PROTECTION OF PERSONAL DATA IN INTERNATIONAL LAW AND THE GENERAL ASPECTS OF THE TURKISH DATA PROTECTION LAW*

Dr. İlke GÜRSEL**

Abstract

Personal data is defined as any information relating to an identified or identifiable natural person. By means of personal data, it is possible to obtain a detailed portrait about an individual to whom personal data relate. Taking account of the rising amount of data processing in the modern world, personal data become more vulnerable to attacks from third parties. The challenges encountered with regard to data protection have been discussed and handled very delicately in international law for a long time. In respect of Turkish legislation, the Law on the Protection of Personal Data No. 6698, which entered into force at the beginning of April 2016, is the first specific and comprehensive law in this field. In this study, our main purpose is to reveal the general terms and principles laid down in the Turkish Data Protection Law and to express some basic similarities and differences between this Law and the EU Data Protection Directive, which is a leading document in the field of data protection.

---

* Have been taken into account some of the findings and analyses discussed within *"The Right to Data Protection of the Employee*" to be presented at the 1st International Scientific Researches Humanity and Social Sciences Conference (May 19-22, 2016, Madrid, Spain).

** Dr. İlke Gürsel is a research assistant at the Department of Social Security and Labour Law, Faculty of Law, Dokuz Eylül University, İzmir, Turkey. (Dokuz Eylül Üniversitesi Hukuk Fakültesi, İş ve Sosyal Güvenlik Hukuku Anabilim Dalı (e-posta: ilkekdas@gmail.com) (Makale Gönderim Tarihleri: 13.05.2016-16.05.2016/Kabul Tarihleri: 13.06.2016-02.09.2016))

Keywords

Personal Data, Right to Data Protection, International Instruments on Data Protection, Data Protection Law No. 6698

ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASI VE TÜRK VERİ KORUMA KANUNUNUN GENEL ÖZELLİKLERİ

Öz

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanabilir. Kişisel veriler aracılığıyla, bu verilerin ilgili olduğu birey hakkında ayrıntılı bir portre elde edilmesi mümkündür. Modern dünyada artış gösteren veri işleme miktarları göz önüne alındığında, kişisel veriler üçüncü kişilerin saldırılarına daha açık hâle gelmektedir. Verilerin korunması hususunda karşılaşılan zorluklar uluslararası hukukta uzun zamandan beri tartışılmakta ve dikkatli bir şekilde ele alınmaktadır. Türk hukuku bakımından ise, Nisan 2016'nın başında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun bu alandaki ilk özel ve kapsamlı kanunu oluşturur. Bu çalışmada temel amacımız, Kişisel Verilerin Korunması Kanununda yer alan genel kavramları ve kuralları ortaya koymak ve bu Kanun ile veri koruma hukuku açısından öncü bir belge niteliği taşıyan Avrupa Birliği Veri Koruma Direktifi arasındaki temel benzerlikleri ve farklılıkları açıklamaktır.

Anahtar Kelimeler

Kişisel Veriler, Kişisel Verilerin Korunması Hakkı, Kişisel Verilerin Korunmasına Yönelik Uluslararası Belgeler, 6698 Sayılı Veri Koruma Kanunu

INTRODUCTION

Any information which can be associated with an individual falls within the content of the term *"personal data*". As presenting information about a natural person regarding his/her private life and even professional activities, personal data have indisputable value for data subjects. In consequence of ever-expanding effects of modern information technology, dependence upon data processing activities has continuously grown. Accordingly, data subject's concern about protecting his/her personal data against unauthorized data processing has deepened increasingly. In this context, the right to protection of personal data basically intends to establish and then pursue the balance between the justified interests of the main actors in data processing (i.e. data subject and data controller).

This study consists of two main sections. The first section begins with general information about data protection in an international perspective. Specifically, the emergence of data protection law, its historical background and leading documents in this field will be explained briefly in this section. This section is followed by a general overview of data protection in Turkey in the light of its former situation and new developments subsequent to the enactment of a specific Law in Turkey.

I. OUTLOOK OF INTERNATIONAL DATA PROTECTION INSTRUMENTS

A. Overview

Today, it is obvious that information has a crucial importance in terms of economic, social and political considerations. Francis Bacon, one of the most notable philosopher during the transition from the Renaissance to the early modern era, stated that knowledge itself has an enormous power. This emphasis on *"having knowledge"* draws attention to the broad competence which will be enjoyed by the owner of information. Due to considerably large scale investments and accordingly the occurrence of innovative applications within information industry over the past decades, dependence on information has increased and leads to the idea that data processing is an indispensable activity.

Widespread usage of the internet around the world is an another substantial factor giving contribution to the increase of data processing. It is doubtless that the internet allows easier and rapid exchanges of information between individuals, no matter how far they are separate from each others. Continuous circulation of individuals' information through the internet facilitates unauthorized access to personal data and therefore reasonable concerns about unfair processing activities have been constantly triggered[1]. Keeping in mind that once we show up on the internet, all our activities being performed or the web-sites being visited are recorded, and subsequently the whole information becomes our digital traces of personal lives[2]. Hence, data protection against abuses by third parties becomes indeed a sensitive and effortful issue to deal with. The developments mentioned above prompted the states and the international institutions to elaborate on this problem and set out a legal framework about data processing.

B. Regulatory Instruments

There have been notable international documents aiming to outline a proper and legitimate processing system. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which were published in 1980, can initially be mentioned among these international instruments. Even if the OECD document has not a binding force, its fundamental principles are regarded as guiding rules for the countries in which the field of data protection was not specifically regulated[3]. New technologies and modern communications networks led to the necessity of updating its rules in order to enhance the level of protection. Accordingly,

---

1 **Klosek**, Jacqueline: Data Privacy in the Information Age, Greenwood Publishing, United States 2000, p. 1; **Sieber**, Ulrich: "The Emergence of Information Law: Object and Characteristics of a New Legal Area", Law, Information and Information Technology, (Ed. Eli Ledermen/Ron Shapira), Kluwer Law International, The Hague 2001, p. 8.

2 **Klosek**, p. 9.

3 **Blume**, Peter/**Saarenpää**, Ahti/**Schartum**, Dag Wiese/**Seipel**, Peter: Nordic Data Protection, Iustus Förlag, Uppsala 2001, p. 6.

