GRIFFITH COLLEGE DUBLIN

LLM Dissertation Submission Cover Sheet

Student name:	Seyma Melekoglu
Student number:	3128792
Dissertation title:	Personal Data Protection Under European and Turkish Law – Assessment of GDPR and PDPL
Supervisor's name:	Elettra Bargellini
Supervisor's signature:	Elettra Bargellini

Plagiarism disclaimer:

I understand that plagiarism is a serious offence and have read and understand the college's policy on plagiarism and that my dissertation will be checked for plagiarism through TURNITIN. I also understand that I may receive a mark of zero if I have not identified and properly attributed sources which have been used, referred to, or have in any way influenced the preparation of this dissertation, or if I have knowingly allowed others to plagiarise my work in this way.

I hereby certify that this dissertation is my own work, based on my personal study and/or research, and that I have acknowledged all material and sources used in its preparation. I also certify that the dissertation has not previously been submitted for assessment and that I have not copied in part or whole or otherwise plagiarised the work of anyone else, including other students.

Signature of student: *Seyma Melekoglu* **Date:** 09.08.2024

Note to LLM students: You **MUST** submit TWO HARD-BOUND COPIES + A COPY ON MOODLE. You MUST retain the receipt issued to you as proof of submission.

FOR OFFICE USE ONLY:

No. of copies received (please tick):	2 x hard-bound	
Confirmation from student that soft copy submitted on Moodle:	Yes	
Date:		
Received by:	**Name:**	
	Signature:	

PERSONAL DATA PROTECTION UNDER EUROPEAN AND TURKISH LAW – ASSESSMENT OF GDPR AND PDPL

Master Thesis of LLM in International Commercial Law

Law School, Griffith College Dublin

Seyma Melekoglu

2024

CANDIDATE DECLARATION

Candidate Name: Seyma Melekoglu

I certify that the dissertation entitled 'PERSONAL DATA PROTECTION UNDER EUROPEAN AND TURKISH LAW – ASSESSMENT OF GDPR AND PDPL' submitted for the degree of LLM in International Commercial Law is the result of my own work and that where reference is made to the work of others, due acknowledgment is given.

Candidate signature: *Seyma Melekoglu*
Date: 09.08.2024

Supervisor Name: Elettra Bargellini
Supervisor signature: 
Date: 09.08.2024

ACKNOWLEDGEMENTS

I would like to thank my supervisor Elettra Bargellini, who guided and patiently supported me with her contributions and guidance in the preparation of this study, and my mother Fatos Gul Melekoglu and my father Haluk Melekoglu who have always supported me.

Seyma Melekoglu

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

EUROPOL	: The European Police Organisation
OECD Guidelines	: Guidelines on the Protection of Privacy and Transborder Movement of Personal Data
The Authority	: Personal Data Protection Authority
The Code No. 4721	: Turkish Civil Code No. 4721
The Code No. 4857	: Turkish Labour Law No. 4857
The Code No. 5237	: Turkish Criminal Code No. 5237
The Commission	: European Union Commission
The Constitution	: Constitution of the Republic of Turkey
The Convention No. 108	: Convention No. 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data
The Council	: The Council of Europe
The Directive 95/46/EC	: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
The ECHR	: European Convention on Human Rights
The EU	: European Union
The EU Convention	: The Treaty on European Union and the Treaty on the Functioning of the European Union
The GDPR	: General Data Protection Regulation
the Member States	: Member States of European Union
The OECD	: The Organisation for Economic Co-operation and Development
The PDPL	: Personal Data Protection Law No. 6698

ABSTARCT

With the rapid development of information and communication technologies, the increasing sensitivity in the collection, processing and storage of personal data has increased the necessity of legal regulations. In 1995 Directive 95/46/EC, the first framework legal regulation in the field of personal data protection in European Union law, entered into force. Later, due to the need for more detailed regulations with the advancement of technology and the inability of Directive 95/46/EC to ensure uniformity in this field, the need for re-regulation was felt and thus, the European Union General Data Protection Regulation (the GDPR) was adopted in May 2016.

Considering the Turkish law, the Personal Data Protection Law (the PDPL), which is the first framework law prepared on the basis of Directive 95/46/EC, entered into force in 2016. The question of whether the PDPL is incomplete in terms of the innovations brought by the repeal of Directive 95/46/EC and the adoption of the GDPR has been raised and the need to carry out this study has been felt.

In this study, firstly, the legal nature of personal data protection law and its historical development in Turkish and European law are emphasised and the legal regulations in Turkey and the European Union in this field are mentioned. Secondly, the basic concepts and the principles and conditions of data processing are explained. Afterwards, based on the guidance of the GDPR, the rights of the data subject and then the obligations of the controller are detailed. Finally, the various means of protection of personal data are discussed within the framework of the application to the controller, administrative sanctions, criminal sanctions and general regulations, and the deficiencies of the PDPL are addressed.

The aim of this study is to reveal the harmonisation and differences between the provisions of the GDPR and the PDPL. Although it is seen that the PDPL is largely compatible with the GDPR in terms of basic principles, it is concluded that it would be beneficial to make changes and additions to the PDPL and to improve it according to the GDPR, especially in terms of issues such as liability, sanctions, individual rights and data protection measures.

INTRODUCTION

In today's digital age, the protection of personal data is becoming increasingly important. With the advancement of technology and the impact of globalisation, rapidly increasing data processing activities in national and international institutions have increased access to and sharing of personal data. The proliferation of the Internet, the acceleration of the digitalisation process and technological advances pose new and complex challenges in the collection, storage, and processing of individuals' personal information. As technology advances, information has gained significant value and turned into an economic asset. This transformation has also brought concerns regarding the protection of personal data. In the event that personal data is obtained without consent, the uncertainty about who will use it and for what purpose has led to many risks that seriously affect the right to privacy. In this context, legal regulations play an important role in ensuring data privacy and security for individuals.

As a result, regulations have been established for the protection of personal data in order to ensure that the individual, who is left behind within the scope of data processing activities, can continue to protect and develop their personality. Therefore, the right to protection of personal data is becoming increasingly important, and more stringent rules and legal regulations are being introduced by regulatory authorities. Regulations such as the European Union's General Data Protection Regulation (the GDPR) and similar laws in other countries regulate how personal data is processed and protected, and they strengthen the rights of individuals in this regard. The GDPR, which I will discuss in detail later in this study, provides a globally accepted framework for the personal data protection.

This study examines the differences and similarities between the Personal Data Protection Law No. 6698 (the PDPL), which was inspired by the Directive 95/46/EC, and the GDPR, as well as the effectiveness of both legislation on the protection of personal data. In this study, answers have been sought to the questions of what the main changes are brought by the GDPR to the law on the protection of personal data and whether the PDPL has any deficiencies in the face of the regulations in the GDPR. In the light of all these questions, the provisions of GDPR and PDPL are compared and analysed. In addition, where necessary, the provisions of Directive 95/46/EC that differ from the GDPR are also referred to.

In Chapter 1, firstly, the legal nature of the right to protection of personal data is emphasised and different perspectives on this issue are examined. Afterwards, the data protection laws of the Member States of the European Union (the Member States) and the international regulations on the protection of personal data that have started to enter into force are mentioned. A general assessment of the purpose, scope and nature of the Directive 95/46/EC and the GDPR, which are the framework data protection regulations in European Union (the EU) law, has been made. Finally, the development of the law on the protection of personal data, in particular the PDPL, in the Turkish legal system is emphasised and the reasons for the emergence of the law, its scope and purpose are also examined.

In Chapter 2, the basic concepts and principles of personal data protection law and the conditions under which lawful data processing can be mentioned are analysed. While analysing and evaluating, the deficiencies in the PDPL compared to the GPDR are indicated.

In Chapter 3, the rights of the data subject arising from the processing of his/her personal data and the obligations of the data controller and the data processor are explained. In terms of the obligations of data controllers, the GDPR and the PDPL are compared and the deficiencies in the PDPL are stated.

In Chapter 4 which is the last part of the study, the remedies for the protection personal data provided by the PDPL and the GDPR are analysed and compared under the headings of application to the data controller, administrative remedies, criminal remedies and protection remedies in general regulations, and the weak points of the PDPL are stated.

This thesis employs doctrinal and comparative analysis methods. The doctrinal analysis allows to explain the main features of the EU and Turkish regimes on data protection. Moreover, thanks to the comparative approach similarities and differences between the regulations were highlighted, and the influence of EU law on the drafting of the PDPL was assessed.

CHAPTER 1
LEGAL NATURE, HISTORICAL DEVELOPMENT AND SOURCES OF THE CONCEPT OF PROTECTION OF PERSONAL DATA

In this chapter, the legal nature, historical development and sources of the concept of protection of personal data are analysed. In the first part, the legal nature of the protection of personal data is emphasised and the evaluation of personal data in terms of the right to property and the right to personality is discussed. In the second part, the historical development and sources of the legislation on the protection of personal data in EU law and Turkish law are analysed. Thus, the emergence process and historical development of Directive 95/46/EC and the GDPR and the PDPL are detailed in this section.

1. Legal Nature of The Concept of Personal Data Protection

1.1. Overview of Nature of the Concept of Personal Data Protection

Determining the legal nature of personal data is extremely important in terms of determining the legal framework for the protection and processing of such data. This determination is important in clarifying many issues such as which rights and obligations personal data are subject to, how they can be processed and how they should be protected. The limits of protection of personal data are directly related to the legal nature attributed to these data. The basic framework in which personal data is evaluated will also determine the scope of the protection to be provided.

There is no direct definition in 'Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (the Directive 96/45/EC), which is the first regulation of the Council of Europe (the Council) on personal data protection and which I will discuss in more detail below. However, in the GDPR[1], which is currently the most comprehensive regulation in the international context, personal data is defined as 'any information relating to an identified or identifiable natural person'.[2] In Turkish law, a qualification very similar to this definition has been made and it is stated in the PDPL that personal data refers to 'any information relating to an identified or identifiable natural person'.[3]

[1] 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 [2016] OJ L119/1 (General Data Protection Regulation).
[2] General Data Protection Regulation, Art. 4.
[3] Personal Data Protection Law No. 6698 (Turkey), 24 March 2016, Official Gazette No. 29677.

