yönetim ve ekonomi araştırmaları dergisi
journal of management and economics research

*Cilt/Volume: 17 Sayı/Issue: 4 Aralık/December 2019 ss./pp. 35-58*
O. Güner, A. Günar Doi: http://dx.doi.org/10.11611/yead.553594

# PROTECTION OF PERSONAL DATA IN THE EUROPEAN UNION-TURKEY RELATIONS: EFFECT OF VISA LIBERALISATION DIALOGUE

**Asst. Prof. Oğuz GÜNER** *

**Asst. Prof. Altuğ GÜNAR** *

*"Privacy is not something that I'm merely entitled to, it's an absolute prerequisite."*
*— Marlon Brando*

## ABSTRACT

*The European Union is rather successful at making regulations and law whose influence go beyond the European territory, as these acts are widely considered as common standards. One of them is about personal data protection. The European Union accepted a new regulation on the protection of personal data which was put in practice in May 2018, after a long period of discussions. The regulation was accepted for the replacement of laws about data protection in member and candidate states. As a European Union candidate country, Turkey started a visa liberation dialogue with the European Union in 2013. Personal data protection issue has been one of the most crucial subjects of the visa liberation process and considered as an important requirement which must be fulfilled by Turkey. In this respect, the study will elaborate the European Union's regulation on new personal data protection under the case of Turkey's visa liberalisation dialogue. In the first chapter, the historical development of personal data protection, the European Union data protection regulation and current situation will be analysed. In the second chapter, the study will elaborate the issue of data protection under the case of visa liberation dialogue between Turkey and the European Union. In the last chapter, aiming to reveal the differences between General Data Protection Regulation and Turkish data protection legislation, Turkey's cohesion to the European Union's data protection regulation within the frame of visa liberation dialogue will be dealt. In this context, differentiating from present studies and researches in the literature, this study asserts that visa liberalisation dialogue catalyses Turkey's compliance with the European Union's data protection standards.*

***Keywords:*** *Personal Data Protection, European Union, Turkey, Visa Freedom, Privacy.*

***JEL Codes:*** *K1, Z00, Z38.*

* Amasya Üniversitesi, Yabancı Diller Yüksekokulu, e mail: oguz.guner@amasya.edu.tr
* Bandırma Onyedi Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, e mail: agunar@bandirma.edu.tr

**Makale Geçmişi/Article History**

Başvuru Tarihi / Date of Application : 14 Nisan / April 2019
Düzeltme Tarihi / Revision Date : 21 Ağustos / August 2019
Kabul Tarihi / Acceptance Date : 30 Aralık / December 2019

**Araştırma Makalesi/Research Article**

*Yönetim ve Ekonomi Araştırmaları Dergisi / Journal of Management and Economics Research*
*Cilt/Volume: 17 Sayı/Issue: 4 Aralık/December 2019 ss./pp. 35-58*
O. Güner, A. Günar Doi: http://dx.doi.org/10.11611/yead.553594

# AVRUPA BİRLİĞİ-TÜRKİYE İLİŞKİLERİNDE KİŞİSEL VERİNİN KORUNMASI: VİZE SERBESTİSİ DİYALOĞU ETKİSİ

## ÖZET

*Avrupa Birliği düzenleme ve mevzuat hazırlama ve bu düzenlemelerle tüm dünyaya etki bırakabilme konusunda oldukça başarılı bir aktördür. Avrupa Birliği'nin hazırladığı düzenlemelerden biri de kişisel verilerin korunması üzerinedir. Avrupa Birliği, uzun tartışmalar sonunda Mayıs 2018'te veri koruma düzenlemesini yürürlüğe koymuştur. Bu düzenleme üye ve aday ülkelerdeki veri koruma kanunlarının yerine geçecek şekilde kabul görmüştür. Avrupa Birliği'nin bir aday ülkesi olarak Türkiye 2013 yılında Birlik ile vize serbestisi diyaloğu başlatmıştır. Kişisel veriler ve bu verilerin korunması hususu da vize serbestisi sürecinin önemli konularından biri olarak yer almış, yerine getirilmesi gereken önemli kriterlerden biri olarak dikkat çekmiştir. Bu bağlamda çalışma, Türkiye'nin vize diyaloğu açısından Avrupa Birliği'nin yeni kişisel veri koruma düzenlemesini analiz edecektir. Birinci bölümde kişisel veri korumanın tarihsel gelişimi, Avrupa Birliği'nde kişisel veri düzenlemesi uygulamalarının gelişimi ve mevcut durum değerlendirilecektir. İkinci bölümde çalışma, kişisel veri koruma sürecini Türkiye ve Avrupa Birliği kapsamında başlatılan vize serbestisi diyaloğu kapsamında ele alacaktır. Son bölümde ise, Türkiye ve Avrupa Birliği arasındaki kişisel veri korumaya yönelik farklılıkların ortaya konması amaçlanarak, Avrupa Birliği'nin yeni kabul etmiş olduğu kişisel veri koruma kanuna Türkiye'nin uyumunun vize serbestisi diyaloğu ile nasıl gerçekleştirildiğine dikkat çekilmektedir. Bu bağlamda çalışma literatürde mevcut olan çalışmalarda farklılaşarak, vize diyaloğu sürecinin Türkiye'nin Avrupa Birliği kişisel veri koruma standartlarına uyumu açısından bir katalizör görevi gördüğünü iddia etmektedir.*

***Key Words:*** *Kişisel Veri Koruma, Avrupa Birliği, Türkiye, Vize Serbestisi, Mahremiyet.*

***JEL Codes:*** *K1, Z00, Z38.*

## 1. INTRODUCTION

Throughout the history, the first attempt to regulate the data protection was implemented under the "Convention for the protection of Human Rights and Fundamental Freedoms" in the year of 1953. In 1980, the Organization of Economic Co-operation and Development accepted a guideline called "Protection of Privacy and Transborder Flow of Personal Data". In 1981, Contract No 108 "Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data" was approved by the Council of Europe. Then, "The Privacy and Data Protection Principles" was accepted by the United Nations in 1990. Regarding the European Union (EU), the European Parliament, together with the European Council prepared a directive "on the protection of individuals with regards to the processing of personal data and on the free movement of such data" and put it into force in 1995. Later on, certain legal arrangements were conducted by the EU. Lastly in 2016, the EU prepared a very

ambitious data protection directive called "The EU General Data Protection Regulation". This new regulation on data protection will be enforced in all EU and partner countries by the end of 2018. For the EU, the regulation is substantial for data privacy. Turkey, a candidate country, and visa liberalisation dialogue launched on March 26, 2013 between Turkey and the EU will be affected by this regulation. This regulation has been a trigger for Turkey to adopt personal data protection legislation.

## 2. LITERATURE REVIEW

After the new EU personal data protection regulation entered into force, there has been a broad discussion regarding its influence on the member and associated states. As a candidate, it is also necessary for Turkey to adopt personal data protection law. However, Turkey's status is rather different than other EU member states. Because of the readmission agreement and visa dialogue between Turkey and the EU that began in 2013, it was compulsory for Turkey to meet the requirements of the EU data protection standards.

