribers of public communications networks or publicly available electronic communications services? (Articles 6 and 9 of EPD)
- Are the exceptions stated under Article 15 EPD applicable?

3.2.1.6 Itemised Billing

Another issue regulated under the EPD is itemised bills. Subscribers have a chance to check the accuracy of their bills, also they can see the details of the rates of each service they used

[117] Supra n.26, p.531
[118] Supra n.116, p.33
[119] Ibid, p.33
[120] Royer D., Deuker A, Rannenberg K., 2009, The Future of Identity in the Information Society: Challanges and Opportunities, Springer, p.220

and therefore they are able to change their tariffs or service provider[121]. The right to receive itemised bills is ruled under Universal Service Directive[122] as a result of enhancing competition in electronic communications sector[123]. Itemised bills include information which belongs to calling users and called subscribers such as the phone number, and the date and time of the call was made. That information is obviously personal data and thus, itemised bills jeopardise the privacy of subscribers and users[124]. Thus, on the contrary of Universal Service Directive, Article 7(1) EPD enables subscribers to receive non-itemised bills[125]. Moreover, service providers may offer their subscribers to mask or deleted the called numbers in their bills to reduce the risk of privacy violations[126].

Furthermore, Member States have a duty of take additional measures to enhance privacy for example to make calls or pay for calls are available to such users and subscribers, to facilitate anonymous calls in particular[127]. Pre-paid phone cards, pre-paid phones, cash payphones[128] or payment by credit cards[129] are the examples implemented by Member States in order to meet this requirement.

3.2.1.7 Calling and Connected Line Identification

EC, tried to accomplish three objectives while enacting provisions with regards to calling line and connected line identification (CLI)[130].

First, the calling party must have a possibility of preventing the presentation of his number[131]. Service provider must offer subscribers a method of preventing the presentation of his number to the called party on a per call basis or on a line basis[132]. In addition, these methods must be

[121] Supra n.85, p.428
[122] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive)
[123] Supra n.85, p.428
[124] Supra n.86, p.339
[125] Supra n.13, Art.7(1)
[126] Supra n.86, p.339
[127] Information Commissioner's Office, 2006, Guidance On The Privacy And Electronic Communications (EC Directive) Regulations 2003 Part 2: Security, Confidentiality, Traffic And Location Data, Itemised Billing, CLI And Directories v3.4, p.12
[128] Ibid
[129] Supra n.86, p.339
[130] Supra n.86, p.339
[131] Supra n.13, Art.8(1)
[132] Supra n.86, p.339

so simple that user is able to change his choice for every call[133]. Moreover, it must be free of charge.

Second, in order to strike balance between calling and called party, the called party must have a possibility to reject a call made from a hidden number[134]. Like the first rule, called party must be offered a method which is simple to use and free of charge.

Third, the called party must have a possibility to withhold the presentation of a number to which the calling party is actually connected. This case may occur, in particular, for forwarded calls.

However, in some cases, the elimination of the presentation of CLI services may not work and although the calling party prevents the presentation of CLI, the called party may have to see the number. The exceptions regarding elimination of CLI are set out under Article 10 EPD. These exceptions so called transparent procedures are applicable under two conditions. First, in case of subscriber is in trouble with the malicious or nuisance calls, depending upon his request, the CLI information may be stored by the provider and used later for the purpose of tracing the origin of calls. Second, in some cases, emergency services are in the need of obtaining the location of the call being made. Because, locating the equipment very quickly is crucial for the police and emergency services in order to provide quick response to incidents.

3.2.1.8 Public Directories

Public directories list the subscribers in a certain geographical area who uses the services of a provider that publishes directory. Its main purpose is to allow the others to obtain a contact detail of someone. Directories may in a form of either printed or electronic. While people can use it for to find the contact details of a relative or friend, they may be used for direct marketing agencies for commercial purposes[135]. Directories may contain some personal data including the full name, address or phone number of subscriber. Due to the directories include personal data and are published by the provider of a publicly available electronic communications service, the circumstances of publishing directory are ruled under the

[133] Supra n.85, p.428
[134] Supra n.13, Art.8(2)
[135] Supra n.26, p.539

provisions of EPD. According to the Article 12(1); "*Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory*"[136]. Moreover, subscribers must be given the choice of being included or not in a directory and able to choose to what extent their personal details will be included in the directory[137].

3.2.1.9 Unsolicited Communications

Unsolicited communications term often addresses the term spam. Even though when spam is mentioned emails come to mind, it is not related with only emails it is also related to other communication ways such as fax and phone calls. There is not an approved unique definition of spam; however most common definition is; unsolicited commercial communication which refers to a communication method made automatically without the person's request, for the purposes of direct marketing. Nevertheless, this description excludes other purposes of spammers such as political messages and some types of fraudulent messages[138]. The main feature of all descriptions and kinds of spam is; it is unsolicited, it wastes time and finally it costs money and it is a nuisance[139] in the electronic communications sector.

There are few provisions under separate Directives in EU level which deal with the spam issue. However, when data protection is considered the main provisions take place under DPD and EPD. Although DPD has no direct reference to spam or unsolicited messages, in some respects, it has an indirect relation with spam according to the directive describes personal data for marketing[140]. Considering the most used form of the unsolicited communication is email; the debate on the provisions of Directive is whether email address is a personal data or not. Because the person's name, political or ideological view or working place may be

[136] Supra n.13, Art. 12(1)
[137] The Office of Data Protection Commissioner, 'Guidance Note on Data Protection in the Electronic Communications Sector',
https://www.dataprotection.ie/documents/guidance/Electronic_Communications_Guidance.pdf
[138] Metchis H., Singleton S., 2003, 'Spam, That Ill O' The ISP: A Reality Check for Legislators, Competitive Enterprise Institute', p.3
[139] Hinde S., 2003, Spam: The Evolution of a Nuisance, Computers & Security Volume 22, Issue 6, p. 474–478
[140] Fleischer P., Cooper D., EU Data Privacy in Practice - Microsoft's Approach To Compliance, Computer Law & Security Report 22, p.64

guessed from the prefix or domain name[141]. On the other hand, there was a debate on whether spammers are data controllers under the provisions of DPD. The key point on this debate is how spammers obtain e-mail addresses and whether harvesting e-mail addresses is illegal[142]. However, EU qualifies email address as a personal data and it is illegal to harvest or sell email addresses, because this activity is an unfair processing of personal data and also it is against the Article 6.2 DPD due to purpose of person's publishing his email address is not the same with the spammers'[143].

The main provisions that indicate spamming take place under Article 13.1 EPD which was written obviously in order to implement opt-in regime stating that; "*The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent*"[144]. However, according to the next paragraph Member States may adopt opt-out regime if customers' data is obtained in the "*context of the sale of a product or a service*"[145].

Owing to the fact that opt-in and opt-out regimes are not defined explicitly in the EPD, Member States have implemented the rules in different approaches especially opt-in regime has been implemented in different ways[146]. Some states had already implemented opt-in regime before EPD, some states interpreted the "*subscribers or users*" expression as individuals and set free sending spam to business. As a result, most of the Member States adopted spam legislation without in harmony[147].