OECD issued the updated Guidelines[4] in 2013. Since still being accepted as a set of special rules regarding data protection, OECD Guidelines have significant impacts on both the OECD Member States and beyond[5]. As regards data protection, the United Nations' (UN) effort must be emphasized. In 1990, *UN Guidelines for the Regulation of Computerized Personal Data Files* adopted by the General Assembly encompass nine basic principles[6], which are all advisory.

The Council of Europe, established in 1949, is an intergovernmental institution focusing on human rights, democracy and the rule of law. In this context, the Council adopted *the Convention for the Protection of Human Rights and Fundamental Freedoms* (European Convention on Human Rights (ECHR)) in 1950. Pursuing an aim to maintain the further acceptance and application of the rules laid down in the Universal Declaration of Human Rights, the Convention particularly provides *the right to respect for private and family life* in Article 8. As it can be seen in the content of this Article, the right to data protection has not explicitly been referred to. However, a special emphasis must be put on the application of this Article developed by the European Court of Human Rights. In consequence of unprecedented technological developments, the Court has expanded the practice of Article 8 so as to examine the complaints with regard to misuse of personal data. For example, the Court highlighted in *M.S./Sweden Case*[7] that protection of

---

4 Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

5 See the OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, (15.04.2016).

6 These rules are as follows: principle of lawfulness and fairness, principle of accuracy, principle of the purpose-specification, principle of interested-person access, principle of non-discrimination, power to make exceptions, principle of security, supervision and sanctions, transborder data flows. For the full text of these principles, see http://www.refworld.org/docid/3ddcafaac.html, (15.04.2016).

7 See *M.S. v. Sweden*, (20837/92), 27.08.1997. In this judgment, without her consent the applicant's medical data was sent to the Social Insurance Office from a clinic in which the applicant had treatment before. The Social Insurance Office had actually examined her medical records upon her application to the Office for obtaining a compensation provided under the Industrial Injury Insurance Act. The applicant claimed that the delivery of her medical records caused an unjustified interference with her right to

personal data *"is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention"*[8]. Thus, it would not be wrong to say that the European standards on data protection have been strengthened and extended through the generous interpretation of the jurisprudence of the Court. Being highly aware of the rapid progress and increase in the field of data processing, the Council of Europe pointed at the importance of adopting international obligatory rules which would serve as a model for national data protection legislations. *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (briefly, the CoE Convention No. 108) was accordingly issued in 1981, which is still accepted to be *the only binding international legal document with a worldwide scope of application in this field since it is open to member and non-member States of the CoE*[9]. While the Council was establishing the principles set out in the CoE Convention No. 108, one of the Council's aim was to materialize the essentials put forward by Article 8 in ECHR and to determine more specific guarantees on data protection.

It is noteworthy that data protection law is of vital importance in European countries since the 1960s, and indeed substantial steps have been taken in this field from those dates. For instance, the Land of Hesse in Germany adopted a data protection act in 1970, which appears to be the first one in this area around the world[10]. Afterwards, some European countries such as Sweden, Austria, Denmark, France followed the same path and

---

respect for private life in light of Article 8. The Court held that there were relevant and sufficient reasons for the submission of the applicant's medical records by the clinic to the Office and that the measure was not disproportionate to the legitimate aim pursued. The Court thus concluded that there was no violation of the Convention (para 44).

8 See **Council of Europe**: Data Protection Compilation of Council of Europe Texts, Strasbourg 2010, p. 7; http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf, (15.04.2016).

9 Data Protection Compilation of Council of Europe Texts, p. 7.

10 **Henderson**, Sandra C./**Synder**, Charles A.: "Personal Information Privacy: Implications for MIS Managers", Information & Management, Vol.36, 1999, p. 214; **Küzeci**, Elif: Kişisel Verilerin Korunması, Turhan Kitabevi, Ankara 2010, p. 107.

enacted specific acts in their domestic laws during the 1970s[11]. It should be underlined that data protection was enshrined in several constitutions as a fundamental right[12] even before particular reference was made in the Article 1/1 of the EU Directive 95/46/EC. In addition to these legislations, *the Population Census Decision* (1983), where the German Constitutional Court recognized *the right to informational self-determination*[13] as a legal reference point for data protection in German law[14], had also a considerable influence on the developments of European data protection law[15].

Moreover, in order to harmonize the free flow of personal data between EU Member States and to provide a general protection level all around the European Union[16], *the Directive 95/46/EC of 24 October 1995* on data protection (the EU General Directive)[17]was introduced and a three-year period was given to the Member States for its implementation. As of today, all EU Member States have complied with the General Directive and have adopted data protection laws at national level. By virtue of its highly

---

11 **Henderson/Synder**, p. 214; **Küzeci**, p. 107-108; **Krause**, Rüdiger: "New Developments in Data Privacy for Employees in German Law", The Law in the Information and Risk Society, (Ed. Gunnar Duttge/Sang Won Lee), Universitätsverlag Göttingen, 2011, p. 89.

12 For example, this right is provided in the Portuguese Constitution of 1976 and the Spanish Constitution of 1978. See **Kuner**, Christopher: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, United Kingdom 2007, p. 18, fn. 67; Also see the Netherlands Constitution of 1983.

13 Under this right, each individual is entitled to make a decision about the time of processing and the authorized person/persons to process his/her data. See **Yıldırım**, Nuriye: "Germany", Employment Privacy Law in the European Union: Human Resources and Sensitive Data, (Ed. Frank Hendrickx), Intersentia Publishers, Belgium 2003, p. 120; For more information, see **Hornung**, Gerrit/**Schnabel**, Christoph: "Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination", Computer Law & Security Review, Vol.25, 2009, p. 85-86.

14 **Hornung/Schnabel**, p. 84-85.

15 **Determann**, Lothar/**Sprague**, Robert: "Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States", Berkeley Technology Law Journal, Vol.26, 2011, p. 1025, fn. 238; **Kuner**, p. 18.

16 **Kuner**, p. 20; **Henderson/Synder**, p. 215; See also Directive 95/46/EC, Art. 1/1-2.

17 Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, (16.04.2016).

developed mechanism for cross-border data transfers, the EU General Directive has a growing effect in the field of data protection throughout the world[18].