Although we can identify the concept of personal data protection with many fundamental rights and freedoms, it is possible to divide it into two as the approach that considers personal data as an economic right and the approach that considers it within fundamental human rights. Considering that personal data is located at the intersection of personal concerns, capital interests and public authority policies, it is possible to say that the legal characterisation of this data varies from country to country.[4] While property rights and intellectual property rights are discussed in the Anglo-American legal system, the prevailing view in continental Europe is that personal data is linked to the personal rights of the data subject.[5]

1.2. The Appeal of a Property Rights

The economic approach, which treats the concept of personal data as an independent product abstracted from its owner, is generally divided into two main groups, namely, whether this data should be considered within the scope of the owner's property rights or within the scope of the owner's intellectual property rights.[6]

The property right approach, which aims to establish full control over personal data, claims that individuals have a property right in personal data within the scope of property law, and based on this right, individuals can sell this data and share it with any organisation or person they wish. However, this view has been criticised on the grounds that a person has an absolute right over the essence of other personal data such as religious beliefs, criminal record history, sexual orientation, biometric data and that it is not possible to transfer or waive these data completely to another person under the law of goods.[7]

The proponents of the view that personal data is the subject matter of intellectual property law argue that the control and disposition powers of the author over their work, such as making changes to the work and prohibiting changes to the work, are similar to the control and disposition powers over the personal data of the person, and therefore the

[4] Rabia Ozkan, 'Evaluation of Personal Data Protection Law within the Frame of Personal Right Protection' (2021) 3 Ankara Sosyal Bilimler Universitesi Hukuk Fakultesi Dergisi (ASBU Law Journal) 675, 680

[5] Huseyin Can Aksoy, 'The Right to Personality and Its Different Manifestations As the Core of Personal Data' (2008) 5 Ankara Law Review 235, 236

[6] Sinan Sami Akkurt, 'A Comparative Overview of the Ideas on the Legal Category of the Personal Data Concept' (2020) 2 Kişisel Verileri Koruma Dergisi 20, 27

[7] ibid 23.

main purpose of both concepts is consistent.[8] This view has been criticised on the grounds that data protection law, unlike the purpose of intellectual property protection, is not concerned with any intellectual production and contribution to such production, and that personal data is not the work of the voluntary production of the data subject, and that such data cannot be considered as a work and therefore cannot be the subject of intellectual property law.[9]

1.3. The Appeal of a Personal Rights

It can be said that the reason for the different evaluation of the legal nature of personal data between Anglo-American law and continental Europe is partly due to the historical experiences of Europeans.[10] The "census decision" of the German Federal Constitutional Court in 1983 pioneered the association of personal data privacy with human dignity and the individual's right to self-improvement.[11] In addition, the Directive 95/46/EC states '...in particular the protection of the right to privacy of individuals...', thus recognising that personal data is closely related to human rights.[12] Furthermore, Article 8 of the European Convention on Human Rights (the ECHR), entitled "respect for private and family life", emphasises that the protection of personal data and privacy are closely associated with fundamental human rights and the right to private life.[13] The GDPR also recognises the protection of personal data as a fundamental human right. Likewise, Article 1 of the PDPL emphasises that personal data shall be considered within the scope of fundamental human rights.[14]

2. Historical Development and Sources of Personal Data Protection

[8] Sinan Sami Akkurt, 'A Comparative Overview of the Ideas on the Legal Category of the Personal Data Concept' (2020) 2 Kişisel Verileri Koruma Dergisi 20, 24
[9] Pamela Samuelson, 'Privacy as Intellectual Property' (2000) 52 Stanford Law Review 1125, 1141.
[10] ibid 1143
[11] Translation of the Census Act Judgement https://freiheitsfoo.de/census-act/ (02.01.2024).
[12] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art. 2.
[13] European Convention on Human Rights (1950) [Council of Europe], Art. 8.
[14] Personal Data Protection Law No. 6698, Art. 1.

2.1. Overview of Historical Development and Sources of Personal Data Protection

The protection of personal data has gained importance in continental Europe, especially since the second half of the 20th century. With the development of technology, advances in information processing and storage methods have enabled the collection and processing of personal data on a larger scale, and the potential risks that may jeopardise the privacy of individuals and the confidentiality of their personal information have led to the need for national and international studies on this issue. In addition, historical experiences have revealed the negative effects of the misuse of personal data on individuals, and the abuse of personal data by Nazi Germany and other totalitarian regimes, especially during World War II, emphasised the importance of protecting these data. In addition, as democratic values and human rights have become increasingly important, demands for the protection of individuals' personal data have increased, and in this period, with the democratisation process and increased respect for human rights in Europe, the protection of personal data has begun to be seen as an important public health issue. For example, the Land of Hesse in Germany adopted a data protection law in 1970 and this law was recognised as the first law in this field in the world. Later on, some European countries such as Sweden, Austria, Denmark and France followed the same path and adopted special laws in their domestic laws in the 1970s.[15]

Following the various regulations made by the countries in their domestic laws, international regulations have been needed especially after 1980, since, as mentioned before, it has caused a number of international restrictions, especially in the field of security and trade.

The Organisation for Economic Co-operation and Development (the OECD) adopted the "Guidelines on the Protection of Privacy and Transborder Movement of Personal Data" (OECD Guidelines) on 23 September 1980, which was one of the first important initiatives in the international protection of personal data.[16] With the developing technology and increasing use of the internet, these principles, which are non-

[15] Ilke Gursel, 'Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law' (2016) 18 Dokuz Eylul Universitesi Hukuk Fakultesi Dergisi 33, 38

[16] Yasime Hosnut, 'Protection of Personal Data in Turkey and International Regulations' (2019) 6 Yeni Medya, Hakemli, Akademik, E-Dergi 32, 38 https://dergipark.org.tr/tr/download/article-file/1302068 (04.04.2024)

binding and advisory in nature, have become inadequate due to the emergence of new risks that were not foreseen at the time these principles were published.[17]

Furthermore, on 28 January 1981, the Council signed Convention No. 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data (the Convention No. 108)[18], which is of great importance as it is the first binding international convention on the protection of personal data.[19] One of the Council's objectives in establishing the principles set out in Convention 108 was to concretise the principle laid down in Article 8 of the ECHR that 'the right to respect for his private and family life, home and correspondence'.[20] Adopted on 18 May 2018, the Protocol Amending the Convention for the Protection of Individuals with regard to the Processing of Personal Data (108+) modernised Convention No. 108. With the signing of this protocol, objectives such as adapting to the innovations brought by information technologies, strengthening the protection of privacy in the digital field and strengthening the monitoring mechanisms of the convention were set.[21]

2.2. Regulations in European Union Law

In the following sections, I will describe the historical development of the EU data protection regime, with a special focus on the GDPR and the Directive 95/46/EC, which forms the basis of the GDPR. In addition, I will analyse the key within the EU data protection regime.

2.2.1. Overview of Regulations in European Union Law

Founded in the second half of the 20th century, the basic philosophy of the EU is based on economic and political partnership and the founding principles of the EU are built on generally accepted common values such as equality, human dignity, protection of

[17] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 74
[18] Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108 (Convention 108).
[19] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 76
[20] Ilke Gursel, 'Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law' (2016) 18 Dokuz Eylul Universitesi Hukuk Fakultesi Dergisi 33, 38
[21] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 78

fundamental rights and freedoms, existence of democratic institutions, rule of law and transparency. Although the EU has made efforts in domestic law to ensure the free movement of persons, goods, services, capital and information, shortcomings have been felt in the area of the free movement of personal data of EU citizens.[22] At the European level, the protection of privacy is recognised as a fundamental human right, as mentioned above, and this principle is enshrined in a number of regulatory texts, most of which were developed after the Second World War. The tragedies and atrocities of this period have shown how large databases of personal data have been used to segregate populations and target minority groups. These experiences have been seen as a clear and tragic demonstration of how dangerous it can be to allow public intrusion into the private sphere.[23]

2.2.2. The Directive 95/46/EC

The Directive 95/46/EC adopted on 20 February 1995 by the European Parliament and the Council of the European Union under the title 'Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data'.[24] By harmonising national legislation with the framework and minimum standards set by the Directive 95/46/EC, it is aimed to protect personal data and thus ensure the secure free flow of data between the Member States. In this way, it is thought that the economic interaction arising from the flow of data between the Member States will not be interrupted.

Considering that legitimacy, limitation of purpose, transparency, proportionality, security and control are among the principles set by the Directive 95/46/EC, it is possible to say that the principles in the Directive 95/46/EC do not differ much from other international and Member State regulations.

With the framework provisions of the Directive 95/46/EC, the Member States have endeavoured to ensure the protection of personal data by making separate national regulations and as a result, different practices have emerged within the borders of the EU.

[22] Dogan Kılınc, 'Protection of Personal Data as a Constitutional Right' (2012) 61 Ankara Universitesi Hukuk Fakultesi Dergisi 1089, 1117
[23] Neil Robinson & Hans Graux & Maarten Botterman & Lorenzo Valeri, 'Review of the European Data Protection Directive' 2019 the RAND Corporation, 5
[24] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The existence of different practices at the EU level is not acceptable for the EU, which claims to be rooted in the protection of human rights and freedoms. This situation shows that personal data processing within the EU should be made more consistent and harmonised.[25] Considering that the founding philosophy of the EU is based on economic and political partnership; with the development of commercial and social relations between the Member States, the need for convergence and coordination of laws in many areas between the Member States has arisen, as the differences between the laws regulated in different Member States make it difficult to regulate in accordance with the internal market objective. Accordingly, the search for uniformity in personal data protection law has emerged. Article 8 of the Directive 95/46/EC also states that this common regulation is the result of a common effort to ensure the free flow of personal data and to equalise the level of personal data protection in all Member States.[26]

In the face of the increasing need for the protection of individuals' data, in June 2011, the need for the renewal of the Directive 95/46/EC was mentioned and at the beginning of 2012, the EU Commission prepared an amendment proposal on this issue. Subsequently, the Article 29 Working Party also recognised the need for reform in the field of data protection.[27]

2.2.3. General Data Protection Regulation

On 12 March 2014, the draft of the GDPR was adopted by the EU Parliament. The Council expressed its views on the Draft on 15 June 2015, negotiations continued in the following process and at the end of the process, the GDPR was adopted on 27 April 2016 and published in the Official Journal of the EU on 4 May 2016. The effective date of the Regulation was set as 25 May 2018 with Article 99/2 of the GDPR.[28] The Regulation entered into force on this date. As of this date, the provisions of the GDPR have become directly binding in all Member States and a period of two years has been stipulated for

[25] Ipek Cimen Bulut, 'New Techniques and Enforcement Mechanisms Provided by the European Union General Data Protection Regulation' (2020) 20 Anadolu Üniversitesi Sosyal Bilimler Dergisi 127, 129
[26] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[27] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 85
[28] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 86

the Member States to incorporate the provisions of the GDPR into their national legal systems.[29]

Regulations and directives are different in their effects. In contrast to the direct effect of regulations, directives indirectly contribute to harmonisation between EU law and the legal systems of the Member States. Directives are harmonisation framework regulations setting out the objectives to be achieved by all Member States but leaving national authorities free to decide how to transpose these objectives into national law, while regulations are unilateral provisions which, once enacted by the EU, automatically become binding and enforceable in all Member States. Thus, unlike the Directive 95/46/EC, the GDPR introduces rules to be directly applied to disputes by the Member States rather than providing guidance to the Member States as it is regulated as a "Regulation".[30] Therefore, within the scope of GDPR, it is aimed to uniformize different legal regulations regarding the protection of personal data among the Member States.