[141] Supra n.46, p. 364
[142] Supra n.3, p.500
[143] Article 29 - Data Protection Working Party, 2000, Working Document Privacy on the Internet- An integrated EU Approach to On-line Data Protection, p.77
[144] Kozyris P. J., 2007, Regulating Internet Abuses: Invasion of Privacy, Kluwer Law International, p.23
[145] Supra n.46, p.371
[146] Asscher, L.F, Hoogcarspel S. A.,2006, Regulating Spam, A European Perspective after the Adoption of the E-Privacy Directive, T.M.C. Asser Press p.23
[147] Moustakas E., Ranganathan C., Duquenoy P., 2005, Combating Spam Through Legislation: A Comparative Analysis of US and European Approaches, Conference on Email and Anti-Spam, http://pdf.aminer.org/000/085/114/combating_spam_through_legislation_a_comparative_analysis_of_us_and.pdf

3.2.1.10 Cookies

One of the issues that regulated under Article 5(3) EPD is cookies which are tools used for storing or retrieving information. Cookies are small text files which located on the user's terminal locally but available to use by third services and contain some information about the user[148]. Cookies may be used for several purposes, however, the main purpose is to make possible that a website on Internet can remember the individual who visited current website before[149]. Cookies can remember the information used when user logging to a website or shopping online, and user does not need the type same information for his next visit to the same website. In this respect, cookies are useful tools. But, user gives his personal data including full name, address, contact details, credit card number, even in some conditions his sensitive data, to website and this data is stored in text files to be used later. Moreover, some websites store information in cookies including the habits and interests of the user, for instance, even user does not complete the purchase process and only look for products on an e-commerce website, later he can see advertisements related to his behaviours in another website, so called behavioural advertising, about the product which looked before[150]. Therefore, although cookies are useful tools, they may be used in a way which threatens privacy. Hence, in order to annihilate this threat, EC adopted some provisions under EU legislation regarding cookies, but the matter was resolved mainly within EPD[151].

Article 5(3) EPD determines the rules of how the use of cookies can be legitimate. *"Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing"*[152]. According to the ruling, cookies may be used for legitimate purposes if the consumer was supplied with clear and comprehensive information about the purpose of processing[153]. The ways of obtaining consent of user for the purpose of behavioural advertising are explained by WP and according to the opinion of WP; consent

[148] Supra n.3, p.512
[149] Debussere F., 2005, 'The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?', International Journal of Law and Information Technology, Vol.13 No.1, p.76
[150] Supra n.5, p.161
[151] Supra n.3, p.513
[152] Supra n.13, Art.5(3)
[153] Supra n.3, p.513

may be obtained via web browser ensuring to convey clear, comprehensive and fully visible information about the processing and advertisement network providers should be in collaboration with browser manufacturers and develop opt-in mechanisms rather than using opt-out mechanisms[154]. Moreover, user must have a possibility to refuse the use of cookies.

In addition to the rulings of the EPD, WP clarifies some issues in its opinions regarding the use of cookies, in particular by the search engines. While searching for any kind of content on Internet by search engines, users remain some valuable information related to their search which may indicate their interests, health conditions or private life[155]. This information is stored in cookies and includes primarily the text of query, IP address of user, date of search with time, information about the web browser of user and unique ID of the user[156] and this information are used for several purposes. This makes this issue controversial, because search engines refuse to be a data controller in the scope of DPD claiming IP addresses are not personal data[157]. WP clarifies this in its WP 136; *"unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side*", stating that these considerations will apply equally to search engine operators[158]. Therefore, search engines are considered data controller in addition to have obligations regarding the processing of cookies.

4. DATA PROTECTION LEGISLATION IN TURKEY

In Turkey, legislation system has been formed hierarchically. Turkish Constitution is situated at the top of legislation and has a framework characteristic for the legislation. Therefore, the Constitution is the most powerful law in Turkey and any legislation should not be incompatible with Turkish Constitution[159].

In Turkey, there is not a specific law regarding the protection of personal data. The Constitution and a few general and sectoral laws such as Civil Code, Criminal Code, Labor

[154] Article 29 Data Protection Working Party, 2010, 'Opinion 2/2010 On Online Behavioural Advertising', p.23
[155] Bodogh Z., 2011, 'Privacy Issues Of The Internet Search Engines - In The Light Of EU Data Protection Legislation', Masaryk University Journal of Law and Technology, Vol.5:2, p.164
[156] Ibid, p.165
[157] Supra n.44
[158] Supra n.45, p.8
[159] Davutoglu U., 2012, 'Privacy and the Role of Regulations Regarding Data Protection in Telecommunications Sector: A case Study on Turkey', University of Westminster Dissertation Thesis, p.42

Law, Banking Law, Bank Cards and Credit Cards Law and Electronic Communications Law contain some provisions which deal with the protection of processing personal data[160]. Moreover, there has been a draft Data Privacy Law for several years waiting to be enacted by Turkish Parliament. In the following part of the study, Turkish legislation regarding data protection and privacy, in particular, in electronic communications sector will be examined.

4.1 General Regulations Regarding Data Protection and Privacy

Section 5 of the Turkish Constitution regulates the confidentiality and protection of private life. Article 20 emphasizes the right to privacy of individuals stating "*everyone has the right to demand respect for his or her private and family life, and the privacy of an individual's or family's life cannot be violated save in accordance with law*[161]". In 2010, Turkish Government submitted a package of amendment of Constitution and at the end of a nationwide referendum that amendment package accepted[162]. Within this package, Article 20 has expanded and new provision added without amending the provision that states right to privacy: *"everyone has the right to request the protection of his personal data. This right includes being informed of, having access to and requesting the correction and deletion of his personal data, and being informed whether this data is used in a way that is consistent with the purposes for which it is collected. Personal data can be processed only in accordance with law or with the concerned individual's consent. Procedures and principles regarding the protection of personal data are regulated by a law.*[163]*"* According to this provision the rights of individuals expanded to the right to request the protection of personal data regarding enabling the prohibition of processing personal data without the data subject's consent[164]. Moreover, the last sentence refers to a specific law to regulate protection of personal data. Restriction and limitation of those rights are possible in exceptional circumstances by governmental authorities, police, courts and by some other legal entities. However, restrictions are not legitimate unless there is a court's decision or a state of emergency or restriction conditions must be defined explicitly in a regulation. In addition to the right of privacy and right to request the protection of personal data, Article 22 states that everyone has a right to request secrecy of

[160] Data Protection Overview (Turkey), http://www.gurlaw.com/data-protection-overview-turkey/ Last accessed on 01.08.2013
[161] Turkish Constitution, Art.20
[162] Tene O. & Saygin Y., 2011, 'Privacy and Data Protection in Turkey: (Inching) Towards a European Framework', Privacy & Security Law Report 10, p.1 http://ssrn.com/abstract=1941005
[163] Supra n.161, Art.20
[164] Supra n.162, p.1

communication[165]. Beyond, secrecy of communication cannot be impeded or violated save in accordance with law[166].