Since 2012, a new legislative framework (so-called General Data Protection Regulation (GDPR)) has been worked on to reinforce the standards of data protection in EU and to update the provisions of the EU General Directive. At the end of December 2015, an agreement on this new framework was reached between the European Parliament, the Council and the Commission of the EU. In April 2016, the last version of the GDPR was respectively approved by the Council of the European Union and the European Parliament[19]. Ultimately, the official text of the GDPR[20] has been published in the Official Journal of the EU on 4 May 2016. Under Article 99 of the GDPR, a two-year transition period starting from its enforcement date (24 May 2016) is given to the Member States and the Regulation shall thus become directly applicable in all Member States on 25 May 2018[21].

Furthermore, the importance of the right to data protection has been once again reiterated by Article 8 of the Charter of Fundamental Rights of the European Union in which a duty is imposed on the Member States to fully respect this right. As the Charter has become legally binding since 2009, the acceptance of data protection as a fundamental citizen right in Europe has been established.

---

18 See the Communication of the European Commission of 4 November 2010 (COM(2010) 609 final), p. 16, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, (16.04.2016).

19 For more information on the developments and the renewals of the GDPR, see http://ec.europa.eu/justice/data-protection/reform/index_en.htm; http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-regulation/, (17.04.2016).

20 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),*OJ L 119, 4.5.2016, p. 1-88,* Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC, (12.05.2016)

21 See http://ec.europa.eu/justice/data-protection/, (12.05.2016).

II. DATA PROTECTION LAW SYSTEM IN A NATIONAL PERSPECTIVE

As stated above, massive progress in electronic data processing and the advent of the internet have simplified data processing. Apart from this, considerable flow of information in each market increases since the actors of the worldwide economy have noticed the economic value of personal data. This combination is virtually putting pressure on natural and/or legal persons to reach third party's data. Consequently, a multiplied need for information leads to raise the amount of unjustified data processing and to endanger the right to data protection of individuals. These adverse effects also exist in our country. Actually, until the enactment of the Data Protection Law No. 6698 on 24 March 2016, the conflicts on data protection were rather handled by several provisions in the Turkish legislation.

In this section, Turkish data protection system will be examined into two subsections to demonstrate general features of data protection in Turkey and consequences resulting from the codification of Data Protection Law. So, the first following part is focusing on the former structure of Turkish legislation (prior to the introduction of the Data Protection Law) and then the second part is exposing the general framework of the Law dedicated to data protection.

A. First Related Regulations in the Field of Data Protection in Turkish Law

Different aspects of the data protection issue have been regulated in a number of Turkish laws. First of all, it is worth referring that Article 20/3 of the Turkish Constitution is the fundamental base of data protection in our law system. According to this Article, everyone has a right to protection of his/her own personal data. The right to data protection confers upon each individual the powers to be informed of his/her personal data, to have access to data, to request the correction or erasure and to find out if his/her data are used in accordance with the prescribed purposes. Personal data shall only be processed under the grounds put forward by the law or with the explicit consent of the data subject.

In addition to this constitutional provision, there are also some legal provisions which partially ensure protection against unfair processing. For instance, *the Turkish Criminal Code No. 5237* brings specific guarantees in case of violation of individuals' personal and fundamental rights on data protection through illegal data processing. In this regard, Article 135 sets out that a person who records personal data unlawfully will be punished with a prison sentence of one to three years. Apart from this, under Article 135/2, it is stipulated that *(i)* the recording of personal data concerning political, philosophical or religious opinions, racial origins; *(ii)* illegally recording of personal data revealing moral tendencies, sex life, health conditions or trade-union relationship is sentenced to a term of imprisonment. According to Article 136, unlawful transmission, dissemination or collection of personal data is a criminal offence with an imprisonment for two to four years. In the event that a person charged with the erasure of personal data does not implement his/her duty in spite of expiration dates prescribed by law, he/she will be imprisoned from one to two years (Article 138/1).

As regards *the Turkish Civil Code*, there is no particular provision regarding data protection. Nevertheless, any person whose personal data is processed in an unlawful manner can invoke the safeguards introduced in Articles 23-25 of the Turkish Civil Code, because unlawful interference with personal data might be considered as a breach of his/her personal right. Under Article 23/2, an individual's waiver of his/her own freedoms or restrictions in breach of law or morals are all invalid. Article 24/2 provides that any person can request the protection of his/her personal right against the offender(s) in case of unlawful attacks on personal rights. Accordingly, an individual may bring a lawsuit to prevent an unlawful imminent attack, to terminate the existing unfair intervention or to determine its contradiction to law. With regards to civil remedies, compensation of his/her pecuniary and/or non-pecuniary damages will as well be requested from the offender (Article 25).

Besides these general guarantees, a more concrete provision is brought by Article 419 of *the Turkish Code of Obligations*. According to this, an

employer shall use[22] personal data of an employee only to the extent that these data are related to his/her aptitude for the job[23] or required by the performance of the employment contract. Thus, without prejudice to compliance with the provisions specified in the Turkish Data Protection Law, the employer should depend on one of these legal grounds in cases of employee's personal data processing in the employment relationship.

Likewise, in labour and social security law legislation, some provisions are applicable to data protection of workers and social insurance beneficiaries. Firstly, Article 28 of *the Turkish Labour Code No. 4857*, where a duty for an employer to draw up a *"certificate of employment"* is provided, states that the employer is under the obligation to reveal correct information about his/her previous employee in the certificate. Otherwise, the employer who fails to fulfill this duty will be requested to compensate the eventual damages of his/her previous employee or of the new employer who has recruited this employee. Secondly, Article 75/2 of the Turkish Labour Law imposes a duty upon the employer to use the information being obtained while keeping a personal file about his/her employee in accordance with good faith and law. In addition to this, the employer shall not reveal the information as long as the employee has a justified interest in keeping this information secret.

Moreover, pursuant to *the Occupational Health and Safety Law No. 6331*, health data of workers derived from medical examinations during the

---

22 It must be emphasized that confining the scope of application of this provision merely to *"using of personal data"* entails to limit its level of protection. Hence, this term can be appreciated as *"processing of personal data"*, which also corresponds to the expression laid down in Article 328b of the Swiss Code of Obligations. See **Sevimli**, Ahmet: "Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419", Sicil İş Hukuku Dergisi, Vol.24, December 2011, p. 134; **Okur**, Zeki: İş Hukuku'nda Elektronik Gözetleme, Legal, İstanbul 2011, p. 77.