In the literature of the EU's new personal data protection regulation and Turkey's visa dialogue, Stiglmayer (2012) claims that the EU needs to cooperate with Turkey to control illegal immigration towards Europe, and a visa exemption for Turkish citizens will develop bilateral relations and help Turkey to improve its conditionality for EU membership. Tekin (2014) discusses the new EU data protection directive and current situation in Turkey in the context of the personal data protection and tries to answer the question of "Why Turkey needs to make an independent data protection law?" Başalp (2015) discusses the fundamental changes in the EU's new data protection regulation. One of the main studies in the literature regarding the visa dialogue between the EU and Turkey was made by Nas (2015), which deals with the readmission agreement and visa dialogue, claims that readmission agreement has paved the way for visa dialogue for Turkey and transformed the candidacy negotiation process. Şen and Özkorul (2016) discuss the issue in the context of the refugee crisis which is not controlled by the EU and claim that readmission agreement and visa dialogue are new dimensions of EU's cooperation with Turkey after refugee crisis. Batır (2017) makes a legal analysis of the readmission agreement between Turkey and the EU and examines the agreement from the date entering into force till today. For the visa dialogue, the article concludes that visa dialogue was not accepted by Turkey in exchange for the readmission agreement. Üstübici (2017) took the issue in regards to irregular immigration between the EU and Turkey and claimed that visa dialogue was signed in exchange for the signing of the readmission agreement. This study differentiates in the literature by discussing the issue of the EU's new personal data protection regulation in the context of visa liberalisation dialogue between the EU and Turkey.

## 3. HISTORICAL BACKGROUND OF PERSONAL DATA PROTECTION IN THE INTERNATIONAL SYSTEM

In shortest and simplest definition, personal data contains information with regard to any individual's private, professional and public life. Any information which identifies a person or a piece of information which leads to identify particular person can be regarded as personal data.

Plenty of entries such as name, surname, residence address, phone number, e-mail address, fingerprint, ID number or location data can be counted as personal data and must be liable to personal data protection law. Laws and legal regulations on personal data protection lie behind the notion of 'privacy'. Privacy can be explained as an ethical issue concerning information about individuals and it is necessity of human dignity, condition of individuality and right of people (Hoven, 2008, p.301-318.).

Privacy of individuals has always been regarded crucial as it has a direct connection with personal freedom, individuality and dignity. In this context, data protection notion has stemmed from the individuals' right to protect the information which belongs to them. This protection right was against not also for people and firms but also the state power.

Privacy is a legal notion and worth to be protected in legal systems because it is considered as touching on private life of people. It is like opposition to what is public and claims respect for people's private life. Privacy, in this sense, serves as a realisation of people's individual lives derived from inherent dignity (Fuster, 2014).

In today's modern societies, there has been a considerable rise in the mobility of the individuals all over the world. Large numbers of people move freely among countries and this rising mobility may cause unexpected vulnerability such as free-riding of criminal behaviour, fraud and tax evasion (Hoven, 2008, p.301-318.).

What is mostly discussed is whether data of these individuals should be easily accessible and shared in order to avoid from the vulnerabilities or certain ethical and moral issues should be taken into consideration. In the information age personal data is utilised in many sectors and disciplines such as banking, transportation, social media, advertisement, search engines and insurance with or without the consent of the holder. Thanks to the information and communications technologies, we can generate, store and process huge quantities of data via web sites and networks every single day. This development raised much concern upon protection of personal data.

The Universal Declaration of Human Rights proclaimed by the United Nations in 1948 was a threshold of personal data due to recognition of the inherent dignity and promotion of respect for human rights and fundamental freedoms.[i] Thereafter "The Convention for the Protection of Human Rights and Fundamental Freedoms" which is largely known as "The European Convention on Human Rights" was

opened for signature in 1950 by the members of Council of Europe and it came into force in 1953. The EU has signed the convention as a single entity independently from its member states.

Thanks to the developments in the information and communication technologies after 1960s, countries and international institutions have had awareness on personal data, privacy and protection of it. The Council of Europe initiated "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data with treaty no: 108", opened it for signature by the member states and for accession by non-member states in 1981 and ratified the convention in 1985. This was the first binding international convention constituted against the processing and collection of personal data and outlawed the processing of sensitive data regarding people's race, politics, religion and criminal records. The convention also implements certain restrictions on personal rights and cross-national flow of personal data unless extraordinary circumstances such as national security or public safety are at stake (Europe, 1985).

This convention applies to all data processed by private sector or public services such as judiciary or enforcement of law. Convention 108 protects people against personal data abuses such as unauthorized collection and processing and makes regulations on trans-border flow of data. Additionally, it outlaws the processing of sensitive data such as individuals' race, political thought, religion, sexual life (Council of Europe & European Union Agency for Fundamental Rights, 2014).

There are certain special categories classified under personal data under the EU law and Council of Europe law. These are sensitive data, anonymised data and pseudonymised data. According to "Data Protection Directive of the European Union[ii]" and "Convention 108 of the Council of the Europe[iii]", sensitive personal data includes individuals' ethnic or racial origin, political opinion, religion or other beliefs, health or sexual life. These data cannot be saved, stored, processed or changed. Also, data protection directive of the EU includes membership of trade union as sensitive data since it can give clue about a person's affiliation or political thought. "Convention 108 of the Council of Europe" regards personal data of individuals' criminal convictions as sensitive. (Council of Europe & European Union Agency for Fundamental Rights, 2014)

When the identifying elements are eliminated, the data remained is anonymised data. This kind of personal data is served for a certain purpose and then used for scientific and statistical purposes anonymously. According to the Convention 108, data anonymised successfully is no longer personal data.

Pseudonymous data is a type of the information needs additional data in order to be able to correlate with the owner of the data. There are certain identifiers such as name, birthday, sex, etc. in the personal data. When these identifiers are replaced by a pseudonym, the personal data is pseudonymised. "Pseudonymised data are not explicitly mentioned in the legal definitions of either Convention 108 or

the Data Protection Directive. However, the Explanatory Report to Convention 108 states in its Article 42" (Council of Europe & European Union Agency for Fundamental Rights, 2014).

## 4. THE EUROPEAN UNION AND PERSONAL DATA PROTECTION

The EU which has 7400 km of external land borders and 57,800 km of external maritime borders with its 28 member states has fewer borders than ever (Bossong, Carrapico, 2016, p.72). This less bordered unification and integrated and more globalised approach in Europe have brought some serious concerns which will be evolving to challenges and hazards in terms of data protection for the EU. Also, thanks to the developments in the information and communication technologies since the mid-1990s, various concerns regarding personal data protection have raised within the EU. Hence, The EU has inevitably prioritized and given importance to personal data and its cross-national protection and commenced to take an action against these challenges and develop comprehensive regulations. Personal data in the EU is substantially exercised in various areas such as fundamental rights and freedoms, neighbourhood policy, corporate law, international law, freedom of movement, organized crimes, terror and border controls.