In Law level, Turkish Criminal Code (TCC) numbered 5237 lays down provisions regarding the processing and protection of personal data under the ninth section which determines the offenses against privacy and secrecy of life. In particular, Article 135, 136 and 138 of TCC deal with the protection of privacy and personal data. In the context of those articles, to those who record or obtain of sensitive data such as political or religious views, or racial or ethnic origin unlawfully, record and transmit personal data illegally or do not delete the data which are no longer needed are imposed imprisonment[167].

In addition to considering processing of personal data unlawfully is a crime under the provisions of TCC, that unlawful process also infringes the person's rights[168]. Violations to the rights of an individual are regulated under Article 24 and 25 of Turkish Civil Code. According to that Article; a person may claim a protection from the judge against the violations and may demand from the judge to take an action for prevention of such infringement or elimination of such threat[169]. Moreover, the person may file a lawsuit and demand compensation for pecuniary and non-pecuniary damages.

The Law on the Right to Access to Information enables that individuals may obtain certain information except confidential information including the information belongs to a person within the scope of personal data[170]. That law indicates that disclosure of personal data is protected.

Electronic Signature Law obliges electronic certificate service providers (ECSP) in order to provide protection of information. ECSP cannot collect data from data subject more than necessary for generating an electronic certificate; also this data must be collected with the

[165] Supra n.161, Art.22
[166] Data protection in Turkey: Overview, http://uk.practicallaw.com/7-520-1896#a120099 Last accessed on 04.09.2013
[167] Turkish Criminal Code (No:5237), 2004, Official Gazette No. 25611 dated 12/10/2004, Art. 135,136,138
[168] Sahin O., 2011, 'Elektronik Haberlesme Sektorunde Kisisel Verilerin Islenmesi, Saklanmasi ve Gizliliginin Korunmasi (Processing, Retention and Protection Personal Data in Electronic Communications Sector), ICT Expertise Thesis ICTA Turkey, p.122
[169] Turkish Civil Code (No:4721), 2001, Official Gazette No:24607 dated 8/12/2001, Art. 24,25
[170] The Law on the Right to Access to Information (No:4982), 2003, Official Gazette No:25269 dated 24/10/2003

consent of data subject[171]. Moreover, the collected data must not be transferred to third parties without the written consent of the data subject[172].

4.2 Draft Law Regarding Protection of Personal Data

Turkey has signed the ECHR and the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* in 1981 and one of the candidate countries for full membership to EU. However, despite all those facts there is not yet a specific enacted law regarding the protection of personal data. In 2003 when the efforts of the Government had gathered speed in order to harmonize domestic laws with EU acquis, Ministry of Justice prepared a Draft Law on the Protection of Personal Data (Draft Law)[173]. Finally, Draft Law was sent to Prime Ministry to be enacted[174]. Draft Law includes general provisions regarding the processing of personal data and is a framework law like DPD. Sector specific procedures and principles are not in the context of that Draft Law, those regulations are left to the other related governmental bodies, authorities or professional organizations[175].

Draft Law considers the OECD guideline governing the protection of privacy and transborder flows of personal data and Convention for determining the principles of data protection[176]. The Draft Law consists of five sections which most of its rules were prepared in the lights of DPD[177].

In the first section the scope and aim of the law is stated and some essential definitions are made. Draft Law incorporate both natural and legal persons in the context of whose data are processed and who processed those data[178]. Personal data may be processed either

[171] Electronic Signature Law (No:5070), 2004, Official Gazette No:25355 dated 23/1/2004, Art.12(a)
[172] Ibid, Art.12(c)
[173] Supra n.162, p.2
[174] Ministry of Justice webpage, http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Basbakanlik.html Last accessed on 06.09.2013
[175] Civelek D., 2011, Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Protection Of Personal Data and a Suggestion For The Institutional Building), The State Planning Organization Thesis for Planning Expertise, p.149
[176] Prime Ministry of Republic of Turkey, 2008, General Preamble fort he Draft Law on Protection of Personal Data www2.tbmm.gov.tr/d23/1/1-0576.pdf Last Accessed on 05.09.2013
[177] Supra n.162, p.2
[178] Supra n.176

automatically or by traditional filing methods. Both processing methods are in the context of the Draft Law[179].

In the second section of Draft Law, data controllers are obliged to inform data subjects including the information of; the purpose and method of collection and processing, method of collection, whether the collected data will be transferred to third parties etc. In addition, data controllers are obliged to take appropriate measures in order to prevent unlawful processing, to provide access by authorized person for legitimate purposes. Besides, appropriate security measures should be implemented for the protection of personal data. Data subject has a right to obtain data relating to him, to request rectification of his data or to request deletion or prevention to transfer his data in case of unlawful processing[180]. Also the principles of the transferring personal data to other countries are laid down under this section. Those principles show parallelism with the principles laid down under DPD.

In the third section, data controller is obliged to notify the Protection of Personal Data Board before launching its operations regarding processing personal data. The notification must be included those information: the name and address of the data controller and the representative (if exists), the purpose of data processing, a description of the data subject and data categories relating to those whose data will be processed, the third parties whom the personal data may be disclosed, the data categories which are proposed to transfer to third countries and general description of the security measures which will be implemented for the reasons mentioned above.

Draft Law set forth an establishment of a Protection of Personal Data Board which is an independent supervisory authority. This authority has some obligations similar to the ones that set out by DPD.

4.3 Legislation on Data Protection in Electronic Communications Sector

Turkish electronic communications sector has made a remarkable progress for the last decade like the other technologically developed countries. In some respects, this progress may be

[179] Ibid
[180] Draft Law on Processing of Personal Data, Articles 11-15
http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Kanuntas/kisiselveriler.pdf

regarded as a transformation[181]. This progress may be linked to the establishment of an independent authority. In 2000, Information and Communications Technology Authority (ICTA)[182] which is an independent regulatory authority was established and was held liable to adopt secondary regulations regarding electronic communications sector and to carry out inspections on electronic communications service providers. Later the establishment of ICTA, several secondary regulations have adopted by ICTA, mostly in line with the EU telecommunication acquis[183]. The Turkish telecommunications sector has been liberalized by putting an end to the monopoly and privatization of Turk Telekom A.S. which is the incumbent fixed line operator in Turkey[184]. In the following part of this study Electronic Communications Law (ECL) and the regulations that adopted by ICTA regarding data protection will be evaluated.

4.3.1 Electronic Communications Law

In Turkey, the main law that regulates the electronic communications sector is ECL. ECL was prepared to create effective competition, to ensure the protection of consumer rights, to promote the deployment of services throughout the country and to ensure efficient and effective use of the resources in electronic communications sector and to determine relevant principles and procedures thereto[185]. In this context, ICTA which is an independent regulatory authority is responsible to adopt secondary regulations regarding electronic communications sector and to carry out inspections on electronic communications service providers. Within the ECL, the duties and the obligations of ICTA are listed.