23 The term *"aptitude"* should be construed as qualifications to demonstrate the suitability of the employee/prospective employee for the related duty such as his/her education, specialty, skills, certifications and diplomas; As to *Sevimli*, efficiency and performance of an employee are also relating to the term *"aptitude"*, so they can be processed during the employment relationship. See **Sevimli**, p. 134.

employment relationship must be kept confidential by their employers in order to safeguard workers' private lives and reputations (Article 15/5).

Similarly, it is essential to observe the secrecy of health data concerning the insured person with regard to general health insurance and his/her legal dependents under Article 78/2 of *the Social Insurances and General Health Insurance Law No. 5510*. Another piece of legislation that will be accepted as a basis of protection of insured persons' data is *the Social Security Institution Law No. 5502*. In accordance with Article 35/6, the transfers to third parties of personal data relating to insured persons which are being processed by the Institution to implement its tasks should take place only if a notarized consent is given by the related data subject.

B. Enactment of the Law on the Protection of Personal Data No. 6698 and Its Protection Regime

It is apparent that the specific provisions listed above are not sufficient to attain satisfactory results on data protection in the absence of a comprehensive law. Therefore, setting out specific principles for data processing activities seems crucial to protect the individual's right to data protection. Besides that, Turkey, as a candidate for EU membership, has committed itself to harmonize its domestic law with EU rules and regulations. As stated before, the Member States of EU have rigorously dealt with this issue for a long time and a high data protection level has been reached. All these considerations are, therefore, incentives to adopt special regulations on data protection in Turkey.

During the 2000s, numerous drafts on data protection were prepared, but none of these texts were enacted. In January 2016, a new draft law issued by the Ministry of Justice was submitted to the Turkish Grand National Assembly by the Prime Ministry and the last version was finally legislated with some changes following two months of intensive negotiations in the Assembly. *The Law on the Protection of Personal Data No. 6698* has then been adopted on 24 March 2016 and published in the Official Journal of 7th of April. Furthermore, another major step has been taken by the Assembly in the data protection area at the beginning of 2016. Although Turkey is among the Signatory States to the CoE Convention No. 108 since 1981, the

ratification procedure has been newly fulfilled. First of all, the Law No. 6669[24] has been enacted to authorize the notification of the Convention No. 108 on 30 January 2016. Hereafter, the decree of ratification (no. 2016/8576) on this subject has been taken by the Council of Ministers and published in the Official Journal[25]. Subsequent to all these steps, the Convention No. 108 has gained a binding force in our national law.

With its enactment of the Data Protection Law, it becomes the primary source governing data processing activities in Turkey. This legislative step is enthusiastically welcomed and it marks a substantial (but not a conclusive) initiative to catch up with the international standards on this matter. While working on the draft law, the Turkish legislator was inspired by the principles and rules set out in the CoE Convention No. 108 and specifically the EU General Directive. Taking account of the Turkish Law on data protection and the EU General Directive, many similarities in their systems will draw attention at first sight. Yet, when carefully compared to the EU General Directive, the Turkish Law has some important differences that hopefully will not undermine the enforcement and strength of this Law in the future.

1. Purpose, Scope and Fundamental Concepts

First of all, the purpose of this Law as stated in Article 1 is to protect individuals' fundamental rights and freedoms (in particular, the right to privacy) with regard to data processing and to administer all rules and procedures to be implemented during processing activities. The provisions in the Law are designed to grant a protection only to natural persons. In other words, legal persons' data cannot benefit from the guarantees envisaged in the Law. In parallel with the related international documents, personal data is defined as *any information relating to an identified or identifiable natural person* in Article 3(d). For instance, name, address, date of birth, passport number, shoe size, DNA sample, credit card number, favourite restaurant, sexual preferences, destination of air travel, license plates, social insurance number, image or sound recording, e-mail address, hobbies, affiliations; all

---

24 Available at the Official Journal No. 29628, published on 18 February 2016.

25 Available at the Official Journal No. 29656, published on 17 March 2016.

this information amounts to personal data. As obvious, every kind of information which concerns a living individual may be within the scope of this definition. The list of personal data can, therefore, be easily extended and diversified[26]. While determining whether an information is a personal data or not, it should suffice that this information matches to a particular person or at least it makes identification of that person considerably easier[27].

This Law applies to all natural and legal persons' data processing activities that are performed by automatic means wholly or partly, and also by manual means on the condition that the related processing activity should be part of a data filing system (Article 2). Thereby, to fall within the scope of application, there is no difference between processing data completely or partially by automatic means[28]. Nevertheless, manual data processing (for example, paper-based records) can be covered provided that these data are involved in a filing system which is structured to supply easy access to the related personal data[29]. This Law provides same protection level without considering if personal data are processed in the public or private sector.

As establishing a number of exemptions to the general data protection system, Article 28 is another important article in the Law with regard to the scope of application. Particularly, the exception of data processing relating to intellectual activities excluded from the scope of the rights and obligations laid down in the Law seems not to be consistent with the EU General Directive. Due to the fact that *"intellectual activity"* is not an explicit term

---

26 **Carey**, Peter: Data Protection: A Practical Guide to UK and EU Law, Third Edition, Oxford University Press, United States 2009, p. 17-18; See also the Judgment of the Constitutional Court of the Republic of Turkey, 9 April 2014, case number 2013/122 - 2014/74.

27 **Kuner**, p. 92; **Council of Europe**: Handbook on European Data Protection Law, 2014, p. 39, Available at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_ documents/handbook_on_european_data_protec.asp, (30.04.2016).

28 The term *"automated means"* can be understood as data processing by computers and software, such as computerized databases and IT networks. See **Büllesbach**, Alfred/**Gijrath**, Serge/**Poullet**, Yves/**Prins**, Corien: Concise European IT Law, Second Edition, Kluwer Law International, United Kingdom 2010, p. 42.