There are two main objectives that the GDPR aims to fulfil. The first objective is to protect the rights of individuals in the EU, which includes providing individuals with greater control and transparency to ensure the privacy and security of personal data. The second objective is to facilitate the free movement of data across the EU. This aims to support the digital economy by reducing data-driven barriers to business and trade.[31] During the Directive 95/46/EC period, the transfer and movement of personal data between the Member States was subject to many bureaucratic obstacles both within and outside the EU. Therefore, the first article of the GDPR clearly states that the free movement of personal data within the EU cannot be prevented or prohibited.[32]

2.3. Regulations in Turkish Law

In the following sections, I will discuss the developments in Turkish law in the field of personal data protection. I will delve into the PDPL, which is the main regulation on the protection of personal data in Turkish law, as well as other Turkish laws and regulations that contain provisions on data protection.

[29] Ayse Nur Akinci, 'Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakimindan Değerlendirilmesi' (2017) 6 T.C. Kalkinma Bakanliği Yayını, 5
[30] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 84
[31] Ozan Baris Yilmaz, *Turkiye ve Avrupa Birliği'nde Kisisel Verilerin Korunmasi ve Uygulanacak Hukuk* (1st edn, Adalet Yayınevi 2022) 80
[32] General Data Protection Regulation, Art. 3(1).

2.3.1. Overview of Regulations in Turkish Law

Concerns arising from the proliferation of new communication technologies in Turkey and the problems experienced in relations with the EU, such as the prevention of data transfer to countries that do not comply with the EU Directive, have made the need for legal regulation on the protection of personal data in Turkish law more evident. Thus, it is aimed not only to protect personal data, but also to eliminate the power imbalance in data transfer between public and private organisations.

Before establishing its own legal regulation on the protection of personal data, Turkey was a party to international agreements such as the Universal Declaration of Human Rights of the United Nations, and until a protective law was enacted, it was tried to be secured separately through articles added to the Constitution, decrees with the force of law and conventions in domestic law.[33]

In Turkish law, the protection of personal data was first included in the Constitution under Article 20 on the right to privacy.[34] With the clause added to Article 20 of the Constitution, it has been stated that everyone has the right to demand the protection of personal data and it has been revealed that the processing of personal data of individuals should only be with explicit consent and in the manner specified in the laws.[35]

Furthermore, there are offences related to personal data between Articles 135 and 140 of the Turkish Criminal Code No. 5237 (the Code No. 5237), and issues such as recording personal data, transferring or seizing data to another person, and not destroying data are regulated.[36] In addition to these, there are also types of offences that indirectly protect and regulate personal data in the Code No. 5237, such as failure to protect and violate confidentiality in relation to communication, recording or listening to conversations between individuals, and disclosure of information regarding the private lives of individuals.[37]

---

[33] Yasime Hosnut, 'Protection of Personal Data in Turkey and International Regulations' (2019) 6 Yeni Medya, Hakemli, Akademik, E-Dergi 32, 39 https://dergipark.org.tr/tr/download/article-file/1302068 (06.05.2024)

[34] Ozan Baris Yilmaz, *Turkiye ve Avrupa Birliği'nde Kisisel Verilerin Korunmasi ve Uygulanacak Hukuk* (1st edn, Adalet Yayınevi 2022) 43

[35] Constitution of the Republic of Turkey, 1982, Art. 20.

[36] Turkish Criminal Code No. 5237, 26 September 2004.

[37] Ozan Baris Yilmaz, *Turkiye ve Avrupa Birliği'nde Kisisel Verilerin Korunmasi ve Uygulanacak Hukuk* (1st edn, Adalet Yayınevi 2022) 35

In addition, Article 75/2 of the Turkish Labour Law No. 4857 (the Code No. 4857) imposes an obligation on the employer to use the information obtained while keeping personal files about the employee in accordance with the rules of honesty and in accordance with the law, and in addition, the employer shall not disclose the information as long as the employee has a legitimate interest in keeping this information confidential.[38]

The Law No. 6563 on the Regulation of Electronic Commerce, which aims to regulate the trade activities on electronic platforms and the responsibilities of the relevant parties, also addresses issues related to personal data at many points, as many personal data can be processed while meeting the requirements of electronic commerce.[39]

According to Article 24 of the Turkish Civil Code No. 4721 (the Code No. 4721), it is stated that attacks on personal rights are unlawful as a rule and those who are subjected to these attacks may request protection from the court.[40] Considering that the most important purpose of the PDPL is the protection of private life and personal rights, as stated in Article 1 of the PDPL, it is clear that this situation is related to the Code No. 4721. Therefore, the data controller and data processor who violate the personal rights of the data subject shall be liable under the Code No. 4721 as well as the PDPL.

2.3.2. Personal Data Protection Law No. 6698

It is clear that the specific provisions mentioned above are insufficient to provide satisfactory results on data protection without a comprehensive framework law.[41] Although Turkey is a party to many international regulations on the protection of personal data, the lack of regulations to provide adequate protection in domestic law is an important factor in the emergence of PDPL. With the development of the perception and awareness of the protection of human rights in Turkey, especially after the 2010 constitutional amendment, a comprehensive framework law on the protection of personal data was needed and as a result, the PDPL entered into force on 7 April 2016. In addition, the Personal Data Protection Authority (the Authority), which is responsible for the

[38] Turkish Labour Law No. 4857, 10 May 2003, Art.75.
[39] Ozan Baris Yilmaz, *Turkiye ve Avrupa Birliği'nde Kisisel Verilerin Korunmasi ve Uygulanacak Hukuk* (1st edn, Adalet Yayınevi 2022) 35
[40] Turkish Civil Code No. 4721, 22 November 2001, Art. 24.
[41] Ilke Gursel, 'Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law' (2016) 18 Dokuz Eylul Universitesi Hukuk Fakultesi Dergisi 33, 44

supervision and enforcement of personal data in Turkey, was established in 2017 with a public legal entity and administrative autonomy.[42]

The absence of a legal framework on the protection of personal data in Turkey has also led to delays and failures in the conclusion of operational cooperation agreements with the European Police Organisation (EUROPOL), as the exchange of information and documents cannot be carried out via electronic transmission.[43] In the general justification section of the PDPL, other reasons for the need for a framework on the protection of personal data are also mentioned, such as Article 135 and its subsequent articles of the Code No. 5237 and Article 24 and its subsequent articles of the Code No. 4721 are abstract in legal disputes regarding the violation of personal data, the fact that four of the chapters in the EU full membership process are directly related to the protection of personal data, the data sharing problems experienced with the Member States and the EU on issues such as military service, identity, citizenship and assets for foreigners living in Turkey and Turks living abroad, and the fact that the existing legislation is insufficient for sanctions and supervision despite the fact that sensitive data are frequently used and kept in the database, especially by health sector organisations.[44]

With the entry into force of the PDPL, which is inspired by Convention No. 108 and in particular the principles and rules set out in the Directive 95/46/EC, Turkey now has the primary source regulating data processing activities in Turkey.[45]

Although the PDPL is not directly based on the GDPR, the Authority strives to harmonise its decisions and directives with the GDPR by following the basic principles and spirit of the GDPR.[46]

CHAPTER 2

BASIC CONCEPTS AND PRINCIPLES OF PERSONAL DATA PROTECTION LAW

[42] Ozan Baris Yilmaz, *Turkiye ve Avrupa Birliği'nde Kisisel Verilerin Korunmasi ve Uygulanacak Hukuk* (1st edn, Adalet Yayınevi 2022) 44
[43] Nurullah Tekin, 'An Assessment of the Turkish Draft Law on Protection of Personal Data in Light of the EU Data Protection Directive' (2014) 4 Uyusmazlik Mahkemesi Dergisi 222, 248
[44] Justification of the Personal Data Protection Law 2016, General Justification.
[45] Ilke Gursel, 'Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law' (2016) 18 Dokuz Eylul Universitesi Hukuk Fakultesi Dergisi 33, 45
[46] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 40

In this chapter, I will compare and evaluate the concepts and principles of the GDPR with those of the PDPL. In this context, the definitions of basic concepts such as personal data, personal data processing, data controller, data processor, and the place of these concepts in these two legal frameworks will be analysed. In addition, information will be given on the legal principles and data processing conditions underlying the GDPR and the PDPL, the points where they are similar and different will be discussed, and if there is any change introduced after the Directive 95/46/EC, it will also be mentioned.

1. Personal Data

The concept of personal data is generally regulated together with the provisions of the Directive 95/46/EC, and the GDPR defines 'personal data' as any information relating to a specific or identifiable natural person.[47] If the information in the data set is sufficient to identify a person or can be linked to other information that will help identify a person, this data is considered personal data and is protected by the GDPR.[48] In other words, it is information that clearly reveals the identity of a person or makes it identifiable with additional information. In Article 4 of the GDPR, an explanatory provision is included as 'an identified natural person is a person who can be identified directly or indirectly, in particular by reference to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, genetic, mental, economic, cultural or social identity of that natural person'.[49]

Article 3 of the PDPL defines personal data as 'any information relating to an identified or identifiable natural person'.[50] In the justification section of the PDPL, it is stated that 'making the existing data identifiable by associating it with a natural person in any way' is sufficient for the data to be accepted as personal data. In the continuation of the justification, it is clearly stated that data such as name, telephone number, motor vehicle registration plate, social security number, passport number, curriculum vitae,

[47] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 87
[48] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 11
[49] General Data Protection Regulation, Art. 4.
[50] Personal Data Protection Law No. 6698, Art.3.

picture, image and sound recordings, fingerprints, genetic information are personal data due to their ability to make the person identifiable, even if indirectly.[51]

Although it is seen that the protection of personal data is limited to the data of natural persons in both regulations, there is no difference between the collection of this data directly due to the legal transactions of a natural person as an organ or representative of a legal entity.[52]

2. Processing of Personal Data

According to the GDPR, 'data processing' is defined as 'any interference with the collection, storage, retrieval, structuring, alteration, reading, querying, use, transfer to third parties, dissemination or making available of personal data or data sets, whether by automated or non-automated means, and any combination, restriction, erasure or destruction of data'.[53] Thus, it can be said that the GDPR interprets the term broadly in such a way as to recognise almost any interference with personal data as data processing. Considering the broad scope of the term, it should be emphasised that even the mere storage of personal data on a floppy disc or CD is considered as 'processing'.[54]

As in the GDPR, the PDPL provides a broad definition of the concept of data processing. As stated in Article 3 of the PDPL:

> Any operation performed on personal data such as obtaining, recording, storing, retaining, modifying, reorganising, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic means or by non-automatic means provided that it is part of any data recording system is considered as processing.[55]

Therefore, under both the GDPR and the PDPL, the activities carried out in the entire process from the acquisition of personal data to its deletion or anonymisation and destruction in a form that cannot be accessed, returned and reused in any way will be

[51] Justification of the Personal Data Protection Law 2016, Art. 3.
[52] Sefer Oguz, 'General Principles of Personal Data Protection Law' (2018) 13 Bilgi Ekonomisi ve Yonetim Dergisi 121, 125
[53] General Data Protection Regulation, Art. 4.
[54] Ilke Gursel, 'Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law' (2016) 18 Dokuz Eylul Universitesi Hukuk Fakultesi Dergisi 33, 47
[55] Personal Data Protection Law No. 6698, Art. 3.

considered as processing.[56] In addition, in both regulations, it is seen that the processing of personal data can be manual or 'automatic'.