According to the Article 6(c) ECL one of the ICTA's duties is "to make necessary regulations and supervisions pertaining to the rights of subscribers, users, consumers and end users as well as processing of personal data and protection of privacy"[186]. At first sight, this provision may be interpreted as ICTA is the responsible supervisory authority to regulate the protection

[181] Kilic D., 2009, 'Regulations On Telecommunication Sector In Turkey During EU Integration Process', University of Bahcesehir Master of Degree Thesis, p.102
[182] The Authority was established with the name of Telecommunications Authority but by the law 5809 its name has been changed in 2008.
[183] Burnham J., 2007, 'Telecommunications Policy in Turkey: Dismantling Barriers to Growth', Elsevier Telecommunications Policy 31, p.197-208
[184] Eke E., 2010, Liberalization of Turkish Telecommunications Industry, Suleyman Demirel University The Journal of Visionary, Vol.2 No.1, p.102
[185] Electronic Communications Law (No:5809), 2008, Official Gazette No:27050 dated 10/11/2008, Art.1
[186] Ibid, Art.6

of personal data. However, ICTA is only responsible for the regulations in electronic communications sector due to scope of this law is restricted with electronic communications sector. Moreover, ICTA may impose obligations to electronic service or/and access providers in order to protect personal data and privacy, considering the factors such as requirements of the sector, international regulations, and technological developments[187]. Hence, all operators which are legal entities that provide electronic communications services and/or provide electronic communications network and to operate the infrastructure providing that to be authorized by ICTA, are obliged to obey to regulations that may be adopted by ICTA regarding data protection and privacy. Although, these provisions impose an obvious authority to ICTA in order to be able to adopt regulations regarding data protection and privacy, Article 51 clarifies it in a more explicit manner: ICTA is entitled to determine the procedures and principles regarding the processing of personal data and the protection of privacy in electronic communications sector[188].

Article 50 ECL regulates the circumstances of unsolicited communication. If any unsolicited communication has been conveyed for the purposes such as direct marketing, political propaganda or transmission of sexual content messages by electronic communications means such as automated dialling machines, fax machines, e-mails and short messages without the prior consent of the subscriber; the subscriber must be provided method by simple means and free of charge to reject receiving such messages henceforth and ICTA shall adopt regulations which must set principles and procedures on that subject[189].

4.3.2 By-Law on Consumer Rights in the Electronic Communications Sector

That secondary regulation has been adopted by ICTA in 2010 with an aim of to protect the rights and interests of consumers who use electronic communications services and amended in 2013. In this study, the amended version will be analyzed.

[187] Ibid, Art.12(2-d)
[188] Ibid, Art.51
[189] Ibid, Art.50

Within that regulation, personal data is described similar to the EU's description: all information relating to an identified or identifiable natural person or legal entities[190]. However, personal data has a wider scope in Turkey, because legal entities are included as well as natural persons.

Article 5 of the By-Law regulates the basic and primary rights of the consumers. Those rights are including but not limited with those; to request whether included in public directories[191] and to request to obtain itemised bills[192]. Subscribers should have a right to be included or not in the public directories and should have a right to use those directories without discrimination and either free of charge or by paying amount. Article 15 determines the method of being included in the directories. Opt-in regime is adapted and subscribers consent is sought to be included in those directories. Moreover, subscribers' approval must be obtained during the signing of subscription contract[193]. Unfortunately, in which detail personal data will be included in directories is not mentioned in the scope of this regulation and subscribers have not an option to choose which their personal data will be published. Under Article 20, operators are obliged to provide itemized billing either free of charge or by paying fee on the demand of the subscriber.

Article 15 sets out the right to refuse unsolicited communications. Subscribers have a right to refuse messages, in case of operator itself or third party service provider make communication for the purpose of direct marketing, political propaganda or sexual content by using electronic communication tools such as automated dialling machines, fax machines, e-mail and SMS. It is obvious that opt-out regime has been implemented even for e-mail communications.

4.3.3 By-Law on Processing of Personal Data and Protection of Privacy in Electronic Communications Sector

The main regulation in Turkish legislation regarding the protection of personal data in electronic communications sector is the "By-Law on Processing of Personal Data and Protection of Privacy in Electronic Communications Sector" (By-Law on Privacy) which was

[190] By-Law on Consumer Rights in the Electronic Communications Sector, 2010, Official Gazette No:27655 dated 28/07/2010, Art.4(f)
http://btk.gov.tr/mevzuat/yonetmelikler/dosyalar/tuketici-haklari.pdf Last Accessed on 07.09.2013
[191] Ibid, Art. 5(1-c)
[192] Ibid, Art. 5(1-e)
[193] Ibid, Art. 15(4)

adopted in 2012 and amended in 2013. As will be seen below, the regulation was prepared in the lights of EU legislation and similar expressions have been used, however not all the aspects of EPD and DPD have been covered. Besides, although some issues regulated, some of the adapted rules differ from the rules of EPD.

Firstly, the regulation covers all operators which are performing activity by giving services or providing electronic communications network[194]. They all have to obey to the principles of procedures ruled by this regulation. The personal data definition is identical to the definition in the By-Law on Consumer Rights[195], therefore both natural persons' and legal entities' data are considered personal data. In addition, the definition of the personal data breach is made as: a breach of security leading to the accidental, unauthorized or unlawful destruction, loss, transmission, alteration, storage, process, disclosure of, or access to personal data[196]. Moreover, consent definition has been made similarly with almost same meaning with the one in DPD. Consent means freely given and provable declaration of the data subject's approval of processing his/her personal data before processing of his/her personal data and within the scope and purpose of the processing of the data[197].

By-Law on Privacy sets out five main principles regarding the processing of personal data. Personal data shall be; processed fairly and lawfully, processed upon consent of the data subject, adequate, relevant and not excessive in relation to the purposes for which they are collected, accurate and kept up to date, 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[198]. As is seen, those principles are based on the principles laid down under EPD. However, EPD uses more explanatory approach than the Turkish regulation. For instance, in the scope of EPD, further processing of personal data for historical, statistical or scientific purposes may be considered compatible with the purpose of collection providing that additional measures are taken. By-Law on Privacy does not clarify this issue and it is understood that personal data shall not be processed for further purposes. Although third principle may be considered to cover that uncertainty, it might be better using more explicit expression. In addition to those principles; the data subject's consent is valid if

[194] By-Law on Processing of Personal Data and Protection of Privacy in Electronic Communications Sector, 2012, Official Gazette No:28363 dated 24/07/2011, Art.1(1)
[195] Ibid, Art.3(1-h)
[196] Ibid, Art.3(1-ı)
[197] Ibid, Art.3(1-ö)
[198] Ibid, Art.4(1)

the data is processed for the same purpose(s) by the third party provider which is authorized by the operator and the operator is also responsible for the breaches that may arise from the third parties[199]. That provision which was added in 2013 with the last amendment provides to make self-test of operators, because they should choose confidential third parties in order to avoid holding liable for violations of third parties. Moreover, regulation rigorously prohibits the transferring of personal data to third countries and there is no circumstance to transfer those data[200].

Operators must implement security policy with respect to processing of personal data. Operators must take appropriate and adequate technical and organizational measures, considering the technological opportunities, in order to provide security of the given services. ICTA is entitled to require operators to provide any information and documents related to the systems in which personal data are kept and to obtain information about security measures taken by operators, and to request for change in the mentioned security measures[201]. Those security related provisions are based on the provisions of EPD and are in line with EPD. Moreover, like EPD, operators are obliged to inform first ICTA, and if it is necessary the subscribers of the current service, in case of any risk of a breach to the secure processing of personal data[202]. This provision is the other measure in order to provide self-test, because operators will make an effort to implement security measures at maximum. Any operator does not desire to lose its reputation.