29 See the EU General Directive Recital 15, 27; **Carey**, p. 21; **Büllesbach/Gijrath/ Poullet/Prin**s, p. 43; Handbook on European Data Protection Law, p. 47.

allowing an exact definition, it is likely to encounter unjustified data processing to be performed by public institutions authorized in collecting intelligence (such as police department, gendarmerie and national intelligence organization). Hence, this exemption grants a broad discretion on processing personal data to the State itself without being subjected to the peremptory rules of the Law, and thereby gives an opportunity to preclude data protection measures for the public sector. On the other hand, it is evident that ensuring effective data protection depends on the extent to which both the public and private sectors are able to fulfill their commitments on this matter. This exemption should therefore be invoked with caution.

According to Article 3, *"data subject"* means a natural person whose personal data are processed. Additionally, *"processor"* is defined as a natural or legal person which processes personal data on behalf of the controller depending on the authorization given by him/her, and *"data controller"* means a natural or legal person which determines the purposes and means of processing of personal data and is liable to establish and manage a data filing system.

The Law defines the term *"processing of personal data"* as any operation which is performed upon personal data, by automatic means in whole or in part, or by non-automatic means insofar as the data processed form part of any filing system, such as collection, recording, storage, retention, alteration, reorganization, disclosure, transmission, acquisition, classification or blocking. This broad list is not exhaustive[30] so that new forms of handling personal data will be added by taking into account innovations in technology market. Given the wide nature of the term, it must be highlighted that even a simple storage of personal data on a diskette or CD is accepted as *"processing"*, regardless of whether the related data are further processed or not[31].

As the term *"explicit consent"* is one of the criteria provided for to make data processing legitimate in the Law, the definition of this term is of substantial importance. Under Article 3(a), it is defined as any freely given

---

30 **Büllesbach/Gijrath/Poullet/Prins**, p. 36; **Carey**, p. 24.

31 **Kuner**, p. 75.

specific and informed indication of the person's wishes to show his/her agreement to data processing. According to the Article 29 Working Party (an expert institution established pursuant to Article 29 of the EU General Directive to prepare advisory opinions on EU data protection legislation), the conditions of a valid consent can be classified as follows: clear and unambiguous indication of wishes, freely given, specific and informed[32]. In addition to these elements, the Turkish legislator seeks one more condition that the data subject shows his/her agreement in an explicit way. In other words, explicit consent must be given by a specific and intentional act, which can be made either orally or in writing. It must, however, be underlined that a simple conclusion to be inferred from the behaviour of the data subject cannot amount to a valid explicit consent[33]. This requirement is regulated differently in the EU General Directive. Because, the General Directive stipulates the existence of an explicit consent only if sensitive data are processed; otherwise the consent given in a non-explicit way is found sufficient as a legal ground to process.

In parallel with the General Directive, the Law created a special category which is called *"sensitive personal data"*. The concept of sensitive personal data is not defined in the Law, whereas an explanatory list and the conditions under which these kinds of personal data are allowed to be processed are arranged in detail. According to the 15th Chamber of the Turkish Council of State *(Danıştay)*, there is a concrete link between sensitive data and fundamental rights of an individual and consequently these kinds of data require more effective and special safeguards in comparison with other personal data[34]. For instance, in the event of public disclosure of sexual orientation or health data about a severe illness, it is more likely that the individual concerned faces with negative consequences

---

32 **Kuner**, p. 67; See also **Article 29 Data Protection Working Party**: Opinion 15/2011 on the definition of consent, 01197/11/EN WP187, 13.07.2011, p. 11-25, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf, (01.05.2016).

33 **Büllesbach/Gijrath/Poullet/Prins**, p. 61; Handbook on European Data Protection Law, p. 56.

34 Council of State 15th Chamber, 8 July 2014, case number 2014/1150.

(such as discriminative treatments) in his/her social life[35]. In this regard, it is essential to set out stringent requirements to protect sensitive data in national data protection legislations. Under Article 6/1, sensitive personal data consist of information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, appearance and clothing, membership of association, foundation or trade-union, health or sexual life, criminal convictions and security measures and also biometric and genetic data.

2. Main Principles and Legal Grounds to Legitimize Data Processing

Throughout data processing activities, there is a number of fundamental principles that the controller shall follow in order to meet data protection conditions. Primarily, data must be processed fairly and lawfully (Article 4/2(a)). This principle involves two independent obligations at the same time, namely *lawfulness* and *fairness*. According to lawfulness, it refers to the need for relying on a legal basis and data processing must be performed in a way that this operation does not violate any data protection provisions or other legal requirements[36]. Additionally, data processing will be considered as *"fairly"* where a balance can be established between divergent interests; the data subject's interest in the right to data protection/the right to privacy on one hand, third parties' interest in obtaining information on the other[37]. Moreover, fair processing needs also *transparency* of data processing, which

---

35 **Article 29 Data Protection Working Party**: Advice paper on special categories of data ("sensitive data"), Ref. Ares (2011) 444105, 20.04.2011, p. 4-5, Available athttp://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf, (01.05.2016); **Büllesbach/Gijrath/Poullet/Prins**, p. 60.

36 **Büllesbach/Gijrath/Poullet/Prins**, p. 51; **Article 29 Data Protection Working Party**: Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN WP 48, 13.09.2001, p. 18, Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf, (01.01.2014); **Yüksel**, Saadet: Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale, Beta, İstanbul 2012, p. 111; **Küzeci**, p. 196.

37 **Büllesbach/Gijrath/Poullet/Prins**, p. 51.

requires a duty for the data controller to keep the data subject informed about at least the purposes of data processing and the identity of the controller[38].

Personal data must be accurate and where necessary, kept up to date (Article 4/2(b)). This principle necessitates the controller to check if the data to be processed are correct and updated. For the sake of actors in data processing, the controller would rather use the information after verifying the correctness and actuality of the related personal data. Otherwise, processing of incorrect and outdated information virtually gives rise to adverse impacts on the interests of the data subject/data controller/third parties[39]. Under Article 4/2(d), personal data must be kept as long as it is required by the related legislation or necessary for the purposes for which personal data are processed. As obvious, this obligation ensures the data subject a guarantee to be protected against serious risks arising from a long-time data storage.

Personal data must be processed for specified, explicit and legitimate purposes. The principle of purpose limitation is internationally accepted as a very substantial rule in the field of data protection. This principle shall be for the controller to determine that the purposes pursued by him/her for processing data are *(i*) defined and made explicit; *(ii)* lawful or legitimate; *(iii)* not incompatible with the purposes for which the data are originally collected[40]. Personal data must be relevant, limited and proportional in relation to the purposes for which they are processed (Article 4/2 (ç)). This principle signifies an obligation for the controller to provide that only relevant and necessary data are collected and used in the sense of the controller's purposes for processing such information[41].