3. Controller and Processor

In the GDPR, the data controller is defined as 'the natural or legal person, public authority, institution or other body which alone or jointly with others determines the purposes and means of processing personal data'.[57] The definition of data controller is stated in Article 3 of the PDPL as 'the natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data filing system'.[58] When these two definitions are compared, although it seems to be a more descriptive definition in the GDPR than in the PDPL, it has not made a difference in essence. In both definitions, the data controller is defined as 'the person who holds personal data', and it is stated that 'it is possible to consider legal person public institutions and organisations as data controllers'.

If more than one institution, organisation, person or legal entity determines the means and purposes of processing in the data processing process, then these parties become 'joint controllers' pursuant to Article 26 of the GDPR.[59] This means that if more than one party involved in the data processing process determines the means and purposes of processing, their responsibilities are shared. Although there is no direct provision in the PDPL, unlike the GDPR, the joint and several liability of these parties can be referred to the general provisions of the Turkish Code of Obligations No. 6098.[60]

The definition of data processor is the same in the GDPR and the PDPL and refers to the natural or legal person who processes personal data on behalf of the data controller based on the authorisation granted by the data controller.[61] The distinction between the data controller and the data processor is that the data controller is the legal or natural person who determines the purposes and methods of data processing, and the data processor is the person who performs data processing on behalf of the data controller and

[56] Ozan Baris Yilmaz, *Turkiye ve Avrupa Birliği'nde Kisisel Verilerin Korunmasi ve Uygulanacak Hukuk* (1st edn, Adalet Yayınevi 2022) 47
[57] General Data Protection Regulation, Art. 4.
[58] Personal Data Protection Law No. 6698, Art. 3.
[59] General Data Protection Regulation, Art. 26.
[60] Turkish Code of Obligations No. 6098, 11 January 2011.
[61] Personal Data Protection Law No. 6698, Art. 3.

in accordance with its instructions, and it is very important to identify the data controller and the data processor in order to determine the responsibilities.[62]

The GDPR states that a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons authorised to process personal data under the direct authority of the controller or processor is a 'third party', and a natural or legal person, public authority, agency or other body to whom personal data are disclosed is a 'recipient'.[63] Unlike the GDPR, the PDPL does not contain these definitions. In addition, although the PDPL mentions a different person, institution or organisation under the responsibility of the data controller by referring to the data controller and 'the person authorised by the data controller' in the section on the obligations of the data controllers, there is no explanation on this issue, and it is defined in Article 4 of the Directive on the Data Controllers Registry and it is stated who will be the person authorised.[64] It can be said that the fact that this definition is regulated by directive instead of by law is an important deficiency.

4. Principles Relating to the Processing of Personal Data

In the regulations on the protection of personal data, some common principles have been determined in order to ensure that data-related transactions are carried out in accordance with human dignity and values.[65] These principles are difficult to distinguish from each other and it is seen that some principles are the basis for the others and some of them play a complementary role.[66] These principles set out certain rules and standards regarding the protection and processing of personal data and aim to ensure that data processing is carried out in a fair, transparent and secure manner. These principles guide every stage of personal data processing and form the basis of data protection laws.

---

[62] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 90

[63] General Data Protection Regulation, Art. 4.

[64] Directive on the Data Controllers Registry 2017, Art. 4. https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=24276&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5 (05.08.2024)

[65] Ibrahim Korkmaz, 'An Assessment of the Law on Protection of Personal Data' (2016) 124 TBB Hukuk Dergisi 81, 99

[66] ibid 99.

Although there are minor differences between the GDPR and the PDPL, which determines its principles by adhering to the Directive 95/46/EC, it is possible to say that they are generally similar to each other.

In parallel with the trend of enhanced personal data protection in the basic approach of the GDPR, the data controller, who is responsible for the implementation of the principles, is directly regulated in Article 5 titled basic principles. In the PDPL, although it is not directly mentioned in Article 4 titled general principles, it is understood from the wording of Article 12 on the obligations of the data controller that the data controller is obliged in this area.[67]

Below, these basic principles are explained on the basis of the GDPR and in comparison with the PDPL.

4.1. Lawfulness, Fairness and Transparency

The principle of lawfulness is enshrined in both the PDPL, the GDPR and the Directive 95/46/EC. This principle requires data controllers to have a legal ground for processing personal data. Processing activities must not be contrary to other laws or legal obligations and fairness must always remain an overriding and general principle.[68]

The fairness of data processing can be judged when a balance is established between different interests, such as the data subject's interest in the right to privacy and the third parties' interest in obtaining information.[69] An important factor of fairness is a clear explanation of how the data is used and not taking any action that the data subject does not expect, which can be guaranteed by ensuring transparency.[70] In PDPL, the principle of fairness is replaced by the good faith. The principle of good faith, which is also included in Article 2 of the Turkish Civil Code No. 4721, is a general principle of law that stipulates that the sense of trust in a legal relationship should not be damaged.[71] Therefore, the principle of good faith in the PDPL and the principle of fairness in the GDPR are not fundamentally different concepts.

---

[67] Ayse Nur Akinci, 'Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakimindan Değerlendirilmesi' (2017) 6 T.C. Kalkinma Bakanliği Yayını 1, 33

[68] Rosemary Jay, *Guide to the General Data Protection Regulation* (1st edn, Sweet & Maxwell 2017) 85

[69] Ilke Gursel, 'Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law' (2016) 18 Dokuz Eylul Universitesi Hukuk Fakultesi Dergisi 33, 50

[70] Laura L Keogh, *Data Protection Compliance A guide to GDPR and Irish Data Protection Law* (1st edn, Clarus Press Ltd) 66

[71] M. Kemal Oguzman & Nami Barlas, *Medeni Hukuk* (20. edn, Vedat Kitapcilik 2014) 253

Prior to the GDPR, commentators considered transparency as part of the principle of fairness, but, for the sake of clarity, the principle of transparency is explicitly included in the GDPR to ensure lawful and fair processing of data.[72] Recital 39 states that data subjects should know to what extent their personal data are or will be processed.[73] It is not clear what is covered by this statement, which does not correspond to any specific information requirement.[74] In particular, the principle of transparency requires information on the identity of the controller, information on the purposes of the processing, confirmation of data subjects and the processing operations carried out on their personal data, awareness of individuals about the risks, rules, safeguards and rights relating to processing operations and how they can exercise these rights.[75]

Although the principle of transparency is not included in the PDPL, this can be assessed can be evaluated within the scope of Article 11 regulating the 'Rights of the Data Subject'.[76] In this article, which will be explained in detail in the following chapters of this study, it can be said that the rights of the data subject such as the right to learn whether personal data is processed, requesting information if personal data has been processed, learning the purpose of processing personal data and whether they are used in accordance with their purpose are linked to the principle of transparency. Moreover, this principle is included in the guidelines and decisions of the Authority and should be interpreted as an extension of the principle of equity.[77]

4.2. Purpose Limitation

In accordance with the principle of purpose limitation, personal data are collected for specific, explicit and legitimate purposes and can only be processed in line with these purposes.[78] The purpose of data processing plays a critical role in the legal compliance of the controller's activities, as it makes it possible to assess whether the principles of data

[72] Christopher Kuner & Lee A. Bygrave & Christopher Docksey (ed), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020) 314
[73] Recitals of General Data Protection Regulation, Recital 39.
[74] Christopher Kuner & Lee A. Bygrave & Christopher Docksey (ed), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020) 315
[75] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 88
[76] Personal Data Protection Law No. 6698, Art. 1.
[77] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 41
[78] General Data Protection Regulation, Art. 5(1).

minimisation, accuracy and storage limitation have been observed.[79] It is also clearly stated in the justification of the PDPL that data controllers will be liable for their actions if they process data for purposes other than the purposes they have stated.[80]

The purposes of data processing must be clear and unambiguous, and the processing of personal data for unspecified or unrestricted purposes is unlawful as it makes it difficult to determine the scope of the processing with certainty.[81]

Although the term 'collected' is used in the PDPL, the GDPR and the Directive, what is meant is 'the evaluation of personal data in a way to cover all subsequent transactions, including the collection of personal data.'

4.3. Data Minimisation

Data minimisation requires a continuous assessment of what personal data is collected, processed and stored, together with the reasons why. Personal data that is not necessary for the purpose should not be collected and continued to be processed.[82] The controller must limit the data collection to information directly relevant for the specific purpose of processing and the categories of data selected for processing must be necessary to achieve the specified purpose.[83] The purpose of data processing is not to keep the data at an absolute minimum level, but to limit the collection to a level that is appropriate and sufficient for the purposes of processing.[84]

The principle of being purpose related, limited and proportionate is regulated in both the GDPR and the PDPL. The term 'not excessive' in the Directive 95/46/EC has been changed to 'limited to what is necessary' in the GDPR. It can be argued that 'limited to what is necessary' imposes a more restrictive limit than 'not excessive'.[85]

---

[79] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 88
[80] Justification of the Personal Data Protection Law 2016, Art. 4.
[81] Christopher Kuner & Lee A. Bygrave & Christopher Docksey (ed), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020) 315
[82] Laura L Keogh, *Data Protection Compliance A guide to GDPR and Irish Data Protection Law* (1st edn, Clarus Press Ltd) 70
[83] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 102
[84] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 90
[85] Rosemary Jay, *Guide to the General Data Protection Regulation* (1st edn, Sweet & Maxwell 2017) 87

4.4. Accuracy

This principle of accuracy in the GDPR and according to the provision; taking into account the purposes for which they are processed, all reasonable steps should be taken to ensure that inaccurate personal data are deleted or corrected without undue delay.[86] In other words, a controller must not use personal data in its possession without first exercising due diligence to ensure with reasonable certainty that the data is accurate and up to date. Pursuant to the principle of accuracy and currency is also regulated in PDPL, it is stated that 'personal data are kept accurate and, where necessary, up-to-date'.[87]

Since the data controller who processes personal data keeps personal data for a specific purpose, inaccurate personal data will damage the interests of the data controller as well as the data subject.[88]

This principle is substantiated by other provisions of the GDPR and the PDPL, such as 'the rights of the data subjects to rectification and erasure of their personal data.'