It is very well-known that security of the EU requires a combination of varied instruments and reciprocal interdependence of external and internal security of the EU is considerably increasing (Słomczynska & Frankowski, 2016). Right along with providing internal and external security, The EU has strived to respect for individual rights and developed directives and regulations accordingly. Constitutively, the EU has always stuck up for the rights of individuals on personal data protection under Article 8 of 'Charter of Fundamental Rights' and continuously debated on how to develop the security and privacy of personal data both in the EU and around the world.

All the EU member states ratified Convention 108 of Council of Europe and Convention 108 was amended to let the EU take part in 1999. Apart from "European Convention on Human Rights and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", the EU has some legal rules and regulations regarding the protection of personal data. Protection of personal data is deeply esteemed peremptory fundamental right (jus cogens) and no derogation against is permitted in Europe.

When we consider the decisions, policies and practises regarding the personal data in the EU, we can inarguably infer that the EU considers data privacy not merely an interest, or a right, but a fundamental right (Bergkamp, 2002). In 1995, the first institutional step was taken by the EU and The European Data Protection Directive with 95/46/EC directive number about protection of processing and movement of data of the individuals was adopted. This regulation entitles the European Commission to review the member states whether they apply protection of personal data sufficiently.[iv]

This directive relies on the idea that free movement of goods, persons and services will not be effectively applicable in the EU internal market unless maximum-level data protection is provided. In addition to the 'Protection of Individuals with regard to Automatic Processing of Personal Data' by the Council of Europe, the European Commission stipulates the foundation of independent auditing organs in the EU countries (İktisadi Kalkınma Vakfı, 2015).

Regulation on the protection of individuals with regard to the processing of personal data by the Community was opened for signature by the EU states in December 2000 and entered into force in 2001. Having regard to Article 286 in the Treaty on the Functioning of the EU, this regulation required the establishment of an independent supervisory body responsible for applications of individuals about the protection of their rights on behalf of the EU.[v]

With this regulation, The European Data Protection Supervisor (EDPS), the independent data protection authority of the EU which is responsible of monitoring and ensuring the protection and privacy of personal data was set up. EDPS ensures the protection of personal data, advises and cooperates with the EU institutions and national authorities about data protection and works with the EU legislator in policy design and legislation process (European Data Protection Supervisor).

In order to increase the security of data in Europe, the EU introduced the directive numbered 2002/58/EC upon the processing and protection of personal data and privacy in the sector of electronics and communications. Because of the advancements in the digital technologies and telecommunications sectors and publicly availability of data in electronic platforms, protection and privacy of the personal data could barely be provided. In order to ensure privacy, minimise the processing of personal data, "the directive 2002/58/EC" was introduced.[vi]

The regulation sets up a central database system collecting fingerprints of asylum seekers and the third country nationals crossing the border illegally. With the establishment of 'Eurodac', "it is aimed to compare fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice" (Official Journal of the European Union, 2013).

Eurodac allows the EU states to determine responsibility for examining asylum seekers' applications. The reason why the EU has needed to initiate this system is that the EU was not efficient and successful enough to collect information about asylum seekers or people who cross the EU borders illegally. In virtue of this regulation, fingerprints of applicants are transmitted to the Eurodac central system when they apply for asylum. Also, this central system is used to find out if the individual has

applied for asylum in any other member state before or not. Fingerprints inserted in the Eurodac system have unique and universal biometric characteristics. Biometric characteristics can be processed and understood by officials and computers in the same way anywhere in the world and searched and determined among the databases of thousands of inputs easily (Roots, 2015).

This regulation (No: 1052/2013) establishes "the European Border Surveillance System (Eurosur) in order to apply to the surveillance of external land and sea borders, including the monitoring, detection, identification, tracking, prevention and interception of unauthorised border crossings for the purpose of detecting, preventing and combating illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants" (Official Journal of the European Union, 2013). Eurosur enables the Member States to exchange information rapidly and ensure necessary cooperation and joint response. Frontex[vii] coordinates the surveillance tools and Member States can request Frontex' assistance using the tools like satellite imagery or ship reporting systems (Commission, 2018).

Establishment of Eurosur clearly indicates that there is a deviation from existing practices of the term, The European Commission has prepared a regulation proposal concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) and it entered into force on May 25, 2018 as well.

The EU has Digital Single Market Strategy (DSM Strategy)[viii] which aims to increase trust in the EU citizens and tighten the security of digital services. The DSM Strategy had already announced the revision of Directive of 2002/58/EC (ePrivacy Directive) to be able to provide more privacy and protection for the users of electronic communication services. The European Data Protection Board which was established under the Regulation (EU) 2016/679 will have competency to ensure the consistency of this regulation. The Commission plans to make an evaluation regarding the functioning of the regulation and present the outcomes to the European Parliament, the European Council and the European Economic and Social Committee three years after the application date of the regulation. After the evaluation, where appropriate, there might be certain amendment or repeal on the regulation if there are any legal, technical or economic developments (European Commission, 2017).

This regulation restricts electronic network and service providers and makes electronic communications' data privacy mandatory. Therefore, bugging of the data, listening the communications on the phone, recording, observing, scanning and obtaining the electronic communication data is strictly forbidden. This regulation inhibits junk mails, SMS, automatic calls and marketing companies will have to use a defined private dialling code for their services (European Commission, 2017).

"Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties and on the free movement of such data" came into force in May 2018. According to the directive; protection of natural persons'

personal data is a fundamental right. Everybody is entitled to protect the personal data concerning them. Whatever their nationality or residence is, everybody deserves to be respected regarding their fundamental rights and freedoms, especially their rights as to the protection of personal data. In this context, this directive aims to contribute to the accomplishment of an area of freedom, security and justice (European Commission, 2016a). The directive contains certain provisions aiming to develop protection of natural persons' rights against possible technological threats and improves the Directive 95/46/EC.

### 4.1. Background of The European Union's Personal Data Protection Regulation

While the current global challenges such as financial crisis, rise of populism, refugee crisis and global terrorism drive most of the EU's debates, the EU keeps maintaining its directive, constructive and transformative role and deals with other subjects.

The world has been passing through a digitalization process and the EU has been swiftly affected by this transformation. The EU believes and supports digitalisation of its functions and empowers its digital market by investing and flourishing. And the EU's single digital market agenda is expected to contribute €415 billion per year to the EU's economy and provide thousands of new jobs (Digital Single Market, 2017). When requirements of the digital world are considered, it is clearly understandable that Data Protection Directive enforced in 1995 is not sufficient and satisfactory to meet these requirements. Furthermore, the directive was open to dissimilar interpretations of the member states, and revision and reformation in personal data (definitions and features) were inevitable. In this regard, the EU has attached too much importance on privacy revealed the draft of General Data Protection Regulation in 2012. The draft was ratified by members of European Parliament in 2016 and promulgated in Official Journal of the EU.

The main logic of the regulation is that all the components which constitute the EU and all the third countries having relationship with the EU -especially those with visa exemption agreements- must have advanced level and adequate standards of data protection in order to be able to share the data mutually. In this respect, along with the member countries, the countries which have economic, political and social ties with the EU must keep pace with it and take actions accordingly. Digital transformation is at an unprecedented pace in the world and border controlling is getting much harder in the EU. In this context, the EU has taken steps such as border controlling of the data protection ecosystem, developing collaboration with non-EU states, standardisation of EUROSUR and EURODAC frames, making relevant PNR[ix] arrangements so as for sharing flight information and reforming visa operations over EU Travel Information and Authorisation System[x] (Eurobarometer, 2015).