Under By-Law on Privacy, ensuring the confidentiality of communications and the related traffic data is essential right and it is prohibited to listening, tapping, storage or other kinds of interception or surveillance of communications unless there exists a consent of the parties of communication or a court decision or provisions that ruled by other relevant regulations[203]. The exemptions to that provision are not detailed under the By-Law on Privacy, but the circumstances of the lawful interception are regulated under the Law 5397[204] and other relevant secondary regulations that adopted by The Prime Ministry and Ministry of Justice[205].

[199] Ibid, Art.4(3,4)
[200] Ibid, Art.4(2)
[201] Ibid, Art.5
[202] Ibid, Art.6
[203] Ibid, Art.7
[204] Law Concerning the Amendment of Certain Laws (No:5397), Official Gazette No:25884 dated 23/07/2005
[205] The Presidency of Communication Webpage, Legislation, http://tib.gov.tr/tr/tr-menu-12-ilgili_denetim_mevzuati.html Last accessed on 08.09.2013

Traffic data has the same meaning and is defined identically under both EU and Turkish legislation. Besides, By-Law on Privacy determines the conditions of processing traffic data similarly to the EPD. Traffic data can only be processed for the purposes of traffic management, interconnection, billing, fraud detection, customer enquiries or settling disputes, in particular regarding interconnection and billing disputes[206]. The only condition to process traffic data for other purposes such as value added services or marketing is to obtain the consent of the data subject. Nevertheless, data subject can be able to withdraw his consent whenever he wishes by simple method and free of charge. Those traffic data must be anonymised or erased when it is no longer. The provisions regarding the processing traffic data are substantially similar to the ones in EPD; however, EPD obliges service providers to inform subscribers about the types of traffic data which are processed and the duration of such processing[207]. Under By-Law on Privacy, operators have such an obligation only in case of traffic data is processed for value added services and marketing purposes.

The location data required for the value added services and which are not traffic data can only be processed if data subject's consent is obtained or data is anonymised[208]. The provisions concerning the location data other than traffic data regulated in line with EPD.

By-Law on Privacy also regulates the conditions of identification of the called and calling line numbers[209]. Like EPD, calling user must be provided a simple use and free of charge method, to prevent his number to be identified to the called party. On the other hand, called party must be offered a possibility to reject the communication which is made by unidentified number. The main difference between the provisions of EPD and By-Law on Privacy; while EPD enables that this feature must be provided either per call or per line basis, under By-Law on Privacy "using a simple means" expression is found sufficient under By-Law on Privacy. However, it may cause disputes in practice.

[206] The provisions related to the processing traffic data laid down under Article 3,8,9 and 10 of By-Law on Privacy
[207] Supra n.13, Art.6(4)
[208] Supra n.194, Art.13
[209] Ibid, Art.17

Service providers may offer their subscribers to mask the called numbers in their bills upon demand of subscribers[210]. This provision reduces the risk of disclosure of the called parties' personal data. However, EPD has a wider protection regarding the issue of itemised bills.

In the last section of the regulation; administrative fines and other sanctions are determined in case operators fail to fulfil the liabilities set out by the regulation. In this context, there have been few violations which some sanctions were imposed to operators. In 2011, Vodafone A.S., which is a mobile operator, punished due to the security gap in one of its services, which caused the subscribers' itemised bills were viewed by unauthorized persons[211]. In this case, current operator was imposed a money fine of 0.05% of its net sales of 2010, due to default in its obligations. In 2011, another mobile operator, Turkcell was imposed a money fine of 0.015 % of its net sales in 2010 due to the personal data was accessible by the unauthorized personnel of Turkcell, and that personnel disclosed some of the subscribers personal data to third parties[212]. In 2011, internet service provider TTNET A.S. was imposed sanction of 0.02% of its net sales of 2010, due to not taking adequate security measures in order to protect personal data in the processes which performed both by its retailers and by authorized third parties[213]. In this case, operator held liable for the infringements that arose from the third party. In 2013, TTNET A.S. again faced with a sanction of 0.05% of its net sales of 2011[214]. It was found that it breached the provision regarding the confidentiality of communications, because some of the subscribers are included in a service which allows listening, tapping, storage or surveillance of a communication, without obtaining the subscribers' consent.

5. CONCLUSION

Personal data, in particular sensitive data provides very important information of individuals which can identifies them and indicates their behaviours or interests or opinions, in brief their lifestyle. So, personal data is an intangible valuable asset which may be used in many ways.

---

[210] Ibid, Art.20
[211] ICTA Board Decision 2011/DK-10/83, 2011, http://btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-10-83sss.pdf Last accessed on 08.09.2013
[212] ICTA Board Decision 2011/DK-10/198, 2011, http://btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-10-198.pdf Last accessed on 08.09.2013
[213] ICTA Board Decision 2011/DK-14/659, 2011, http://btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-14-659.pdf Last accessed on 08.09.2013
[214] ICTA Board Decision 2013/DK-SDD/228, 2013, http://btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2013%20DK-SDD-228.pdf Last accessed on 08.09.2013

Although, sole personal data is not a tangible value, it may be converted into actual money after it is processed for some purposes like marketing. Thus, while business organizations are willing to obtain and process personal data, individuals are in need to protect their rights regarding personal data. However, it is not easy to protect their personal data without legal regime.

Many academicians agree that data protection is a kind of privacy. Thus, before the examining the legal regime regarding data protection, privacy notion and the level of privacy protection should be analyzed. Although there is not a common definition of privacy, privacy is considered as a basic human right under almost all legal regimes and the right to privacy is protected in the highest level. For instance, in Europe the right to privacy is protected under ECHR and in Turkey, in addition to being Turkey is one of the signatory country of ECHR; it is assured by Constitution. Therefore, privacy of an individual is a human right in both Europe and Turkey. Also, both EU and Turkey in accordance with the view of *data protection is a form of privacy*, the right to protection of personal data is assured in high level by TFEU and Turkish Constitution. In those respects, both the right to privacy and the right to protection of personal data have the same level protection in Turkey. However, protection of personal data is guaranteed by Turkish Constitution since 2010. And this is interpreted as; Turkey is making effort in order to attend the European Union and this amendment reflected to the 2010 progress report. EU evaluated that Turkey made progress regarding the protection of personal data[215].