4.5. Storage Limitation

The principle of storing personal data for a limited period of time for the purpose for which it is intended is enshrined in both the GDPR and the PDPL.[89] According to this principle, personal data should be processed only for the period required by the relevant purpose, and at the end of this period, the processing should be terminated. The data should either be destroyed or anonymised in such a way that the data subject cannot be identified. The requirement to retain data only for the period necessary for the purpose of processing is directly linked to the right to be forgotten.[90]

Recital 39 states that the period for which personal data are stored should be limited to a strict minimum period.[91] According to the PDPL; when determining the period of retention of personal data, the legislation will be looked at first, if a period is determined in the legislation, it will be kept for this period, if no period is determined in

[86] General Data Protection Regulation, Art. 5(1).
[87] Personal Data Protection Law No. 6698, Art. 4(2).
[88] Ibrahim Korkmaz, 'An Assessment of the Law on Protection of Personal Data' (2016) 124 TBB Hukuk Dergisi 81, 101
[89] Personal Data Protection Law No. 6698, Art. 4(2); General Data Protection Regulation, Art. 5(1).
[90] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 92
[91] Recitals of General Data Protection Regulation, Recital 39.

the legislation, personal data can only be kept for the period required for the purpose for which they are processed.[92] In addition, Article 16 of the PDPL stipulates that data controllers are obliged to notify the Data Controllers' Registry, to which they are obliged to register before starting data processing, of the maximum period required for the purpose for which personal data are processed.[93]

4.6. Integrity and Confidentiality

The principle of integrity and confidentiality in the GDPR provides for the processing of personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[94]

In the Directive 95/46/EC, security requirements are set out in Article 17, although they are not part of the principles.[95] Similarly, although the principle of integrity and confidentiality is not recognised as a separate principle in the PDPL, it is directly related to Article 12(4). According to this provision, it is regulated that the data controller and the data processor are obliged to protect the confidentiality of personal data and cannot disclose it to others in violation of the PDPL.[96]

4.7. Accountability

Unlike the Directive 95/46/EC, the principle of accountability, which has been added as a principle to the GDPR, states that data controllers are responsible for all activities related to the processing of personal data and bear the burden of proving compliance with all other principles of the GDPR.[97] The requirement to not only ensure but also demonstrate compliance is detailed in Article 24 of the GDPR on the responsibility of the controller.[98]

---

[92] Justification of the Personal Data Protection Law 2016, Art. 4.
[93] Personal Data Protection Law No. 6698, Art. 16(3).
[94] General Data Protection Regulation, Art. 5(1).
[95] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art.17.
[96] Personal Data Protection Law No. 6698, Art. 14(2).
[97] Paul de Hert & Guillermo Lazcoz, 'When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance' (2022) 8 Eur Data Prot L Rev 31, 35
[98] Christopher Kuner & Lee A. Bygrave & Christopher Docksey (ed), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020) 318

Although the principle of accountability is not regulated in the PDPL, it is directly related to the obligations imposed on the data controller and data processor regarding data security in Article 12.[99]

As a result, it is seen that the principles listed are generally the same between the two frameworks but some of them are not explicitly stated in the PDPL. It is possible to link the principles regulated in the GDPR but not separately regulated in the PDPL with other principles in the PDPL.

5. Conditions for Processing of Personal Data

In this section, the conditions for processing personal data stipulated in the GDPR and the PDPL will be discussed comparatively and the legal grounds that allow the processing of personal data in both regulations will be examined in detail. In addition, the similarities and differences between in both regulations will be emphasised and it will be discussed which regulation is more comprehensive or restrictive in which cases.

5.1. Legal Grounds

In the following sections, the legal grounds for the processing of personal data from the perspective of the GDPR and the PDPL will be discussed and the personal data processing conditions and legal exceptions foreseen or missing in both regulations will be determined.

5.1.1. Consent

In case of processing personal data, the data processor must prove that the processing is lawful. The GDPR defines consent as any freely given, specific, informed and unambiguously stated request, where the data subject indicates that the data subject, by a declaration or by a clear affirmative action, consents to the processing of personal data concerning him or her.[100] The PDPL, on the other hand, does not include the concept of consent alone, and the term 'explicit consent' is used. Article 5 of the PDPL regulates the

[99] Personal Data Protection Law No. 6698, Art.12.
[100] General Data Protection Regulation, Art. 4.

conditions for processing personal data, and according to this article, as a rule, it is prohibited to process personal data except in cases where the data subject has explicit consent or the exceptions listed in the article.[101] Although the concept of 'explicit consent' is not defined in the GDPR, when compared to the PDPL, it can be said that 'informed' consent has the same meaning as explicit consent.[102]

This provision in Article 5 of the PDPL has led to the understanding that consent is the main basis and that other cases of lawfulness are only possible if consent is not obtained.[103] However, the Authority has clarified that consent is not mandatory for a processing activity if other legal grounds specified in Article 5(2) of the PDPL are available.[104]

In the justification of the PDPL, explicit consent is defined as the declaration of consent given freely, with sufficient information, in a clear manner that leaves no room for doubt and limited to that processing, by the data subject to the processing of data concerning him/her, with reference to the Directive 95/46/EC.[105] Here, the question arises whether silence is considered sufficient for consent. In some cases, although legal texts and jurisprudence have interpreted silence as consent[106], since explicit consent is sought for the processing of personal data, it should be accepted that silence means refusal, not acceptance.[107]

In the GDPR's recital, it is stated that ticking a box when visiting a website, selecting technical settings for information society services, or in this context, the data subject may make statements that clearly indicate that he/she agrees to the proposed processing of his/her personal data, and that silence, pre-ticked boxes or inactivity should not constitute consent.[108]

In the doctrine, it is controversial whether the implicit declaration is sufficient to give consent, and according to some opinions, the implicit declaration that reveals the will of the data subject in a way that leaves no room for doubt will be sufficient to be

[101] Personal Data Protection Law No. 6698, Art. 5.
[102] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 114
[103] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 43
[104] ibid 43.
[105] Justification of the Personal Data Protection Law 2016, Art. 5.
[106] Gokhan Antalya, *Borclar Hukuku Genel Hukumler* (2nd edn, 2019, Seckin Yayincilik) 148
[107] Sefer Oguz, 'General Principles of Personal Data Protection Law' (2018) 13 Bilgi Ekonomisi ve Yonetim Dergisi 121, 131
[108] Recitals of General Data Protection Regulation, Recital 32.

accepted as consent, while according to another opinion, it is not possible to accept the implicit declaration as explicit consent.[109]

In addition, the validity of the consent given for the processing of personal data depends on the fact that this consent is given freely. The GDPR's recital states that consent will not constitute a valid legal basis for the processing of personal data, in particular where there is a clear imbalance between the data subject and the controller.[110] For instance, the Article 29 Working Party has noted that workers often cannot freely give or withdraw consent because of their relationship with their employer.[111]

Consent must be obtained for a specific, not general, processing activity and in an informed manner.[112] In other words, each situation in which consent is given for the processing of personal data must be specific and consent must be given in accordance with this specific situation. If there is more than one purpose, approval must be obtained separately for each purpose.[113]

It is not regulated in the PDPL, the GDPR and the Directive 95/46/EC that written consent is a condition of validity. Although there is no obligation to obtain consent in writing, since the burden of proving that the data subject has consented to the processing is on the data controller, obtaining consent in writing makes it easier for data controllers to fulfil this obligation.[114]

Although the data subject has the right to withdraw his/her consent at any time, the withdrawal of consent shall not affect the lawfulness of the processing activity carried out on the basis of consent before withdrawal.[115] Thus, its exercise only produces effects for the future. Withdrawal of consent is different from the right of data subjects to object, and the controller is not required to erase personal data processed legitimately on the basis of withdrawn consent, unless there is no other legal basis for retaining the data.[116] The data controller must inform the data subject about the right of withdrawal before giving

[109] Sefer Oguz, 'General Principles of Personal Data Protection Law' (2018) 13 Bilgi Ekonomisi ve Yonetim Dergisi 121, 132
[110] Recitals of General Data Protection Regulation, Recital 43.
[111] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 116
[112] ibid 115.
[113] Laura L Keogh, *Data Protection Compliance A guide to GDPR and Irish Data Protection Law* (1st edn, Clarus Press Ltd) 44
[114] Rosemary Jay, *Guide to the General Data Protection Regulation* (1st edn, Sweet & Maxwell 2017) 90
[115] General Data Protection Regulation, Art. 7(3).
[116] Christopher Kuner & Lee A. Bygrave & Christopher Docksey (ed), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020) 351

consent and ensure that withdrawal of consent is as easy as giving consent.[117] In the same way that consent is not subject to any validity condition, withdrawal of consent is not subject to any validity condition. A commitment that the consent cannot be withdrawn will be invalidated as it is against personal rights.[118]

There is a separate provision in the GDPR on how to proceed in the processing of personal data of children and according to this provision, the child must be at least 16 years old in order for the processing of personal data when providing information society services to a child to be validly based on his/her consent.[119] Where the data subject is under 16 years of age, the consent must be given by the right of custody holder or given by the child and approved by the right of custody holder.[120] The GDPR also provides that Member States may prescribe by law a lower age, provided that it is not below 13 years of age.[121] Since there is no provision in the PDPL regarding the processing of personal data of children, in such a case, the provisions of the general law will be taken as basis.

5.1.2. Necessary For the Conclusion and Performance of the Contract

In Article 6(1)(b) of the GDPR and Article 5(2)(c) of the PDPL, it is regulated that if it is necessary to process data for the establishment or performance of a contract to which the data subject is a party, this transaction may be deemed lawful. This provision is legally identical to the relevant provision under the Directive 95/46/EC.