### 4.2. The EU General Data Protection Regulation (GDPR)

After prolonged discussions and preparations, General Data Protection Regulation of the EU was approved by the EU Parliament in April, 2016, enforced on May 25, 2018.

GDPR (Regulation EU 2016/679) replaces The European Data Protection Directive (95/46/EC) which cannot meet the requirements of information age, enlarge the protection area of data and empower the EU citizens' in terms of data privacy. The regulation is going to be enforced with a powerful jurisdiction and will be applied to processing of personal data by controllers and processors in the EU, although it doesn't take place in the EU. Non-EU countries which process the data of the EU citizens will have to assign a representative in the EU. The companies which earnestly breach the regulation can be penalized with up to 4% of the amount of money they generate. This is the maximum fine amount and applied when the companies process data without consent of their customers. The companies not having records, not notifying the supervising authority and not conducting impact assessment can be penalized with up to 2%. The regulation is going to be implemented both for controllers and processors, so there will be no exemption for clouds in new data protection regulation. The companies will not be able to use long and illegible terms and conditions. Consent forms will be easily understandable and accessible with the attachment indicating what the data processing is. Language of consent forms will be clear, simple and plain and customers will be allowed to withdraw anytime they desire. Also, all member states are obliged to notify the data processor within 72 hours upon detecting the breach of data which may have risks for human rights and individual freedoms. Right after the notification, data processors will be required to inform their customers without delay.[xi]

With the regulation, individuals will be entitled to obtain the data controller confirmation if their personal data about them is being processed with a purpose anywhere or not. Also, the controllers must provide a copy of the personal data in a cost-free electronic format.[xii]

There is a right to be forgotten in the regulation also known as the right to erasure. Individuals are entitled to have data controller erase the personal data, end further dissemination of the data and stop the third parties to process the data. This includes the data which is no longer relevant to the purpose, or a data subjects withdrawing consent. Additionally, with the regulation, data portability right which lets individuals receive personal data about them or transmit data to another controller is introduced.[xiii]

GDPR brings an internal record keeping requirements in place of the current system in which controllers are required to notify their data processing activities. In the internal record keeping requirements, appointment of data protection officers' will be compulsory for those who regularly and systematically monitor data subjects on large scales or special categories. In this context, data protection officers;

- must possess professional qualities and expertise in data protection law and practises,
- can be a staff member or an external service provider,

- contact details must be shared with relevant data protection officers,
- must have relevant, sufficient resources to be able to conduct their duties and continue their expert knowledge,
- must report to the highest rank of the management,
- must avoid from other tasks which may result in an interest conflict.[xiv]

Thus, one can legitimately infer that the EU is very motivated and determined to protect personal data and develop a sustainable mechanism depending on the privacy of personal data.

## 5. PERSONAL DATA PROTECTION IN TURKEY: HISTORICAL BACKGROUND

Turkey which began EU accession process in 2005 is different from other EU countries in the area of personal data protection. Its story and historical developments on personal data protection began in 1981 with the signature of the Council of Europe Convention No: 108. There were only 41 Council member states which signed the Convention by 2010 and all the member of Council of Europe ratified the Convention by 2016. Turkey signed the Convention No: 108 and ratified the protocol in May 2016. The reason of Turkey's disapproval was the article 4 of the Convention (İktisadi Kalkınma Vakfı, 2015, p.20). But, during the process of visa liberalization, the Convention entered into force in Turkey in September, 2016. According to the article 4 of the Convention 108, each contracting party has to take necessary precaution in her domestic law to implement Convention principles. In addition to that, those measures have to be taken on the date when the protocol is entered into force for contracting parties (Council of Europe, 1981). Therefore, it was very difficult to ratify or implement the Convention No:108 for Turkey, because of Turkey's lack of legal basis and regulations for personal data protection (Atak, 2010, p.94). But, Turkey's motivation for visa liberalization and the EU's conditions make the enforcement of these regulations possible.

Developments aimed at protection of personal data in Turkey accelerated after 2010 by the constitutional amendment package. The purpose of the amendment was the internalization of the EU 95/46/EC directive, but Turkey didn't possess the necessary institutional capacity then. After the internalization, the amendment replaced the old sentence "concerned personal data are protected" with the new one "right to demand protection of personal data" (Özsöz, Bozcağa, 2010, p.2).

In the process of visa liberalisation dialogue between Turkey and the EU, Turkey had crucial responsibilities. According to the European Commission evaluation report for visa liberalisation, The Commission underlined the approval of Council of Europe Convention 108 and pointed out that it was mandatory to have a law on personal data protection in harmony with the EU personal data protection directive. By this aim, it was underlined by the European Commission that Turkey had to harmonise its domestic law with EU's 95/46/EC directive on personal data protection, then Turkey has to establish an independent and neutral institution to regulate personal data. Also, in the light of the Turkey's second

action plan on the issue of accession to the EU, it had to ratify "the Council of Europe Convention 108" and its "Additional Protocol No: 181" by the mid-2016 (İktisadi Kalkınma Vakfı, 2015, p.21).

Turkey, determined to keep visa-free dialogue with the EU and get visa exemption for its citizens, ratified the Convention 108, enforced the data protection law and established a neutral, independent institution for data protection services. The establishment of neutral institution named as 'Personal Data Protection Authority'[xv] (PDPA) was accepted in Grand National Assembly of Turkey in March 2016 and Law No. 6698 on the Protection of Personal Data was published in the Official Gazette in April, 2016 (numbered 29677). The Board of PDPA has 9 members at present. According to the provisions of the relevant law, 3 candidates for Board of PDPA were elected by Grand National Assembly of Turkey in October 2013. 2 candidates were selected by Council of Ministers with decision no 2016/9597 in October 2016. 2 candidates were selected by President of Turkey in December 2016 and 2 candidates were elected by Grand National Assembly of Turkey on January 4th, 2017 in the 50th session. According to the 21st article of the Personal Data Protection Law (6698), the members of the Personal Data Protection Board swore in the Court of Cassation on January 12th, 2017 (Kişisel Verileri Koruma Kurumu, 2019).

The importance of the personal data protection revealed itself in the process of visa liberalization and Turkey the EU accession negotiation. First of all, Chapter 23th of the EU-Turkey negotiation process determined the framework of the fundamental rights of the freedoms and it was mandatory to fulfil the necessary reforms in the area of personal data protection for Turkey. Secondly, as a part of the 24th chapter of negotiation process which is called Justice, Freedom and Security, it was vital to ratify and accept the law on personal data protection. Moreover, due to not to have a legal regulation to manage personal data in Turkey, it was impossible to make cooperation between Turkey and the EU related institution including European Police Office (Europol) and EU Judicial Cooperation Unit (Eurojust). Thirdly, economic cooperation between Turkey and the EU is the most important aspect of having an EU level personal data protection law. Recently, international trade became digitalised and moved to the digital platforms. Also, with the rising trade value of the personal data, the personal information turned out to be a rising star of the globalised trade relations. For this reason, it was crucial to have a personal data protection regulation for Turkey, to make or establish efficient trade relations with EU centred companies and EU based capital. Last but not least, having personal data protection law or regulation was a prerequisite for Turkey's visa liberalisation dialogue with the EU. In the visa liberalisation roadmap, Turkey was invited to make necessary obligations by European Commission including ratification of Council of Europe Convention no: 108. (İktisadi Kalkınma Vakfı, 2015, p.24-25). Therefore, Turkey had to legislate an EU level personal data protection law for visa-free Europe and took actions accordingly.