---

38 Handbook on European Data Protection Law, p. 73-74; **Yüksel**, p. 111; **Büllesbach/Gijrath/Poullet/Prins**, p. 51; See more, **Kuner**, p. 20.

39 In terms of examples, see Handbook on European Data Protection Law, p. 71-72.

40 **Bygrave**, Lee Andrew: Data Privacy Law: An International Perspective, Oxford University Press, United Kingdom 2014, p. 153, 155; See also **Article 29 Data Protection Working Party**: Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 02.04.2013, p. 15-23, http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf, (01.05.2016).

41 Handbook on European Data Protection Law, p. 70; **Carey**, p. 50; **Kuner**, p. 21.

Article 5 stipulates a set of legal basis to ensure data processing legitimate. The first paragraph states that it is not permitted to process data without the explicit consent of the data subject. This article, however, contains some other legal grounds to process data, irrespective of whether the explicit consent is obtained from the data subject or not (Article 5/2). Accordingly, data processing operations can be carried out under the following conditions where (a) data processing is clearly provided for by law; (b) processing is essential to safeguard the vital interests or physical integrity of the data subject or of another person in the event that the data subject is physically or legally incapable of giving his/her consent; (c) processing of personal data relating to the parties of a contract is necessary providing that the processing activity has a direct relationship with the establishment or fulfillment of this contract; (ç) data processing is required to meet legal obligations of the data controller; (d) personal data have been made public by the data subject; (e) data processing seems obligatory for the establishment, exercise or defence of a right; (f) processing is necessary for the legitimate interests of the controller insofar as this operation does not endanger the fundamental rights and freedoms of the related data subject. As a consequence, the controller should keep in mind these legal grounds enumerated above to perform legitimate processing.

With regard to sensitive data, the legislator has introduced another piece of legal grounds for processing in order to supply further protection to these kinds of data. However, it must be stated that these legal grounds are narrow in comparison with the provisions laid down in Article 8 of the EU General Directive. First of all, it is forbidden to process sensitive data without the explicit consent of the data subject. Conversely, to the extent that it is laid down by law, the controller is entitled to process sensitive data which are referred to in the paragraph 1 except for data relating to health and sexual life (Article 6/3, first sentence). As regards to data revealing health and sexual life, it is valid to process such data only if individuals subjected to the confidentiality obligation or authorized institutions perform processing activity on the purpose of the protection of public health, preventive medicine, medical diagnosis, the provision of care and treatment, the planning and management of health-care services and their finance.

Furthermore, the controller is liable to meet adequate conditions to be provided for by the Personal Data Protection Board (Article 6/4).

3. The Rights and Obligations of the Parties of Data Processing

In order to maintain justified processing operations, the Law provides for a group of rights for the data subject and corresponding responsibilities with regard to the controller. The obligation of controllers to give information to data subjects is explicitly acknowledged in Article 10. In accordance with this Article, the controller or his/her representative shall provide the data subject whose data are obtained with the following information: (a) the identity of the controller and of his/her representative, if any; (b) the purposes of data processing; (c) the recipients to whom personal data are transferred and the purposes pursued in the transmission; (ç) the method and legal ground to collect personal data; (d) other rights of the data subject laid down in Article 11. Taking account of the scope of the information to be provided to data subjects, there is no doubt that the obligation to inform makes a significant contribution to ensure transparency and accordingly fairness of data processing[42]. The controller must comply with this obligation without considering if the data subject makes a request to obtain information or not[43]. According to Article 10, this obligation must be fulfilled, at the latest, at the time of obtaining information[44].

Besides, the obligation to implement security of processing is also incumbent on the controller (Article 12/1). In this regard, the controller is obliged to take all necessary technical and organizational measures to offer an appropriate level of security in an effort to prevent unlawful data processing/access and to ensure the maintenance of personal data. On the other hand, Article 12/2 stipulates that the data controller and processor shall

---

42 **Şimşek**, Oğuz: Anayasa Hukukunda Kişisel Verilerin Korunması, Beta, İstanbul 2008, p. 88; **Küzeci**, p. 212-213.

43 Handbook on European Data Protection Law, p. 96.

44 In the EU General Data Protection Regulation (GDPR), the content and time of providing information differ based on personal data collected from the data subject or third parties. See Articles 13-14.

be jointly responsible for implementing security measures referred to in paragraph 1.

The rights of the data subject are comprehensively introduced in Article 11. This Article primarily sets out that every data subject shall have the right of access. As being indispensable to protect personal data effectively, the right of access has been guaranteed by the Charter of Fundamental Rights of the European Union as a fundamental right in the data protection field[45]. Generally speaking, this right involves two mutually complementary rights; the right of access to one's own data and the right to rectification and erasure. The right of access to one's own data enables the data subject to ask from the controller *(i)* confirmation as to whether his/her personal data are being processed, *(ii)* information as to the data processing operation concerned; the purposes for data processing and whether data relating to him/her are used in accordance with the purposes for which they are processed; third parties to whom these personal data are transferred abroad/within the country (Article 11(a-ç)). It is accepted that this right requires an application of the data subject in order to trigger the responsibility of the controller on his matter[46].

In the event that the data processing operation has been carried out in an incomplete or inaccurate way, the data subject is entitled to request the rectification of these related data. Additionally, this right encompasses an opportunity to demand the erasure or destruction of personal data in the light of the conditions provided for in Article 7[47]. Within the framework of this right, the notification of any operation about any rectification or erasure to third parties to whom personal data have been transferred can be asked from the controller, as well (Article 11(f)).

---

45 **Büllesbach/Gijrath/Poullet/Prins**, p. 73.

46 **Büllesbach/Gijrath/Poullet/Prins**, p. 73.

47 If the grounds on which data processing operations are based no longer appear, the controller shall erase, destruct or anonymize personal data by himself/herself or upon the request of the data subject. This obligation is also valid even if the personal data concerned has been processed in accordance with this Law and other related acts (Article 7/1).