The concept of 'performance of a contract' should not be limited to a specific phase of the contract, but should be taken broadly and cover data processing activities related to any phase of the contract.[122] However, it must be carefully assessed whether such processing is actually necessary for the fulfilment of the contract. This means that data processing may only be carried out if it is really necessary for the fulfilment of the contractual terms and purpose.[123] When assessing whether a data processing activity is necessary, it is necessary to consider the purpose of the contract from the perspective of both the controller and a reasonable data subject. In this way, it can be determined more

[117] General Data Protection Regulation, Art. 7(3).
[118] Sefer Oguz, 'General Principles of Personal Data Protection Law' (2018) 13 Bilgi Ekonomisi ve Yonetim Dergisi 121, 131
[119] General Data Protection Regulation, Art. 8(1).
[120] ibid.
[121] ibid.
[122] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 102
[123] ibid 102.

objectively whether the data processing is indeed necessary for the performance of the contract.[124] For instance, in an online shopping contract, transactions such as the delivery of the product using the customer's address details are considered within this scope.

5.1.3. Legal Obligation

The 'legal obligation' as a legal ground is similarly regulated in Article 6(1)c of the GDPR and Article 5(2)ç of the PDPL. While the regulation here is an obligation arising from the law of the EU and the Member State in terms of the GDPR, it is an obligation arising from Turkish law in terms of the PDPL.

Although the wording of Article 6(1)(c) does not clarify the type of legal obligations covered, it is understood to relate only to obligations arising directly from a provision in the law.[125] It would also apply where the obligation is not set out in a law but is determined by an additional legal act under public law, such as secondary or separate legislation, or by a binding decision of a public authority in a concrete case.[126]

Although there seems to be a difference in wording between the two regulations, the legal ground as a 'legal obligation' under the GDPR is essentially the same as the legal basis 'expressly provided for by law' in the PDPL, because the scope of the legal ground under the PDPL is wider and includes legal obligations arising from legal relations other than the law.

5.1.4. Vital Interest

The principle that the processing is necessary to protect the vital interests of the data subject or a third party is regulated in Article 6(1)(d) of the GDPR. Recital 46 describes a 'vital interest as one which is 'essential for the life of an individual and states that the processing of personal data pursuant to this legal basis should only take place where the processing cannot be explicitly based on any other legal basis.[127] Unlike the Directive

[124] Christopher Kuner & Lee A. Bygrave & Christopher Docksey (ed), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020) 331
[125] ibid 332.
[126] ibid 333.
[127] Recitals of General Data Protection Regulation, Recital 46.

95/46/EC, in the PDPL, as in the GDPR, the relevant provision includes not only the vital interests of the data subject, but also the equivalent interests of other natural persons.[128]

The PDPL explicitly authorises data processing based on this ground if the data subject is unable to express his/her consent and the data processing is necessary to protect his/her or others' life or physical integrity. Thus, while the PDPL's vital interest can only be applied in cases where consent is not possible, the GDPR has no such limitation. The PDPL's practice in this regard is more in line with Article 9(2)(c) of the GDPR on the processing of special categories of personal data in order to safeguard the vital interests of data subjects or others where data subjects are physically or legally incapable of giving consent.[129] Unlike Article 9 of the GDPR, Article 6(1)(d) does not mention that the processing decision may be taken by the controller only if the data subject is unable to give consent.[130] As a result, it is possible to say that the scope of this basis in the PDPL is broader than in the GDPR.

5.1.5. Legitimate Interest

Article 6(1)(f) of the GDPR provides that processing shall be lawful if it is necessary for the purposes of those interests, except where the interests or fundamental rights and freedoms of the data subject, in particular in the case of a child, requiring the protection of personal data outweigh the legitimate interests pursued by a controller or a third party.[131] Pursuant to this provision, data processing shall be lawful when the legitimate interests of the controller or third party outweigh the need to protect data subjects. This is determined as a result of a balancing of interests.[132]

When processing data on the basis of its legitimate interests, the controller must also take into account the reasonable expectations of the data subject.[133] If the rights of the data subject outweigh the legitimate interests of the controller, the controller may

[128] Personal Data Protection Law No. 6698, Art. 5(2)(b).
[129] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 46
[130] Christopher Kuner & Lee A. Bygrave & Christopher Docksey (ed), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020) 334
[131] General Data Protection Regulation, Art. 6(1)(f).
[132] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 103
[133] Laura L Keogh, *Data Protection Compliance A guide to GDPR and Irish Data Protection Law* (1st edn, Clarus Press Ltd) 46

protect the lawfulness of the processing by taking measures and providing safeguards aimed at minimising the effects of the processing on the rights of the data subject.[134] The data controller must provide a convincing legitimate reason to continue processing, otherwise it must stop processing.[135]

A similar provision is also regulated in the PDPL and Article 5(2)(f) stipulates that data processing is possible if it is necessary for the legitimate interests of the controller, provided that it does not prejudice the fundamental rights and freedoms of the data subject.[136] While under the GDPR, data processors are obliged to state clearly and in detail which legitimate interests they are processing data based on, there is no provision in the PDPL stating that data processors are obliged to detail their legitimate interests. Nevertheless, data subjects may claim that data processing based on legitimate interest is unlawful based on the general conditions.[137]

5.1.6. Performance of a Public Interest Task or the Exercise of Official Authority

Article 6(1)(e) of the GDPR provides that data processing will be lawful if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This legal basis applies to public authorities, such as law enforcement or government agencies, which may need to process personal data in order to fulfil their tasks, but also to third parties if this task is outsourced.[138]

Article 5(2)(a) of the PDPL regulates that the processing shall be deemed lawful if the possibility of data processing is expressly provided for in the law, without the requirement of public interest, and thus a broader expression is used compared to the GDPR. In the justification of the article, 'Taking the fingerprints of the suspects in accordance with Article 5 of the Police Duties and Powers Law No. 2559; The Ministry

[134] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 119
[135] ibid 120.
[136] Personal Data Protection Law No. 6698, Art. 5(2)(f).
[137] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 48
[138] ibid 48.

of Justice's processing of data regarding criminal convictions of individuals in accordance with the Criminal Records Law No. 5352' is given as an example.[139]

5.1.7. Personal Data Have Been Made Public by the Data Subject

Unlike the GDPR, in Article 5(2)(d) of the PDPL, making public of personal data by the data subject is also a ground for compliance with the law.[140] It is assumed that the legal interest to be protected has disappeared in the processing of such data, which is publicised by the data subject and therefore becomes accessible to everyone.[141] Personal data made public by the data subject himself/herself may be processed only for the purpose for which the data subject made the data public.[142]

In conclusion, although making public of personal data is accepted as a legal basis under the PDPL, the use of publicised data is quite limited and it is emphasised that this situation should be approached and handled with caution.[143]

5.2. Legal Compliance of Processing of Special Categories of Personal Data

Personal data that are particularly sensitive in terms of fundamental rights and freedoms of individuals deserve special protection.[144] Special categories of data are subject to separate protection due to the fact that they are data that may violate the fundamental rights and freedoms of the data subject more than other personal data, and the GDPR, The PDPL and the Directive 95/46/EC enumerate what these data are without any definition. The main reason why special categories of personal data are secured with additional protections is that these data have the potential to harm the person more than other personal data.[145]

---

[139] Justification of the Personal Data Protection Law 2016, Art. 5(2)(a).
[140] Personal Data Protection Law No. 6698, Art. 5(2)(d).
[141] Justification of the Personal Data Protection Law 2016, Art. 5(2)(b).
[142] Ozan Baris Yilmaz, *Turkiye ve Avrupa Birliği'nde Kisisel Verilerin Korunmasi ve Uygulanacak Hukuk* (1st edn, Adalet Yayınevi 2022) 53
[143] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 49
[144] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 110
[145] Ibrahim Korkmaz, 'An Assessment of the Law on Protection of Personal Data' (2016) 124 TBB Hukuk Dergisi 81, 113

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and genetic data, biometric data for the purpose of uniquely identifying a natural person, data relating to health or data concerning a natural person's sex life or sexual orientation are special categories of data as set out in Article 9(1) of the GDPR. Similarly, Article 6(1) of the PDPL explains that data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data are special categories of personal data. Although the Directive 95/46/EC does not include genetic and biometric data within the scope of personal data of a special nature, it is possible to say that these data are processed under health data of the Directive 95/46/EC and that it does not feel the need to specify separately.

While Article 9(2) of the GDPR details different legal exceptions for each category of special categories of personal data, the PDPL takes a more restrictive approach to the processing of special categories of personal data, providing limited grounds for processing such data.[146]

The PDPL sets out two different situations for the processing of sensitive personal data. In addition to the prohibition of processing sensitive personal data without the explicit consent of the data subject, it is stated that data other than health and sexual life can be processed without consent in cases stipulated by law. In this case, data on health and sexual life can only be processed without explicit consent for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing, by persons or authorised institutions under the obligation of confidentiality. This Article of the PDPL is similar to the preventive or occupational medicine purposes in Article 9(1)(h) of the GDPR. However, since employers are not covered by this exception in the PDPL, they need to obtain consent from data subjects, which causes practical difficulties for employers.[147] Nevertheless, according to the Authority's guidelines, which are similar to the decisions and guidelines of the European Data Protection Board, the validity of

[146] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 51
[147] ibid 52.

consent in employer-employee relationships is questionable, and data subjects have the right to withdraw their consent.[148]

While dress and attire and membership of associations and foundations are considered as special categories of personal data in the PDPL definition, they are not in the GDPR. In the doctrine, there are opinions in the doctrine that since the membership of associations and foundations and clothing preferences may be perceived as a reason for discrimination in Turkey, it is appropriate to consider these as special categories of personal data.[149]

Within the scope of Article 6 of the PDPL, the PDPL regulates the processing of data on health and sexual life within the framework of 'cases stipulated by law'. Even in Article 5 of the PDPL, where the conditions for the processing of non-special categories of data are specified, 'expressly provided for by the laws' is stated as a reason for compliance with the law, although it can be considered as a deficiency that it does not use this expression for special categories of data, it is seen that the preamble of the article refers to the explicit regulation of the law as in Article 5.[150]

Unlike the Directive 95/46/EC and PDPL, the GDPR provides for the appointment of a mandatory data protection officer for the processing of sensitive personal data. Article 37 of the GDPR provides for the appointment of a data protection officer if the processing is carried out in public institutions or organisations, except in the exercise of judicial activity, if the main activities of the controller or processor consist of processing activities that require monitoring of data subjects' data to a large extent, and if the activities of the controller and processor consist of large-scale processing of special categories of data specified in Articles 9 and 10 of the GDPR.[151]

6. Transactions Related to Personal Data

In this section, transactions related to personal data, which are regulated in separate articles in the PDPL, will be discussed, and their relation with the GDPR will be analysed.