### 5.1. Visa Liberalisation Dialogue between Turkey and the EU

Visa liberalisation dialogue between Turkey and the EU had launched with the signature of the readmission agreement in December 16th, 2013 (Ministry of Foreign Affairs of Turkey, 2013). With the visa liberalisation process, Turkey wants to be a part of countries with visa exemption. Turkey is the only state citizens of which are obliged to apply for visa to travel across the Europe. In the past, the EU has initiated a visa liberalisation process with Ukraine, Moldova and some Balkan countries. However, EU has never offered a visa liberalisation to Turkey which mutual relations of have almost continued for sixty years. Furthermore, the EU is especially eager to remove the visa restriction in exchange of some reforms in domestic law in the area of protection of external borders (Stiglmayer, p.99). In fact, visa liberalisation dialogue is the outcome of the readmission agreement in which Turkey was charged of controlling illegal immigration in the case of transit country (Bürgin, 2013, p.1). In other words, Turkey had launched visa liberalisation in exchange of readmission agreement.

After visa liberalisation dialogue had launched, the European Commission issued a roadmap to answer and guide for Turkey to obtain visa free entry to Europe. In the roadmap of visa liberalisation dialogue prepared by the European Commission underlined the legislative and administrative reforms for Turkey to create secure and safe visa free travel. Roadmap for visa free travel consists of four pillars including; security of documents, migration and management of border, public order and fundamental rights. The first pillar of the visa liberalisation dialogue is "Document Security". Turkey is obliged to fulfil some requirements; Using biometric documents in harmony with International Civil Aviation Organization (ICAO), Using biometric data consist of finger prints, photo and in accordance with Council Regulation 2252/2004, ensuring distribution and verification methods for international passports, preventing corruption on the issue of visa policy and adopt ethic rules for corruption, cooperation with International Police Organizations (Interpol) and related institutions for missing passports, providing heightened security measures for identification cards and strong controls for their use and application, cooperation with the EU on the document security in the area of visa-policy, ensuring the security and integrity of fundamental personal data (European Commission, 2013).

In the second pillar of the visa free Europe, roadmap is related with the migration management. In migration management pillar, Turkey is responsible to protect its external borders and borders along with EU member states to prevent illegal entering. Taking necessary precautions in compatible with "National Action Plan" for the implementation of Turkey's "Integrated Border Management Strategy" the laws approved on March 27th, 2006, EU Schengen Border Code, EU Schengen Catalogue for efficient control of the movement of person on exterior borders were implemented ensuring the good governing of the outer border and EU member states frontiers. With this purpose, Turkey has to financially and administratively support external borders including sufficient guards, technological infrastructure and equipment. Cooperation with related institutions and bodies associated with border security and management, training border officials and adopting anti-corruption regulations to stop illegal initiatives, sharing possible risks, making cooperation and exchanging data with the "European

Border and Coast Guard Agency" (Frontex), tracing international law regulations -especially refugee law, principles and asylum procedures-, cooperation with neighbouring EU member states on border management are crucial for the progress of visa liberalization (European Commission, 2013).

Visa policy is the subtitle of the migration management pillar and Turkey is expected to fulfil necessary measures. In visa policy area, Turkey is obliged to enhance its own visa information system and provide document security, cancelling the issuance of visas on the borders, using new visa stickers for higher security, issuing transit visas in airport, tightening the rules and regulations for people who are entering to Turkey's territory with illegal ways and preventing illegal cross borders to EU countries, harmonize the Turkish visa policy with EU acquis as much as possible (European Commission, 2013).

Another subtitle of the migration management is the international protection. In the area of International protection, Turkey have to take some responsibilities including; harmonization with EU acquis and 1951 Geneva Convention on refugees and 1967 Protocol, provide a healthy institution to determine refugee status (European Commission, 2013).

Third pillar of the visa free Europe is the public order and security. In this area, main aim is to fight against organised crime and to struggle with terrorism and corruption. By this aim, roadmap underlines; following National Action Plan and Turkey's National Strategy, ratification of Council of Europe Convention on Action Against Human Trafficking and Convention on Laundering, Search, Seizure, confiscation of the proceeds from crime and of the financing of terrorism and Convention on cybercrime. In the subtitle of the third pillar of judicial cooperation; it is expected to comply with international agreement and Conventions in the area of judicial cooperation. In addition to that, importance of the cooperation with "Eurojust", "European Anti-Fraud Office" (OLAF) and "Europol" was emphasized. Most importantly, the third pillar of visa liberalisation dialogue consists of data protection obligations. In the data protection subtitle, Turkey was in charge of ratification, signature and implementation of "Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 and additional Protocol no: 181". (European Commission, 2013). In parallel with these responsibilities, Turkey ratified the Convention and Protocol in July 2016 and make it enter into force in November 2016.

The last pillar of the visa free Europe is the fundamental rights. Also, in the area of fundamental rights Turkey has to ensure information about changing personal data. It can be seen that the visa liberalisation dialogue is consist of broad reforms in Turkey's domestic law. Besides, European Commission has monitored the reformation process with regular reports. After dialogue launched between the EU and Turkey, the European Commission published its first report on October 20th, 2014.

### 5.2. Visa Liberalisation Dialogue and Personal Data Protection

After visa liberalisation dialogue had been launched between the EU and Turkey, the European Commission released its first report in October 20th, 2014. While Turkey's performance was praised in some areas, the European Commission underlined that certain reforms were necessary including document security, migration management, border management, fundamental rights and data protection. Data protection merits particular attention, the European Commission expects Turkey to improve its relationship with Europol and Eurojust. Regarding personal data protection, Turkey had succeeded in amending and changing status of personal data, but it is emphasized that Turkey had to take necessary measures such as adopting a legislation, setting up an independent institution and ratification of Convention on personal data protection (European Commission, 2014).

On November 29th, 2015, the EU and Turkey met on the level of head of states or governments to discuss visa liberalisation dialogue and decided to speed up visa free Europe by 2016 (Europa NU, 2016). As a conclusion, the EU and Turkey agreed to revive the EU-Turkey accession process, adopt a joint action plan for refugee crisis and lifting visa measures for Turkey by October 2016. On March 4th, 2016, a second report on Turkey's visa liberalisation dialogue was issued by European Commission. In the second progress report, Turkey's efforts had been criticised by the EU and depicted as limited, compared to report of 2015. Regarding personal data protection, Turkey's efforts were found less advance in 2016. Not to adopt legislation and set up an independent institution and not to ratify Council of Europe 1981 Convention and its additional protocol 181, it was emphasised that Turkey had to fulfil its obligations (European Commission, 2016b; European Council, 2018).