Under Article 11(g), the right to object grants a competence to object to unfavorable decisions about the data subject arising from the analysis of personal data solely by means of automated systems. The main purpose to provide this kind of right is to prevent considerable adverse consequences of automated decisions relating to the data subject, which are taken by using only automated means[48]. This right is also recognized in the EU General Directive, but more comprehensively. According to the General Directive (Article 15), every person has the right to object to a decision (i) *which produces legal effects or significantly affects him/her*; and (ii) *which is solely based on automated processing of data in order to evaluate certain personal aspects of the data subject (such as his/her performance at work, creditworthiness, reliability, conduct etc.).* As obvious, this provision is more concrete about the circumstances in which the data subject is eligible to exercise this right in comparison with the foregoing article in the Turkish Law. Thereby, the implementation of the right to object to automated decisions in Turkish data protection system should be materialized within the framework of the decisions to be held by the Personal Data Protection Board.

In line with the right to compensation, the data subject can also request the data controller to indemnify his/her damages resulting from the controller's unlawful data processing operations (Article 11(ğ)).

According to Article 13, it is necessary for data subjects that their requests about the implementation of this Law be submitted to the controller in written form or through other methods to be determined by the Personal Data Protection Board. Therefore, the rights mentioned above must be primarily asked to be performed from the data controller. The controller shall provide that the requests involved in the data subject's application must be concluded within the shortest time (depending on the nature of the request) and in thirty days at the latest. In this context, the controller has two options to follow: If he/she accepts the application, the request in question should be fulfilled by the controller. On the other hand, the controller should

---

48 Handbook on European Data Protection Law, p. 112; **Büllesbach/Gijrath/Poullet/ Prins**, p. 84.

reject the request by explaining his/her reason and notify his/her response in written or electronically to the data subject.

4. Independent Supervision of the Law

There is no doubt that the proper implementation of the rules is crucial as much as the introduction of modern and functional rules in national data protection law. Hence, it is essential that an independent national data protection authority with an expert knowledge be established to govern and to monitor the application of the respective rules in this field. So, being unprejudiced/independent and having technical expertise, adequate powers and satisfying resources to cope with data protection issues seem indispensable qualifications of effective data protection authorities[49]. The existence of supervisory authorities with complete independence has been indeed emphasized as a precondition for a robust data protection mechanism in the EU General Directive (Recital 65)[50].

Influenced by the EU Directive, a national supervisory authority, which is called *Personal Data Protection Authority (Authority)*, is set up to carry out the tasks entrusted by the Turkish Data Protection Law (Article 19/1). Moreover, *the Personal Data Protection Board (Board)* is also required to be established as a decision making body of the Authority (Article 19/4). During the discussions of this Law in the Turkish Assembly, one of the provisions raising serious concerns and hesitations in the public was the article in which the designation procedure of the Board members was regulated. Because, in its first version submitted to the Assembly in January 2016, four members of the seven-seat Board would be nominated by the Council of Ministers and the rest would be nominated by the President. This nomination method was highly criticized on the ground that a wide margin of appreciation of the executive body in constructing the Board could

---

49 **Büllesbach/Gijrath/Poullet/Prins**, p. 131-132.

50 The same necessity has been also highlighted in several international data protection documents, such as the OECD updated Guidelines (2013), art. 1(d); the Additional Protocol to Convention No. 108 (2001); the Charter of Fundamental Rights of the European Union, art. 8/3. For more information, see Handbook on European Data Protection Law, p. 115-116; **Büllesbach/Gijrath/Poullet/Prins**, p. 131.

possibly endanger independent supervision. In the final version of the Law, this provision has been modified as follows: the Board consists of nine members. Five out of nine Board members are appointed by the Turkish Grand National Assembly, two members by the President and the other two members by the Council of Ministers (Article 21/2). For the time being, it is too early to comment on whether this modification is enough to grant complete independence to the Board. Accordingly, decisions to be held in the forthcoming days by the Board can be seen as a considerable indicator of the level of its independence.

The Personal Data Protection Board is endowed with a group of tasks. According to Article 14, the Board is competent to hear complaints lodged by data subjects. The data subject is enabled to make a complaint to the Board when the request of the data subject submitted to the controller is rejected or not responded in time, or the controller's response is not found sufficient by the data subject. In the light of these possibilities, a complaint shall be lodged by the data subject within thirty days from his/her being informed of the controller's response and (in any case) within sixty days as of the date of his/her application to the controller. It should therefore be reminded that the data subject can invoke the Board following his/her application to the controller. Upon receipt of the complaint, the Board shall inspect the issue to the extent necessary for the performance of its task and notify the conclusion of its research. If any breach is detected at the end of the review, the Board makes an order to get this issue fixed by the controller. However, in the event that the Board does not give any response to the application within sixty days as of the date of complaint, the data subject's claim will be regarded as rejected (Article 15/1, 4, 5).

Furthermore, under the inspection of the Board, a publicly available register shall be kept by the Chairmanship of the Authority. Under Article 16/2, it is an obligation for controllers to enroll in *the Register of Data Controllers (Register*) prior to processing personal data[51]. In order to enroll

[51] On the other hand, the Board will provide for an exemption from the obligation to enroll in the Register having regard to the criteria to be determined by the Board as to the qualification and number of personal data processed, data processing based on a reason required by law, disclosure of personal data to third parties etc.

in the Register, the data controller shall notify a set of information as follows: (a) the identity and address of the controller and his/her representative, if any; (b) the purposes for which personal data are processed; (c) information about the categories of data relating to data subjects; (ç) the recipients or categories of recipients; (d) information about personal data which are anticipated to be transferred abroad; (e) the measures taken to maintain security of personal data; (f) maximum duration necessary for the purpose for which personal data are processed.

In addition to the foregoing functions and powers, the Board is also competent to take steps in respect of temporary measures during its inspection on alleged violations, to specify sufficient conditions under which sensitive personal data shall be processed, to present its opinion on draft legislations consisting of provisions on personal data which are prepared by other institutions, to determine administrative sanctions laid down in this Law[52]. Among these administrative sanctions, the Board's power to impose administrative fines on data controllers failing to comply with the respective obligations referred to in the Law draws attention due to very substantial fine amounts (Article 18/1).