[148] Personal Data Protection Authority, Explicit Consent 2017, 7 https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf (03.08.2024).
[149] Sefer Oguz, 'General Principles of Personal Data Protection Law' (2018) 13 Bilgi Ekonomisi ve Yonetim Dergisi 121, 127
[150] Justification of the Personal Data Protection Law 2016, Art. 6.
[151] General Data Protection Regulation, Art. 37(1).

6.1. Deletion, Destruction or Anonymisation of Personal Data

The PDPL regulates the deletion, destruction and anonymisation of personal data in Article 7. In the first sub-article of the Article, it is stipulated that the data processing carried out in accordance with the legal regulations shall be deleted, destroyed or anonymised ex officio or upon request in case the interest required for processing disappears, and in the third sub-article, it is stated that the procedures and principles regarding these transactions shall be regulated by regulation.[152] The erasure and destruction of personal data are regulated in Article 17 of Chapter 3 of the GDPR, which regulates the rights of the data subject. This issue will be discussed separately under the sub-heading 'right to be forgotten', which is analysed under the heading 'rights of the data subject' explained in Chapter 3 of this study.

In the justification of Article 7 of the PDPL, it is explained that erasure means the destruction of data in such a way that they cannot be used or retrieved in any way. In other words, erasure is the transformation of data into a form that cannot be accessed by any alternative means for the relevant users and persons and cannot be used again. In the same justification article, it is stated that the destruction of data refers to the destruction of the materials suitable for storing data in such a way that the data cannot be recovered and used again.[153] For destruction, it is necessary to identify the systems where copies of personal data exist and destroy each of them.[154]

In Article 3 of the PDPL titled 'Definitions', anonymisation is defined as 'rendering personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching with other data'.[155] Thus, the link between personal data and the personal data subject is completely eliminated. There is no definition of data anonymisation in the GDPR and Article 4 titled 'Definitions' does not mention data anonymisation but pseudonymisation. Accordingly, 'pseudonymisation' means 'processing of personal data in such a way that such additional information is kept separately and the personal data can no longer be associated with a specific data subject without the use of the additional information'.[156] Recital 26 of the GDPR states that

[152] Personal Data Protection Law No. 6698, Art. 7.
[153] Justification of the Personal Data Protection Law 2016 Art. 7
[154] Ozan Baris Yilmaz, *Turkiye ve Avrupa Birliği'nde Kisisel Verilerin Korunmasi ve Uygulanacak Hukuk* (1st edn, Adalet Yayınevi 2022) 55
[155] Personal Data Protection Law No. 6698, Art. 3.
[156] General Data Protection Regulation, Art. 4.

‘personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person’.[157] This means that, unlike data anonymisation, pseudonymised data will still be considered personal data under the GDPR.

6.2. Transfer of Personal Data

The GDPR has introduced many reforms regarding the transfer of personal data abroad. As stated many times in the justification of the PDPL, one of the reasons for the entry into force of the PDPL is the transfer of personal data abroad. Although there is no definition of cross-border transfer in both the GDPR, the Directive 95/46/EC and the PDPL, what should be understood by the word cross-border transfer within the scope of the GDPR and the Directive is personal data travelling outside the EU, and within the scope of the PDPL, personal data travelling outside the borders of Turkey. The transfer of personal data outside the borders of Turkey is considered sufficient for cross-border transfer, and transfer to a third party is not required as a condition.

Similarly, the GDPR and PDPL make a binary distinction in transfers abroad. While Article 9 of the PDPL regulates the transfer abroad in cases where the Authority's authorisation is and is not required, Article 45 of the GDPR regulates the cases where the EU Commission's (the Commission) authorisation is required and Article 46 regulates the cases where the Commission's authorisation is not required.

6.2.1. Transfers On the Basis of An Adequacy Decision

In Article 9 of the PDPL, the explicit consent of the data subject is sought as a rule in the transfer of personal data abroad. In the second paragraph, the cases in Articles 5 and 6 of the PDPL are specified and it is ruled that the transfer may be made in the presence of one of these conditions.[158] According to the PDPL, if the conditions set out in Articles 5(2) and 6(3) of the PDPL regarding the processing of personal data are fulfilled, whether the transfer abroad is appropriate is regulated separately for the countries where the Authority recognises that there is adequate protection and for

[157] Recitals of General Data Protection Regulation, Recital 26.
[158] Personal Data Protection Law No. 6698, Art. 9.

others.[159] This distinction is made in order to determine whether the necessary level of protection is provided for the transfer of data abroad.

The Authority shall assess whether a country is safe for the transfer of personal data within the framework of Article 9(4) and shall clearly announce the countries where it assesses that there is adequate protection. Accordingly, the Authority will assess whether there is adequate protection in the foreign country by taking into consideration the international conventions to which Turkey is a party, whether there is reciprocity between the country where the personal data is requested and Turkey in terms of data transfer, the nature of the personal data according to the concrete situation, the purpose and duration of processing, the relevant legal regulations and practices of the country to which the personal data will be transferred, the measures undertaken by the data controller in the country to which the personal data will be transferred, and if necessary, the opinions of the relevant institutions and organisations.[160]

Similar to the PDPL, Article 45 of the GDPR requires a decision of the Commission for transfers abroad. The conditions for the Commission to make an adequacy decision are explained in Article 45 of the GDPR and the Commission will consider whether there are adequate legal arrangements for the protection of personal data in both the public and private sectors, whether there is adequate judicial and administrative redress in case of damage to the data subject as a result of the transfer, and whether there is an adequate supervisory authority for the protection of personal data in the country of transfer.[161] This is intended to ensure that when personal data are transferred from the EU to controllers, processors, other recipients or international organisations in third countries, the level of protection afforded to natural persons by the GDPR is not undermined.[162]

While it is observed that the criteria listed in the PDPL largely overlap with the criteria in Article 45 of the GDPR, the 'reciprocity criterion' has been met with concern by some authors as it raises the question of whether the Member States will be considered as countries with an appropriate level of protection.[163] Considering that the GDPR is a

[159] Berna Akçalı Gür, 'Transborder Flows of Personal Data: An International Law and EU Law Perspective' (2019) 25 Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 850, 868
[160] Personal Data Protection Law No. 6698, Art. 9(4).
[161] General Data Protection Regulation Art. 45
[162] Ljubica Pendaroska, 'International Transfer of Personal Data between the EU and Countries outside the EU' (2022) 13 Iustinianus Primus Law Review 1, 4
[163] Sevde Pelen, 'Transborder Transfer of Personal Data in Turkish Personal Data Protection Law' (2021) 12 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 458, 463

more detailed and advanced piece of legislation than the PDPL, it is unlikely that this outcome will occur. However, due to this reciprocity criterion, key questions are whether Turkey will be recognised as a country with an appropriate level of protection under the GDPR, as well as whether it will prevent the Member States from being recognised as countries with an appropriate level of protection under the PDPL.[164]

6.2.2. Transfers without An Adequacy Decision

Article 9 of the PDPL stipulates that, in the absence of an adequacy decision, personal data shall be subject to the existence of one of the conditions set out in Articles 5 and 6, a written undertaking by the data controller in Turkey and in the relevant country that adequate protection will be provided, and the Authority's authorisation in this regard.[165] In Turkey, it is possible to say that the lawfulness of the transfer of personal data abroad depends more on the compliance with the protection and supervision standards provided by the country where the personal data will be sent and the country where it is obtained.[166]

Article 46 of the GDPR regulates the cases where an adequacy decision is not required for the transfer of personal data, and if a data transfer cannot be carried out on the basis of an adequacy decision, the GDPR authorises the movement of data if the controller or processor provides adequate safeguards.[167] Since the absence of an adequacy decision means that there is no adequate data protection in the third country, appropriate safeguards are intended not to prevent the development of activities connected with the transfer of personal data.[168]

Pursuant to Article 46(2) of the GDPR, a transfer without the requirement of adequacy may be made in the presence a legally binding document, binding corporate rules, standard data protection terms, approved codes of conduct and approved certification mechanism between public authorities and organisations. These binding rules are regulated in Article 47 of the GDPR and there is no provision in the PDPL regulating such binding corporate rules. Considering that binding rules are intended to

[164] ibid 463.
[165] Personal Data Protection Authority, Transfer of Personal Data Abroad 2017 https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20YURTDI%C5%9EINA%20AKTARILMASI.pdf (03.08.2024)
[166] Berna Akçalı Gür, 'Transborder Flows of Personal Data: An International Law and EU Law Perspective' (2019) 25 Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 850, 870
[167] General Data Protection Regulation, Art. 46.
[168] Ljubica Pendaroska, 'International Transfer of Personal Data between the EU and Countries outside the EU' (2022) 13 Iustinianus Primus Law Review 1, 15

facilitate the transfer under certain conditions, especially for large-scale institutions or organisations carrying out joint economic activities, it would be possible to say that the PDPL is incomplete in this regard.

6.3. Exceptional Circumstances in Data Processing

Article 28 of the PDPL regulates the exceptional cases where the PDPL is not applicable or partially applicable. Below, firstly, the subparagraphs of Article 28 of the PDPL will be explained and compared with the similar provisions of the GDPR, if any.

Article 28(1)(a) of the PDPL states that the provisions of the PDPL shall not apply if personal data are processed by natural persons within the scope of activities related to themselves or their family members living in the same dwelling, provided that they are not disclosed to third parties and data security obligations are complied with. Article 2(2)(c) of the GDPR clearly states that the GDPR shall not apply to data processing carried out by a natural person in the course of a purely personal or household activity. Although these two provisions are similar, there are some differences between them. While the term ‘related to themselves’ is used in the PDPL, the term ‘personal’ is used in the GDPR. In addition, while only ‘family members living in the same dwelling’ are included in the scope of the provision in the PDPL, due to the use of term ‘household activities’ in the GDPR, the roommate of the person is not considered an exceptional case according to the PDPL since it is not a family member, but it will be for the GDPR. Thus, it is seen that the wording of the GDPR is more comprehensive and broader.

While Article 28(1)(b) of the PDPL regulates ‘the processing of personal data for purpose such as research, planning and statistics by anonymisation with official statistics’ as an exception, there is no similar provision in the GDPR.

Article 28(1)(c) of the PDPL stipulates that personas data shall not be considered within the scope of the PDPL if they are processed for artistic, historical, literary, or scientific purposes or within the scope of freedom of expression, provided that such processing does not violate national defence, national security, public security, public order, economic security, right to privacy or personal rights or constitute a criminal offence. A similar regulation is also seen in Article 85 of the GDPR. Accordingly, the right to protection of personas data shall be reconciled with the right to freedom of expression and information for journalistic, academic, artistic, or literary purposes.