After Turkey and the EU met on March 18th, 2016, the third report was issued for visa liberalisation dialogue by European Commission. Turkey's effort had been evaluated as well advance, while in 7 requirements out of 72, objectives had not been completed by Turkey. In the area of personal data protection, Turkey was urged to amend new legislation in the light of the EU acquis and cooperate with Europol and to set up an independent authority in EU level (European Commission, 2016c).

After 3 years of handworks and cooperation between the EU and Turkey, the European Commission suggested lifting visa requirements for Turkey in the light of the visa liberalisation dialogue. However, Turkey needs to work further in some areas. In the visa liberalisation roadmap, Turkey was obliged to fulfil all 72 requirements for visa free Europe. According to the last document, 5 requirements out of 72 needed further work. In the document security and migration management pillar, Turkey succeeded top meet all criteria. Besides, in public order and security area, Turkey still needed to follow National Action Plan and GRECO policy recommendations in the area of corruption. Additionally, Turkey has to prove its effective demand on the matter of judicial cooperation with the EU member states' relevant authorities. Also, it is mandatory to make cooperation with Europol. In the fundamental rights pillar, Turkey is still expected to revise its terrorism legislation in parallel with the

EU and other legal frameworks including European Court of Human Rights and EU member states (European Commission, 2016d).

### 5.3. Personal Data Protection Law (No:6698) and Current Situation in Turkey

After Turkey had made significant reforms on visa liberalisation dialogue, Personal Data Protection Law (No:6698) came into force on March 7th, 2016. It is aimed to provide privacy and protection of personal data and fundamental rights of persons. Adopting a new legislation, Turkey has had an opportunity to cooperate with international institutions and ability to process personal data which was the basic input for various sectors such as finance, banking and etc. Also, with the law, Turkey set up an independent data protection authority, while it was fulfilling vital criteria by adopting legal infrastructures (T.C Kalkınma Bakanlığı, 2017, p.26). It can also be said that visa liberalisation dialogue had an impetus effect on Turkey to adopt a globalised personal data protection act. And in this context, motivation of Turkey regarding the data protection strengthened.

The content of the law shows that the legislation can be operative and applicable for reel and legal person. Also, article 12 of the legislation makes data officers compulsory for the protection of personal data (Mevzuat.gov.tr, 2016, p.12301-12305).

#### *5.3.1. Basic Principles and Concepts of 6698 Turkish Personal Data Protection Legislation*

According to the OECD (Organization of Economic Cooperation and Development), protection of personal data became more important with the globalization and development of information technologies and internet. Especially, internet has transformed the whole information infrastructure with its speed (OECD, 2002, p.7), and rise in the use of internet and variations in the technological developments increased day by day. This situation makes the issue of personal data more important and it brings some effects with it (Küzeci, p.143). In this respect, not only protection of personal data but also methods of processing the data are very important. The Turkish Legislation no: 6698 on Personal Data Protection answers this question with article 4. In article 4, it is underlined that personal data can only be processed properly as shown in this legislation and other related acts. By this aim, article 4 lists the main basic principles of how to process personal data (Mevzuat.gov.tr, 2016, p.12302).

- "Lawfulness and conforming with rules,
- Being up to date and being accurate,
- Being processed for specific and legitimate purposes,
- Being proportional and limited to the purposes for which they are processed,
- Being retained for the period of time stipulated by relevant legislation or the purpose for which they are processed" (KVKK, 2019).

Under the no: 6698 legislation personal data protection legislation, there are basic concepts including personal data, processing of personal data, data record system, data officer, data processor, open consent, becoming anonymous. For legislation no: 6698 personal data can be explained as every kind of information which belongs to a reel or determinable person. In this respect legislation no: 6698 gives the definition of personal data in article 3 (d). From this explanation, it can be said that personal data includes name, surname, identity records, addresses, physical features of person, economic and social status, phone number, motor vehicle license, social security number, passport number, curriculum vitae information, photo, image, voice records, finger prints and genetic information. Another key concept of no: 6698 legislation is the processing of personal data. Under the legislation, processing of personal data regulated in article 3 (e). Processing of personal data includes every kind of transaction from creation of personal data to every kind of processing transaction on data. From this perspective, article 3 (e) can be interpreted very broad in nature (T.C Kalkınma Bakanlığı, 2017, p, 27).

Third key concept of the legislation is the data record system. With the data record system, it refers to the storage for data processing. This system can be created physically or electronically. Data officer is another key concept of the 6698 legislation. Article 3 (i) regulates the data officer as a person who is in charge of determining the purpose of processing of data and who is charge of creation of data record system and regulation of this system. Data officer can be real person or legal person. Data processor is the fifth concept of the legislation 6698. For the legislation, data processor can be accepted as a person who is processing data by the name and authority of data officer. In this respect, data processor can be reel or legal person under the control of the data officer. Another key concept is the open consent. With the term open consent, giving information regarding the processing of personal data is referred. In other words, open consent means the statement of a person who accepts the conditions and gives consent for the processing of personal data. Finally, becoming anonymous is other key concept of no: 6698 personal data protection legislation. The related key concepts are regulated under article 3(b) of this regulation. Shortly, being anonymous is referred to separate data related determinable person. By this way, it is impossible to determine the identification of the data which belongs to. Consequently, data which became anonymous cannot be accounted for personal data (T.C Kalkınma Bakanlığı, 2017, p. 28).

### *5.3.2. Importance of Personal Data and Its Institutional Aspects in the Direction of Visa Free Europe*

Relationship between Turkey and the EU has almost continued for more than 50 years. After Ankara Agreement was signed, the customs union was established and Turkey gained candidacy status of the EU in 1997. The accession negotiations began in 2005. However, Turkey did not obtain free movement of the persons which is the most important aspect of the relationship. Therefore, visa liberalisation can be accounted for a milestone in the context of Turkey – the EU relationship.

Free movement of persons is a fundamental right for United Nations Universal Declaration of Human Rights in article 13. According to the European Convention on Human Rights Protocol 4, free movement of persons had been recognised in principle (United Nations, 1948). Moreover, European Union Fundamental Rights underlined the importance of the factor of mobility including free movement of persons, free movement of goods, services and capital (European Union, 2000, p,8; İktisadi Kalkınma Vakfı, 2015, p. 54).

The main condition of visa free Europe is the strong and reliable infrastructure and Turkey's approach on security issues. In the visa liberalisation roadmap, there were 10 related areas out of 72 requirements. Therefore, it is vital to have an EU level personal protection legislation for Turkey to succeed visa liberalisation.

The visa liberalisation roadmap requires Turkish authorities to issue biometric passports. In addition to that, Turkey has to set up an effective border security management which can co-operate all related institutions of the EU and member states. By this aim, it is necessary to reach all personal data easily and transfer all data between related units reciprocally. Also, the issue of personal data protection is considered to develop institutional aspects. Turkey has to develop an effective cooperation with Europol and Eurojust. The most important point of this cooperation is an instantaneously data sharing in judicial and criminal matters (İktisadi Kalkınma Vakfı, 2015, p.55-57).