5. Transitional Provisions and Enforcement of the Law

A number of transitional provisions is introduced in the Law (Provisional Article 1). In accordance with these clauses, the members of the Board shall be nominated in conformity with the procedure provided for in Article 21 within six months as of the publication of this Law. Data controllers are liable to enroll in the Register within the period to be determined and announced by the Board. Personal data which were processed before the publication of the Law shall be brought in compliance with this Law within two years as of its publication. However, personal data which are determined to be in contradiction with this Law are required to be erased, destructed or anonymized promptly. The consents that were obtained in a lawful manner prior to the publication of the Law will be considered valid on the condition that an opposite statement is not communicated by the

---

[52] For more information about the functions and powers of the Board, see Article 22.

data subject within one year. Regulations that have been laid down in the Law must be entered into force within one year from the publication of this Law.

As mentioned before, the Data Protection Law was published on 7 April 2016. Under Article 32(b), many articles in this Law shall come into force on the date of publication. Nevertheless, it is provided that some considerable articles (regarding the transfer of personal data to third parties/abroad, the rights of the data subject, application to the controller, complaints lodged with the Board, the procedure of Board's inspection upon the complaint, the Register of Data Controllers, offences and misconducts) shall be effective after six months following the publication.

CONCLUSION

The right to data protection grants data subjects the power to control data processing operations relating to them. This right has been acknowledged as a fundamental right in numerous international documents and state constitutions. Today, it is widely accepted that the right to data protection is absolutely necessary to exercise other fundamental rights and freedoms such as human dignity, the right to privacy, the right to protect and improve one's own material and spiritual being. On the other hand, this right does not have an aim to offer safeguards against all kinds of data processing, but to avoid the operations incompatible with fundamental rules in data protection law.

A growing interest in processing personal data resulting from the increasing developments in information technology gives rise to the necessity of protecting individuals' personal data against intrusions of others. Accordingly, data protection conflicts have been regarded as a serious challenge by many states for a long time. In this regard, there is a real attempt to introduce specific data protection legislations in national laws around the world.

In parallel with worldwide efforts for data protection, the right to data protection is being approved as a fundamental right in the Turkish Constitution since 2010. Even if several data protection provisions were provided for in our national law, there was an urgent need to enact a specific

law to implement the proper functioning of the data protection system. Finally, the long-awaited Turkish Data Protection Law has been adopted and became effective as of its publication on 7 April 2016. When compared to corresponding provisions in the EU General Directive, it can be seen that the Data Protection Law No. 6698 takes the data protection mechanism of the EU General Directive as a guiding example. This Law provides a great deal of stringent rules and responsibilities that data controllers are obliged to align their processing activities with the related provisions. Additionally, it is a crucial requirement that an independent national data protection authority be established to administer data processing activities in compliance with fundamental rights and freedoms.

Enacting of a specific law dedicated to data protection is a substantial step taken to prevent unfair and unlawful processing activities; but of course it is not sufficient. Certainly, the proper implementation of data protection rules laid down in national law and the strict monitoring of supervisory authority are considered as preconditions of exercising the right to data protection adequately and enjoying the powers entrusted to data subjects. Therefore, the strong will to follow data protection rules by both the public and private sectors and authorized bodies becomes decisive in the future of the data protection system in Turkey.

BIBLIOGRAPHY

BOOKS AND ARTICLES

Blume, Peter/**Saarenpää**, Ahti/**Schartum**, Dag Wiese/**Seipel**, Peter: Nordic Data Protection, Iustus Förlag, Uppsala 2001.

Büllesbach, Alfred/**Gijrath**, Serge/**Poullet**, Yves/**Prins**, Corien: Concise European IT Law, Second Edition, Kluwer Law International, United Kingdom 2010.

Bygrave, Lee Andrew: Data Privacy Law: An International Perspective, Oxford University Press, United Kingdom 2014.

Carey, Peter: Data Protection: A Practical Guide to UK and EU Law, Third Edition, Oxford University Press, United States 2009.

Determann, Lothar/**Sprague**, Robert: "Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States", Berkeley Technology Law Journal, Vol.26, 2011, p. 979-1036.

Henderson, Sandra C./**Synder**, Charles A.: "Personal Information Privacy: Implications for MIS Managers", Information & Management, Vol.36, 1999, p. 213-220.

Hornung, Gerrit/**Schnabel**, Christoph: "Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination", Computer Law & Security Review, Vol.25, 2009, p. 84-88.

Klosek, Jacqueline: Data Privacy in the Information Age, Greenwood Publishing, United States 2000.

Krause, Rüdiger: "New Developments in Data Privacy for Employees in German Law", **The Law in the Information and Risk Society**, (Ed. Gunnar Duttge/Sang Won Lee), Universitätsverlag Göttingen, 2011, p. 83-99.

Kuner, Christopher: European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, United Kingdom 2007.

Küzeci, Elif: Kişisel Verilerin Korunması, Turhan Kitabevi, Ankara 2010.

Okur, Zeki: İş Hukuku'nda Elektronik Gözetleme, Legal, İstanbul 2011.

Sevimli, Ahmet: "Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419", Sicil İş Hukuku Dergisi, Vol.24, December 2011, p. 120-139.

Sieber, Ulrich: "The Emergence of Information Law: Object and Characteristics of a New Legal Area", Law, Information and Information Technology, (Ed. Eli Ledermen/Ron Shapira), Kluwer Law International, The Hague, 2001, p. 83-99.

Şimşek, Oğuz: Anayasa Hukukunda Kişisel Verilerin Korunması, Beta, İstanbul 2008.

Yıldırım, Nuriye: "Germany", Employment Privacy Law in the European Union: Human Resources and Sensitive Data, (Ed. Frank Hendrickx), Intersentia Publishers, Belgium 2003, p. 119-131.

Yüksel, Saadet: Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale, Beta, İstanbul 2012.

REPORTS AND OPINIONS

Article 29 Data Protection Working Party: Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN WP 48, 13.09.2001.

Article 29 Data Protection Working Party: Advice paper on special categories of data ("sensitive data"), Ref. Ares (2011) 444105, 20.04.2011.

Article 29 Data Protection Working Party: Opinion 15/2011 on the definition of consent, 01197/11/EN WP187, 13.07.2011.

Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, 02.04.2013.

Council of Europe: Data Protection Compilation of Council of Europe Texts, Strasbourg 2010.

Council of Europe: Handbook on European Data Protection Law, 2014.