Indeed, the emergence of data protection laws is the result of the technological developments; in particular, the developments in the transistor technology caused that computers have become smaller and computers are started to be used in several areas. Hence, collecting, storing and processing personal data got easier than before and threat to personal data, therefore concerns on privacy increased. In order to eliminate that concern and to assure the right to privacy by protecting personal data, at first CoE introduced the Convention and upon to the fail in adapting the Convention by Members, EC enacted the most comprehensive data protection regulation: DPD. DPD is a mandatory regulation that all Member States have to adopt their own data protection laws in the light of the provisions of that Directive. Thus,

[215] EC, 2010, Commission Staff Working Document Turkey 2010 Progress Report, p.10 http://ec.europa.eu/enlargement/pdf/key_documents/2010/package/tr_rapport_2010_en.pdf Last accessed on 09.09.2013

within EU there has been a harmonized and well established data protection regime for almost 20 years. That harmonization provides an equivalent level of protection of the right to privacy with respect to personal data and as a result of that assurance; personal data may be transferred among the Member States. However, EU adapted a flexible regime concerning the transferring personal data to the third countries and if a country, outside the Union, provides an adequate level of protection in their law, personal data may be transferred to that country[216]. Up to now, 43 CoE Members which Turkey is one of them, have ratified the Convention. Besides, Turkey is a candidate country for the full EU membership and one of the prerequisite for the full membership is to harmonize national laws with the EU legislation. However, Turkey is one of the three countries which still has not have enacted data protection law within CoE[217]. That has been criticized by EC in the progress reports[218]. Therefore, Turkey is not considered as a safe harbour regarding personal data to be transferred. This situation is at a disadvantage with respect to the Turkish business sector who wishes to process personal data from Europe, meets with legal obstacles.

In order to remove legal obstacles on transferring personal data and to provide harmonization with EU acquis, but most importantly, to provide a high level protection for personal data and privacy for the individuals living in Turkey, Draft Law on processing personal data has been introduced by the Ministry of Justice to be enacted. Unfortunately, almost a decade has passed since that introduction and the Draft Law is still pending to be enacted in the Parliament. Considering the technology is a rapidly developing area, that period is too long for the law to be enacted. Because, in some respects, when Draft Law is enacted and take force, new business models might be created, even the EU Legislation might be amended and Turkey might have adopted an outdated law[219]. Although, the right to privacy and the right to request the protection of personal data are guaranteed by Constitution, lack of a general framework law remains this area not to be regulated. Because, the obligations of the parties who process personal data, the rights of the data subjects, the principles and procedures for collecting storing, processing and transferring personal data are indefinite and there is not an authorized governmental body to deal with these issues. In other words, in theory both privacy and

[216] Supra n.6, Art.25
[217] Greenleaf G., 2012, 'The Influence of European Data Privacy Standards Outside Europe: Implications For Globalisation Of Convention', University of Edinburgh School of Law Research Paper Series No 2012/12, p.19
[218] EC, 2012, Commission Staff Working Document Turkey 2012 Progress Report, p.54 http://ec.europa.eu/enlargement/pdf/key_documents/2012/package/tr_rapport_2012_en.pdf Last accessed on 09.09.2013
[219] Supra n.162, p.3

personal data are protected rights but in practice there is a significant legal gap in this area. In order to fill this gap and to provide a protection in real terms that Draft Law must be passed into law as soon as possible. Although public awareness is not high in Turkey[220], the business sector supports that this area should not be remain unregulated[221].

The rapid improvements in the electronic communications sector, in particular the Internet, the variations of services in this sector and the value added services caused significant changes in electronic communications sector with respect to the laws as well as the habits. Most of those newly services collect and process personal data and threaten privacy. Moreover, due to the new innovations and fast change in the technological infrastructure and accordingly the habits of user, the DPD was found insufficient to deal with the privacy concerns in electronic communications sector. As a result, the EPD which is a sector specific regulation regarding privacy and data protection was enacted in 2002. EPD does not replace EPD, even complements DPD. Within EPD, the principles and the procedures related to sector specific issues are regulated. It was aimed to prepare a technology independent regulation by using flexible expressions and by avoiding addressing a certain technology.

In Turkey, main law regarding electronic communications sector is ECL which was enacted in 2008. According to the ECL, ICTA is obliged to adopt necessary secondary regulations in order to determine the principles and procedures on the issues related with that sector. In this direction, ICTA adopted the By-Law on Privacy in 2012 in order to deal with protection of personal data and privacy. That regulation was mostly prepared in the lights of EPD, however while some issues regulated differently, some remain unregulated.

The scope of the EPD and By-Law on Privacy include big difference. By-Law on Privacy includes both natural persons and legal entities in the scope of regulation. From this point, in addition to the individuals, legal persons' data is under protection. So, personal data has a wider scope in Turkey.

Both in EPD and By-Law on Privacy the electronic communications service providers have same obligations to ensure the security of their services and to provide the secrecy of

[220] Supra n.159, p.53
[221] Türkiye Bilisim Dernegi (Informatics Association of Turkey), 2008, Kişisel Verilerin Korunması (Working Group Report on Protection of Personal Data), www.tbd.org.tr/usr_img/cd/kamubib14/raporlarPDF/RP2-2008.pdf Last accessed on 28.08.2013

communications. Under EPD, while electronic communications service providers notify the authorized national supervisory agency, the operators in Turkey, notify ICTA which is also the governmental regulatory body of electronic communications sector due to lack of a specific authorized regulatory body for data protection.

The traffic data is considered as a personal data and processing of traffic data is linked to the some similar rules both under EPD and By-Law on Privacy. Electronic communications service providers are allowed to process traffic data for the billing purposes and interconnection payments and for the value added services if the data subject's consent is obtained. The rules of the processing of location data other than traffic data are similar as of traffic data.

Also the rules regarding the itemised billing and calling line identification are determined similarly and while privacy is pursued, also a fair balance is provided between the called and calling party.

The right to choose being included in public directories is determined both in EU and Turkish legislation. In Turkish legislation, that right is described under two regulation; By-Law on Privacy and By-Law on Consumer Rights. In Turkey, opt-in regime is adapted for being included in public directories. However, the subscribers have not an option to choose which personal data they wish to publish and there is not an unambiguous expression about who determine the scope of the data. Moreover, although both regulation consider it as a right and same legal regimes is adapted, this situation may cause confusion. In order to remove the distributed situation, it would be more appropriate to be included those provisions under only By-Law on Privacy.

One of the remarkable differences between EU and Turkish legislation is on the unsolicited communications. Under EU legislation, unsolicited communications is a well defined issue and considering the problem on spam emails opt-in regime has been implemented. On the other hand, in Turkey, unsolicited communications is mentioned under ECL. While the concept has expanded to political propaganda and sexual messages, on the contrary to the EU the opt-out regime has been implemented which means, each customer may receive at least one legal e-mail or other type of communications from each spammer. So, that regime is far away from combating against unsolicited communications, in particular spam emails. Also,

ICTA is obliged to adopt regulations regarding that issue. However, without the duplication of the same provision which is under By-Law on Consumer Rights, there is still not a specific regulation or detailed provisions under By-Law on Privacy. This caused an incompatibility with the EU legislation, moreover, due to the legal gap subscribers are faced with spam e-mails.

Cookies is the other issue that is not regulated under Turkish legislation. Moreover, there is no related provision that may be linked to the cookies. Considering the widely use of cookies on Internet, the protection of personal data depends on the awareness of the user and the initiative of the service provider. However, this constitutes a critical threat to privacy and it means that privacy is not under complete protection on Internet.