After Turkey adopted personal data protection legislation no: 6698, it is mandatory to fulfil remaining reforms in the line of the EU acquis. Judicial Cooperation and domestic security are the most important aspects of the Schengen System. The EU leads to the world in norms and standards. Therefore, it is not wrong to say that the EU is a shaper of international standards including personal data protection. That is why Turkey has to complete its responsibilities and duties. In this line, the National Jurisdiction Network Project (UYAP) had been praised, but further endeavours are needed for Turkey (İktisadi Kalkınma Vakfı, 2015, p.59).

## 6. DIFFERENCES BETWEEN TURKEY'S PERSONAL DATA PROTECTION LEGISLATION AND EU'S GDPR

In the new EU personal data protection regulation which entered into force on May 25th, 2018, it can be observed that it solves the principal problems that couldn't met by the old EU directive on personal data protection. The EU aimed to take competitive advantage in international arena and wanted to set up a data market with the new GDPR. When the GDPR was compared to Turkey's 6698 legislation, the first thing which needs to be emphasized is the differentiated approach to the data processor responsibility. In the GDPR, the responsibility of every kind of data processing action is charged to all sides in any illegal situation including data officers and third parties in non-EU member states. Therefore, GDPR foresees high penalties. However, in Turkey's legislation, there is a strict separation for data officer and data processor. According to this approach, in any illegal situation, data

officer is the person who has main responsibility. In this respect, it can be inferred that legislation of Turkey has a different approach in the frame of the responsibility of data officers compared to GDPR of the EU (T.C Kalkınma Bakanlığı, 2017, p.33).

Secondly, other distinction reveals itself in 'the right to be forgotten' between the legislation 6698 and EU GDPR. The right to be forgotten is firstly retrieved as a legal status in the GDPR. In this respect, the right to be forgotten means that a person may demand to delete his/her personal data at any time and data officer is responsible to delete the data immediately. Additionally, there are some limitations to use the right to be forgotten. These exemptions include using right of information and expression of freedom, public interest and other mandatory issues related to public health, archive research for scientific and historical purposes. However, legislation 6698 does not have any similar right or any measure. But, it can be seen that Turkey's Supreme Court and Constitutional Court referred the right to be forgotten with their decision. Turkish Supreme Court had made a decision of compensation and breach of personal rights with its 2013/6256 decision in a demand to delete archive. Also, Turkish Constitutional Court had firstly underlined the term right to be forgotten with its B.2013/5653 decision. Turkish Constitutional Court was applied by a person demanding to make his/her personal data to be deleted on the internet. Thirdly, when the GDPR and 6698 personal data protection legislation are compared, there seems discrepancies on the sanctions. GDPR has clearly much stronger sanctions than 6698 legislation (T.C Kalkınma Bakanlığı, 2017, p. 35; Çelik, 2017, p. 403).

Mobility of data and impact assessment are other distinctions between GDPR and 6698 Turkish legislation. Basically, a person can demand to move his/her personal data from a data officer to another. But, 6698 legislation do not include similar measures. Lastly, other distinction between GDPR and 6698 legislation can be observed in the area of data protection approach. In the EU GDPR, it is clearly seen that approach to protection of data is different. By including "data protection by default and data protection by design", GDPR sets more comprehensive approach forth than 6698 legislation. However, Turkish legislation 6698 does not have any direct regulation (T.C Kalkınma Bakanlığı, 2017, p. 36).

## 7. CONCLUSION

With the General Data Protection Regulation, the EU, one of the most influential lawmakers in the world defined and designed international personal data protection standards affecting the candidate countries as well. The Union's GDPR came into prominence with its well-advanced framework differentiated from other legal norms and rules in terms of responsibility of data processors, right to be forgotten and its sanctions, mobility of data, impact assessment and data protection measures.

The aim of this study was to reveal the willpower of Turkey in terms of meeting the EU's requirements in data protection and privacy within the frame of visa liberalisation dialogue between the EU and Turkey launched in 2013. Apparently, necessary regulations related to data protection were fulfilled and actions were accordingly taken by Turkish government. The country adopted legislation

6698 regarding to Personal Data Protection and established an institutional body under the name of 'Personal Data Protection Authority' in March 2016. Interestingly, Turkey, which was the only country which didn't ratify among the Council of Europe countries, ratified the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' in May, 2016 and the law entered into force in September 2016 in Turkey.

Regulations and legal actions regarding data protection in Turkey has been slow for a long time. However, visa-free travel for Turkish citizens has been the objective of Ankara. Thanks to the visa dialogue with the EU after 2013, Turkey prepared and adopted personal data protection legislation.

One can legitimately argue that the visa liberalisation dialogue has propelled Turkey's efforts to meet the challenges of the digital age. No other recommendation or requirement by the EU could affect Turkey's willpower to legislate on personal data protection as the visa liberalisation dialogue. From now on, Turkey is expected to fulfil the rest of the requirements demanded by the EU. Upon fulfilling and achieving all the requirements and standards, Turkish citizens will be entitled to travel in Schengen zone with no visa requirement.

## REFERENCES

Akıncı, A., N. (2017) "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi", İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü T.C Kalkınma Bakanlığı.

Atak, S. (2010) "Avrupa Konseyi'nin Kişisel Verileri Açısından Sağladığı Temel Güvenceler", Türkiye Barolar Birliği Dergisi, 87: 90-120.

Başalp, N. (2015) "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 21(1): 77-106.

Batır, K. (2017) "Avrupa Birliği'nin Geri Kabul Anlaşmaları: Türkiye ile AB Arasında İmzalanan Geri Kabul Anlaşması Çerçevesinde Hukuki Bir Değerlendirme", Yönetim Bilimleri Dergisi, 15(30): 585-604.

Bürgin, A. (2013) "Salience Path Dependency and the Coalition Between the European Commission and the Danish Council Presidency: Why the EU opened a Visa Liberalisation Process with Turkey?", European Integration Online Papers, 1: 1-19.

Bergkamp, L. (2002) "The Privacy Fallacy: Adverse Effect of European Data Protection Policy in an Information-Driven Economy", Computer Law & Security Report, 31-35.

Bossong, R. & Carrapico, H. (2016) "EU Borders and Shifting Internal Security", Technology, Springer, 72.

Council of Europe (1981) "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", retrieved from https://rm.coe.int/1680078b37

Commission, E. (2018) "European Border Surveillance System (EUROSUR)", retrieved from Migration and Home Affairs: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/eurosur

Council of Europe, European Union Agency for Fundamental Rights (2014) "Handbook on European Data Protection Law", Luxembourg: Publications Office of the European Union.

Çelik, Y. (2017) "Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı", Türkiye Adalet Akademisi Dergisi, 8(32): 387-406.