As a result, EU has reduced anxieties on privacy in electronic communications sector by adopting mandatory law, EPD. EPD has been tried to be prepared in a technology independent manner, therefore it provides convenience to keep pace with the developments in technology. The issues which raise concerns on privacy are mostly addressed directly under EPD. For the debates on new services or technologies such as social networks or RFID technologies, WP clarifies the issues with the papers which include opinions. In short, within EU there is a well established regulation which provides high level and harmonized protection for the personal data and privacy in electronic communications sector. On the other hand, in Turkey, there is a critical legal gap in data protection area. That legal gap has been trying to patch by sectoral regulations. Considering the electronic communications sector that gap is substantially filled by the secondary regulations which are adopted by ICTA. However, these regulations are in By-Law level and do not provide high level protection and therefore their effectiveness are very weak. Moreover, not all the issues related with privacy in electronic communications sector are covered by those regulations such as unsolicited communications and cookies. Additionally, some issues are ruled under separate regulations and this is the other factor that reduces the effect of the regulations. It may be regarded as an indicator of this issue is not persisted adequately. Turkey has to pass the Draft Law on data protection as soon as possible in order to have effective rules and to meet the requirements of the Constitution in real terms which guarantee the right to privacy.

BIBLIOGRAPHY

I. Books

Asscher, L.F, Hoogcarspel S. A.,2006, Regulating Spam, A European Perspective after the Adoption of the E-Privacy Directive, T.M.C. Asser Press

Bell R. & Neil R., 2004, EU Electronic Communications Law, Richmond Law & Tax Ltd.

Edwards L. & Waelde C., 2009, Law and the Internet, Hart Publishing, 3rd Edition

Farr S. & Oakley V., 2006, EU Communications Law, Second Edition, Sweet & Maxwell

Jorgensen R. F., 2006, Human Rights in the Global Information Society, MIT Press

Koenig, C., Bartosch A.,Braun J.D., Rames M., 2009, EC Competition and Telecommunications Law, Kluwer Law International, Second Edition

Kozyris P. J., 2007, Regulating Internet Abuses: Invasion of Privacy, Kluwer Law International

Kuner C., 2003, European Data Privacy Law and Online Business, Oxford University Press

Lloyd, I. J., 2011, Information Technology Law, Oxford University Press, 6th Edition

Nihoul P. & Rodford P., 2011, EU Electronic Communications Law Competition and Regulation in the European Telecommunications Market, Oxford University Press, Second Edition

Reed C. (Ed.), 2011, Computer Law, Oxford University Press, 7th Edition

Royer D., Deuker A, Rannenberg K., 2009, The Future of Identity in the Information Society: Challanges and Opportunities, Springer

Rowland D., Kohl U., Charlesworth A., 2012, Information Technology Law, Routledge 4th Edition

II. Articles

Banisar D. & Davies S., 1999, 'Global Trends in Privacy Protection: An International Survey Of Privacy, Data Protection, And Surveillance Laws And Developments', Journal Of Computer & Information Law, Vol. 18

Bergkamp L. & Dhont J., 2000, 'Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web', EDI Law Review 7

Bing J., 1984, 'The Council of Europe Convention and the OECD Guidelines on Data Protection', 5 Michigan Yearbook of International Legal Studies

Birnhack M. D., 2008, 'The EU Data Protection Directive: An Engine Of A Global Regime', Computer Law & Security Report 24

Blume P., 2012, 'The Inherent Contradictions in Data Protection Law', International Data Privacy Law, Vol. 2, No. 1

Bodogh Z., 2011, 'Privacy Issues Of The Internet Search Engines - In The Light Of EU Data Protection Legislation', Masaryk University Journal of Law and Technology, Vol.5:2

Borghi M., Ferretti F. & Karapapa S., 2013, 'Online Data Processing Consent Under Eu Law: A Theoretical Framework And Empirical Evidence From The UK', International Journal of Law and Information Technology, Vol. 21, No. 2

Burnham J., 2007, 'Telecommunications Policy in Turkey: Dismantling Barriers to Growth', Elsevier Telecommunications Policy 31

Busch A., 2010, 'The Regulation of Privacy', Jerusalem Papers in Regulation & Governance Working Paper No. 26

Civelek D., 2011, Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Protection Of Personal Data and a Suggestion For The Institutional Building), The State Planning Organization Thesis for Planning Expertise

Davutoglu U., 2012, 'Privacy and the Role of Regulations Regarding Data Protection in Telecommunications Sector: A case Study on Turkey', University of Westminster Dissertation Thesis

Debussere F., 2005, 'The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?', International Journal of Law and Information Technology, Vol.13 No.1

Dolin R.A., 2010, 'Search Query Privacy: The Problem of Anonymization', Hastings Science & Techonology Law Journal, Vol. 2, No. 2

Eke E., 2010, Liberalization of Turkish Telecommunications Industry, Suleyman Demirel University The Journal of Visionary, Vol.2 No.1

Fleischer P., Cooper D., 'EU Data Privacy in Practice - Microsoft's Approach To Compliance', Computer Law & Security Report 22
http://www.sciencedirect.com/science/article/pii/S0267364905001858
Last accessed on 20.08.2013

Greenleaf G., 2012, 'The Influence of European Data Privacy Standards Outside Europe: Implications For Globalisation Of Convention', University of Edinburgh School of Law Research Paper Series No 2012/12

Hinde S., 2003, 'Spam: The Evolution of a Nuisance', Computers & Security Volume 22, Issue 6

Kilic D., 2009, 'Regulations On Telecommunication Sector In Turkey During EU Integration Process', University of Bahcesehir Master of Degree Thesis

Kirsch M., 2011-2012, 'Do-Not-Track: Revising The EU's Data Protection Framework To Require Meaningful Consent For Behavioural Advertising', Richmond Journal of Law & Technology, Vol.18 Is.1

Lipton J. D., 2010, 'Digital Multi-Media and the Limits of Privacy Law', Case Western Reserve University Case Research Paper Series in Legal Studies Working Paper 2010-16

Magee J., 2002-2003, 'The Law Regulating Unsolicited Commercial E-Mail: An International Perspective', 19 Santa Clara Computer & High Tech. Law Journal

Metchis H., Singleton S., 2003, 'Spam, That Ill O' The ISP: A Reality Check for Legislators, Competitive Enterprise Institute'

Moustakas E., Ranganathan C., Duquenoy P., 2005, Combating Spam Through Legislation: A Comparative Analysis of US and European Approaches, Conference on Email and Anti-Spam,
http://pdf.aminer.org/000/085/114/combating_spam_through_legislation_a_comparative_analysis_of_us_and.pdf
Last accessed on 03.09.2013

Newell B. C. , 2011, 'Rethinking Reasonable Expectations of Privacy in Online Social Networks', Richmond Journal of Law and Technology, Vol. XVII, Issue 4

O'Beirne B., 2009, 'The European Court of Human Rights' recent expansion of the right of privacy: a positive development?', Coventry Law Journal

Sahin O., 2011, 'Elektronik Haberlesme Sektorunde Kisisel Verilerin Islenmesi, Saklanmasi ve Gizliliginin Korunmasi (Processing, Retention and Protection Personal Data in Electronic Communications Sector), ICT Expertise Thesis ICTA Turkey

Tan D. R., 1999, "Personal Privacy In The Information Age: Comparison Of Internet Data Protection Regulations In The United States And The European Union", Loyola of Los Angeles International and Comparative Law Journal 21