Digital Single Market (2017) "Bringing Down Barriers to Unlock Online Opportunities", retrieved from https://ec.europa.eu/commission/priorities/digital-single-market_en

Europa Nu (2016) "Q&A: Third Report on Progress by Turkey in fulfilling the requirements of its Visa Liberalisation Roadmap", retrieved from https://www.europa-nu.nl/id/vk3sgwa3a0z4/nieuws/q_a_s_third_report_on_progress_by_turkey?ctx=vgaxlcr1jzmx

European Commission (2013) "Roadmap Towards a Visa-Free Regime with Turkey", retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/news/news/docs/20131216-roadmap_towards_the_visa-free_regime_with_turkey_en.pdf

European Commission (2014) "Report From the Commission to the European Parliament and The Council on the Progress by Turkey in Fulfilling the Requirements of its Visa Liberalisation Roadmap", retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0646&from=EN

European Commission (2016a) "Directive on Protection of Natural Persons in relation to the Processing of Personal Data", Brussels: Official Journal of the European Union.

European Commission (2016b) "Report From the Commission to the European Parliament and the Council Second Report on Progress by Turkey in Fulfilling the Requirements of its Visa Liberalisation Roadmap", http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52016DC0140

European Commission (2016c) "Report From the Commission to the European Parliament and the Council Third Report on Progress by Turkey in Fulfilling the requirements of its Visa Liberalisation Roadmap", retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0278&from=EN

European Commission (2016d) "Turkey's Progress on the Visa Liberalisation Roadmap", retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we- do/policies/european-

agenda-migration/background-information/docs/20160504/turkey_progress_visa_liberalisation_roadmap_en.pdf

European Council Council of the European Union (2015) "Meeting of the EU heads of state or government with Turkey", 29/11/2015, retrieved from http://www.consilium.europa.eu/en/meetings/international-summit/2015/11/29/

Eurobarometer (2015) "Special Eurobarometer 431 Data Protection", Brussels: Directorate-General for Justice and Consumers (DG JUST).

Europe, C.O. (1985, 10 1) "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. May 4th, 2018 retrieved from Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", on https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

European Commission (2017) "Regulation on Privacy and Electronic Communication", Brussels.

European Data Protection Supervisor (no date information), "European Data Protection Supervisor", May 5th, 2018, retrieved from https://edps.europa.eu/about-edps_en

Fuster, L. G. (2014) "The Emergence of Personal Data Protection as a Fundamental Right of the EU", Brussel: Springer International Publishing.

Hoven, J., V. (2008) "Information Technology, Privacy, and the Protection of Personal Data", J. V. Hoven, & J. Weckert, Information Technology and Moral Philosophy (s. 301-318). Newyork: Cambridge University Press.

İktisadi Kalkınma Vakfı (2015) "Türkiye'de ve AB'de Kişisel Verilerin Korunması", İstanbul: İKV Yayınları.

Jeandesboz, J. (2017) "European Border Policing: EUROSUR, Knowledge, Calculation", Global Crime, p. 257-258.

Kişisel Verileri Koruma Kurumu (2019) "Kişisel Verileri Koruma Kurumu", April 13th, 2019, retrieved from https://www.kvkk.gov.tr/Icerik/5398/History

Küzeci, E. (2011) "Anayasal Bir Hak: Kişisel Verilerin Korunması", Bilişim Dergisi, 38(128): 142-149.

KVKK (2019) "Law on the Protection of Personal Data), September 30, 2019, retrieved from https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aea97a33-089b-4e7d-85cb-694adb57bed3.pdf

Mevzuat.gov.tr. (2016) "Kişisel Verilerin Korunması Kanunu", retrieved from http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

Nas, Ç. (2015) "Türkiye – AB İlişkilerinde Geri Kabul ve Vize Serbestliği: Hareketliliğin Yönetimi", Marmara Avrupa Araştırmaları Dergisi, 23(2):169-186.

OECD (2002) "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", Paris, France: OECD Publishing.

Official Journal of the European Communities (2000) "Charter of Fundamental Rights of The European Union", retrieved from http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Official Journal of the European Union (2013) Regulation (EU) No 603/2013. Brussels.

Official Journal of the European Union (2013) Regulation (EU) No: 1052/2013. Brussels.

Özsöz, M. & Bozçağa, M., Ö. (2010) "Anayasa Değişikliği Paketinin Türkiye'nin AB Müktesebatına Uyumuna Etkisi, İKV Değerlendirme Notu", retrieved from https://www.ikv.org.tr/images/upload/data/files/anayasa_degisikligi_degerlendirme_notu(1).pdf

Roots, L. (2015) "The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination", Baltic Journal of European Studies- Tallinn University of Technology, p. 108-125.

Republic of Turkey Ministry of Foreign Affairs (2011) "Turkey and the European Union Have Launched a Dialogue on Visa Liberalisation and Signed the Readmission Agreement", retrieved from http://www.mfa.gov.tr/turkey-and-the-european-union-have-launched-a-dialogue-on-visa-liberalisation-and-signed-the-readmission-agreement.en.mfa

Stiglmayer, A. (2012) "Visa-Free Travel for Turkey: In Everybody's Interest", Turkish Policy Quarterly, 11(11): 99-109.

Şen, Y.F., Özkorul G. (2016) "Türkiye-Avrupa Birliği İlişkilerinde Yeni Bir Eşik: Sığınmacı Krizi Bağlamında Bir Değerlendirme", Göç Araştırmaları Dergisi, 2(2): 86-119.

Tekin, N. (2014) "Kişisel Verilen Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", Human Rights Review, 4(1): 21-89.

United Nations (1948) "Universal Declaration of Human Rights", retrieved from http://www.un.org/en/universal-declaration-human-rights/

Üstübici, A.(2017) "Türkiye'de Göç Politikalarının Dönüşümü: Yasadışılığın Uluslararası Üretiminden makbul Yabancıya", Toplum ve Bilim, 140: 106-121.

(2016)., "Patrolling Power Europe: The Role of Satellite Observation in EU Border Management", I. Słomczynska, & P. Frankowski içinde, EU Borders and Shifting Internal Security (s. 73-74). London: Springer International Publishing.

## ENDNOTES

[i] Universal Declaration of Human Rights, United Nations, For more information, see: http://www.un.org/en/universal-declaration-human-rights/

[ii] 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"

[iii] Council of Europe Treaty No.108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

[iv] Directive 95/46/EC.

[v] Regulation (Ec) No 45/2001 of the European Parliament and of the Council of 18 December 2000 "On the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data", (Online) https://edps.europa.eu/sites/edp/files/publication/reg_45-2001_en.pdf Date accessed: 04.05.2018

[vi] Directive 2002/58/EC. For more information, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML

[vii] European Border and Coast Guard Agency. It helps the EU countries and Schengen associated countries manage their external borders and cooperates with border authorities. For more information, see: https://europa.eu/european-union/about-eu/agencies/frontex_en

[viii] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe.

[ix] PNR is Passenger Name Record. It is a collection of data regarding the information of traveller individuals.

[x] ETIAS. EU Travel Information and Authorisation System is an electronic system in which tracks of visitors with visa exemption for Schengen Zone are kept.

[xi] EU General Data Protection Regulation (GDPR), Key Changes, For more information, see; https://www.eugdpr.org/the-regulation.html Date accessed: 06.05.2018

[xii] Ibid.

[xiii] Ibid.

[xiv] Ibid.

[xv] 'Kişisel Verileri Koruma Kurumu' in Turkish.