Tene O. & Saygin Y., 2011, 'Privacy and Data Protection in Turkey: (Inching) Towards a European Framework', Privacy & Security Law Report 10 http://ssrn.com/abstract=1941005

Warren S.D., Brandeis L.D., 1890, 'The Right to Privacy', Harvard Law Review, Vol.4 No.5

Wong R., 2007, 'Data Protection Online: Alternative Approaches to Sensitive Data?', Journal of International Commercial Law and Technology Vol. 2, Issue 1

III. Official Reports

Article 29 - Data Protection Working Party, 2000, Working Document Privacy on the Internet- An integrated EU Approach to On-line Data Protection

Article 29 – Working Party, 2002, 'Opinion 5/2002 On The Statement Of The European Data Protection Commissioners At The International Conference In Cardiff (9-11 September 2002) On Mandatory Systematic Retention Of Telecommunication Traffic data'

Article 29 – Working Party, 2005, 'Opinion 5/2005 On the Use of Location Data With a View to Providing Value-Added Services'

Article 29 - Data Protection Working Party, 2008, 'Opinion 1/2008 On Data Protection Issues Related To Search Engines'

Article 29 Data Protection Working Party, 2010, 'Opinion 2/2010 On Online Behavioural Advertising'

Article 29 - Data Protection Working Party, 2011, 'Opinion 15/2011 On The Definition Of Consent',

Article 29 Working Party, 2013,' Opinion 03/2013 On Purpose Limitation'

Cuijpers C., Roosendal A., Koops B., 2007, 'D11.5 The Legal Framework for Location Based Services in Europe', Future of Identity in the Information Society Working Party Report
http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP11-del11.5-legal_framework_for_LBS.pdf
Last accessed on 25.08.2013

European Commission, 2010, Commission Staff Working Document Turkey 2010 Progress Report,
http://ec.europa.eu/enlargement/pdf/key_documents/2010/package/tr_rapport_2010_en.pdf
Last accessed on 09.09.2013

European Commission, 2012, Commission Staff Working Document Turkey 2012 Progress Report,
http://ec.europa.eu/enlargement/pdf/key_documents/2012/package/tr_rapport_2012_en.pdf
Last accessed on 09.09.2013

Information Commissioner's Office, 2006, Guidance On The Privacy And Electronic Communications (EC Directive) Regulations 2003 Part 2: Security, Confidentiality, Traffic And Location Data, Itemised Billing, CLI And Directories v3.4

The Office of Data Protection Commissioner, 'Guidance Note on Data Protection in the Electronic Communications Sector',
https://www.dataprotection.ie/documents/guidance/Electronic_Communications_Guidance.pdf
Last accessed on 20.08.2013

Türkiye Bilisim Dernegi (Informatics Association of Turkey), 2008, Kişisel Verilerin Korunması (Working Group Report on Protection of Personal Data), www.tbd.org.tr/usr_img/cd/kamubib14/raporlarPDF/RP2-2008.pdf
Last accessed on 28.08.2013

IV. Legislation

By-Law on Consumer Rights in the Electronic Communications Sector, 2010, Official Gazette No:27655 dated 28/07/2010
http://btk.gov.tr/mevzuat/yonetmelikler/dosyalar/tuketici-haklari.pdf Last Accessed on 07.09.2013

By-Law on Processing of Personal Data and Protection of Privacy in Electronic Communications Sector, 2012, Official Gazette No:28363 dated 24/07/2011

Draft Law on Processing of Personal Data,
http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Kanuntas/kisiselveriler.pdf
Last accessed on 25.08.2013

European Commission, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data

European Commission, Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive)

European Commission, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector (Directive On Privacy And Electronic Communications)

European Commission, Directive 2006/24/EC of the European Parliament and of the Council Of 15 March 2006 On The Retention Of Data Generated Or Processed In Connection With The Provision Of Publicly Available Electronic Communications Services Or Of Public Communications Networks And Amending Directive 2002/58/EC

European Convention on Human Rights, 1953

Turkish Civil Code (No:4721), 2001, Official Gazette No:24607 dated 8/12/2001

Turkish Constitution

Turkish Criminal Code (No:5237), 2004, Official Gazette No. 25611 dated 12/10/2004

Turkish Electronic Communications Law (No:5809), 2008, Official Gazette No:27050 dated 10/11/2008

Turkish Electronic Signature Law (No:5070), 2004, Official Gazette No:25355 dated 23/1/2004

Turkish Law Concerning the Amendment of Certain Laws (No:5397), Official Gazette No:25884 dated 23/07/2005

Turkish Law on the Right to Access to Information (No:4982), 2003, Official Gazette No:25269 dated 24/10/2003

United Nations, 45/95 Guidelines For The Regulation Of Computerized Personal Data Files

V. Cases

Case C-101/01, 2003, Criminal proceedings against Bodil Lindqvist,
http://curia.europa.eu/juris/liste.jsf?language=en&num=C-101/01

ICTA Board Decision 2011/DK-10/83, 2011,
http://btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-10-83sss.pdf
Last accessed on 08.09.2013
ICTA Board Decision 2011/DK-10/198, 2011,
http://btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-10-198.pdf
Last accessed on 08.09.2013

ICTA Board Decision 2011/DK-14/659, 2011,
http://btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-14-659.pdf
Last accessed on 08.09.2013

ICTA Board Decision 2013/DK-SDD/228, 2013,
http://btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2013%20DK-SDD-228.pdf
Last accessed on 08.09.2013

VI. Other Sources

Altheim M., 2011, 'The Meaning of "Consent" in the EU Data Protection Framework: A New Article 29 Working Party Opinion',
http://ediscoverymap.com/2011/07/the-meaning-of-%E2%80%9Cconsent%E2%80%9D-in-the-eu-data-protection-framework-a-new-article-29-working-party-opinion/
Last Accessed on 22.08.2013

Clarke R., 2006, Introduction to Dataveillance and Information Privacy, and Definitions of Terms, http://www.rogerclarke.com/DV/Intro.html
Last Accessed on 18.08.2013

Data protection in Turkey: Overview, http://uk.practicallaw.com/7-520-1896#a120099
Last accessed on 04.09.2013

Data Protection Overview (Turkey), http://www.gurlaw.com/data-protection-overview-turkey/
Last accessed on 01.08.2013

EU: IP Addresses Are Personal Information, 2009, http://www.cbsnews.com/2100-205_162-3734904.html
Last Accessed on 20.08.2013

Gartner Says Worldwide PC, Tablet and Mobile Phone Shipments to Grow 5.9 Percent in 2013 as Anytime-Anywhere-Computing Drives Buyer Behaviour, http://www.gartner.com/newsroom/id/2525515
Last Accessed on 10.08.2013

Ministry of Justice webpage,
http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Basbakanlik.html
Last accessed on 06.09.2013

Prime Ministry of Republic of Turkey, 2008, General Preamble fort he Draft Law on Protection of Personal Data www2.tbmm.gov.tr/d23/1/1-0576.pdf
Last Accessed on 05.09.2013

The Presidency of Communication Webpage, Legislation, http://tib.gov.tr/tr/tr-menu-12-ilgili_denetim_mevzuati.html
Last accessed on 08.09.2013