Another exceptional case regulated in the PDPL is the cases specified in Article 28(1)(ç), where personal data are processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organisations entrusted and authorised by the law ensure national defence, national security, public safety, public order or economic security. A similar provision is regulated in Article 2(2)(b) of the GDPR, and it is stated that these activities are outside the scope of the GDPR by referring to Chapter 2 of Title 5 of the EU Convention.[169]

CHAPTER 3
RIGHTS AND OBLIGATIONS

In this chapter, the rights granted by the GDPR and the PDPL to data subjects and the obligations imposed on data controller will be discussed comparatively. In the first part, since the systematic of the GDPR is more comprehensible and comprehensive, the GDPR will be explained and evaluated in comparison with the scope of the PDPL. In the second part, the obligations of the data controller as regulated in the GDPR and PDPL, along with the cases in which the data controller is released from liability, are explained under separate headings. The similarities and differences between them are also stated. In addition, the amendments introduced by the GDPR on liability data controller and data processor are also mentioned.

1. Rights of Data Subjects

1.1. Right to Information

In accordance with the principle of fairness and transparency, the data subject should be informed about the existence of any processing activities regarding his/her personal data, their legal basis and purposes. The right to be informed is addressed in Article 13 of the GDPR, which includes the information to be provided in cases where personal data is collected from the data subject, and in Article 10 of the PDPL under the title of 'obligation

[169] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 26.10.2012 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M/TXT (05.08.2024).

to inform' of the data controller. According to both legal regulations, from the moment of collection of personal data, there is an obligation to provide information about the identity and contact information of the data controller and, if any, the data protection officer, as well as the purpose of processing the data and the processing activities.

While the GDPR defines the right to information as a right, the PDPL sees it as an obligation for data controllers, but in the end, there is no difference between them.[170]

Information on the intended processing of personal data must be provided to the data subject at the time the data is collected.[171] If the data is not obtained directly from the data subject but from another source, the data subject shall be informed within a reasonable time, depending on the circumstances of the case, within 1 month at the latest. Articles 13 and 14 of the GDPR are parallel to each other and Article 14 mentions the information to be provided in cases where personal data is not received from the data subject.

As a result, while the GDPR regulates the right to information in detail, such as how and within what period of time the information should be provided, the PDPL is limited to specifying the subjects to be informed and explaining what the obligations of the data controller are.

1.2. Right of Access

The right of access applies to data controllers carrying out data processing and obliges data controllers to provide individuals with access to their data and to provide them with the additional information envisaged in relation to the processing.[172] While the right of access regulated under Article 15 of the GDPR covers a wide range of issues, including the purposes of processing, objection to processing, rectification or erasure, and filing a complaint to the supervisory authority, the right of access regulated under Article 11 of the PDPL is more limited compared to the GDPR.

[170] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 52
[171] General Data Protection Regulation, Art. 13.
[172] Ozan Baris Yilmaz, *Turkiye ve Avrupa Birliği'nde Kisisel Verilerin Korunmasi ve Uygulanacak Hukuk* (1st edn, Adalet Yayınevi 2022) 90

Although it is possible to say that the right of access and the right to information are intertwined, it is accepted that the right to information precedes the transaction, whereas the right of access comes into play after the transaction has taken place.[173]

Pursuant to the right of access in the GDPR, the controller must provide the data subject with a copy of the personal data undergoing processing and any information provided must be understandable.[174] Since the PDPL explicitly includes the phrase 'to request information if personal data has been processed' instead of the phrase 'right of access', it is open to debate whether it includes the obligation to provide a copy of the processing activities. However, in addition, the explicit recognition in Article 20 of the Constitution of the right of every individual to access personal data should be interpreted in such a way that 'access' is constitutionally guaranteed and data subjects can request a copy from controllers.[175]

1.3. Right to Rectification

Article 16 of the GDPR states that 'the data subject shall have the right to request the controller to rectify, without undue delay, inaccurate personal data concerning him or her'. The right to rectification is closely linked to the controller's obligation under Article 5(1)(d) GDPR to take all reasonable steps to ensure that personal data are accurate. Similarly, Article 11(1)(d) of the PDPL provides that 'the data subject may request rectification of inaccurate or incomplete personal data'. This is in line with the principle laid down in Article 4(2)(b) of the PDPL that the processing of personal data shall be accurate and, where necessary, up-to-date.

Since the right to rectification re-establishes a lawful data processing situation, data subjects are not obliged to state the grounds for their requests when exercising this right.[176] However, since data subjects have the burden of proving inaccurate or

[173] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 56
[174] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 154
[175]Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 56
[176] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 154

incomplete personal data, they are required to attach supporting documents to their requests under this right.[177]

1.4. Right to be Forgotten (Right to Erasure)

In Article 17 of the GDPR, the conditions under which personal data should be deleted are explained in detail and regulated. Accordingly; if there is no purpose for the data controller to retain the data, if the data subject has withdrawn his/her consent for the processing of his/her personal data, if the data controller has no legitimate interest to process the personal data or if there is an unlawful processing or if the personal data must be deleted in order to fulfil the obligations arising from legal obligation, the data controller must delete the personal data of the data subject without delay.[178] There are opinions that the right to erasure exists only in the presence of certain circumstances such as unlawful processing or no longer necessary for the purpose of processing, while the right to be forgotten exists without such limitation, and although there is a debate in the doctrine as to whether the 'right to be forgotten' and the 'right to be erased' are the same concepts, Article 17 of the GDPR calls this right 'the right to request erasure (right to be forgotten)'.[179]

The right to erasure is not regulated in the PDPL in as much detail as in the GDPR, and Article 11(e) of the PDPL states that data processing carried out in accordance with legal regulations may be deleted ex officio or upon request if the interest required for processing disappears.

The right to be forgotten is not an absolute right and needs to be balanced with other rights, such as the right to information.[180] As seen in Article 17 in the GDPR, the rights and responsibilities of the controller are not absolute and, as with other rights in the GDPR, there are various grounds justifying the restriction of the right to erasure.[181] With regard to legitimate interest, the approach of the GDPR will apply similarly to the PDPL.

[177] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 154
[178] General Data Protection Regulation, Art. 17.
[179] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 157
[180] Michael Douglas, 'Questioning the Right to Be Forgotten' (2015) 40 Alternative Law Journal 109, 109
[181] Christopher Kuner & Lee A. Bygrave & Christopher Docksey (ed), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020) 477

If a controller does not have an overriding and balanced interest, the processing is considered unlawful and requires erasure ex officio or at the request of data subjects.[182]

1.5. Right to Restriction of Processing

The right to restriction of processing set out in Article 18 of the GDPR aims to strike a balance between the data subject's interest in having his or her data rectified or erased and the controller's interest in continuing to process that data.[183]

The relevant article enumerates the circumstances under which a restriction may be requested. Accordingly, if the accuracy of the personal data is contested by the data subject, it may be restricted for a period of time enabling the data subject to confirm the accuracy of the personal data. In addition, data use may be restricted if the processing is unlawful and the data subject objects to the erasure of the personal data and requests restriction of the use of the data instead. On the other hand, the controller may request the restriction of the use of personal data if the controller no longer has a need for the personal data but the data subject needs the personal data for legal reasons. Finally, the use of data may be restricted if the data subject objects to the processing until it is verified whether the legitimate grounds of the data controller outweigh the legitimate grounds of the data subject.[184] In addition, subsection 3 of the same Article provides that the controller has an obligation to inform the data subject prior to the lifting of a restriction on a data processing activity.[185]

Looking at the PDPL, there is no provision similar to the right of data subjects to restrict processing regulated in the GDPR. Considering that the right to restrict processing is of great importance in terms of strengthening the control of data subjects over their personal data, the absence of such a provision in the PDPL can be said to be a deficiency.[186] Although it can be reconciled with the principle of retention of personal data for a reasonable period of time within the scope of the purpose for which they are

[182] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 57
[183] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 164
[184] General Data Protection Regulation, Art. 18(1).
[185] General Data Protection Regulation, Art. 18(3).
[186] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 57

processed as set out in Article 4(2)(d) of the PDPL, it is not possible to say that it is fully equivalent to Article 18 of the GDPR.

1.6. Right to Request Notification

Article 19 of the GDPR contains a section on the notification obligation regarding rectification, erasure or restriction. Accordingly, the controller shall communicate the rectification or erasure of personal data or the restriction of processing carried out pursuant to Articles 16, 17(1) and 18 to each recipient to whom the personal data have been disclosed, unless it can be demonstrated that this is impossible or involves disproportionate effort.[187] Although this provision is generally related to the obligation of data controllers rather than the rights of the data subject, it is regulated in the section on the rights of the data subject, taking into account the relevant articles.

Article 11(1)(f) of the PDPL stipulates that third parties to whom personal data are transferred may request notification of the actions taken pursuant to paragraphs (d) and (e) of the same Article.[188] The PDPL does not contain a provision confirming that the notification obligation will continue unless it requires a disproportionate effort similar to that in the GDPR, and makes this obligation mandatory for controllers subject to the PDPL.[189] Where controllers subject to the PDPL receive notification requests that require disproportionate effort, they may need to rely on general legal principles, such as abuse of a right or breach of good faith.[190]

1.7. Right to Data Portability

The right to data portability is not included in the PDPL and the Directive 95/46/EC but is regulated for the first time in the GDPR. This right, set out in Article 20 of the GDPR, will enable the data subject to transfer his/her personal data from one controller to another, thereby strengthening the data subject's control over his/her data where the processing is

[187] General Data Protection Regulation, Art. 19.
[188] Personal Data Protection Law No. 6698, Art. 11(1)(f).
[189] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 58
[190] ibid 58.

carried out by automated means.[191] This right allows to data subjects to change their service providers as simply as possible.[192]

The right to data portability and the right of access to data have similarities and it would be correct to see the right to data portability as an advanced version of the right of access.[193] This is because the right to data portability allows not only access to data, but also to transmit them to other controllers in appropriate format.

Furthermore, the right to data portability will strengthen competition between controllers in favour of data subjects and encourage the development of data formats that respect consumer protection and privacy.[194]

As a result, considering that this right provides more control and benefits to data subjects, it would be possible to say that it is a deficiency that the PDPL does not include this right.

1.8. Right to Object

Pursuant to Article 21 of the GDPR, the data subject may object at any time to the processing of personal data concerning him or her on grounds relating to his or her particular situation, where the legal basis for the processing is the performance of a task carried out in the public interest or the legitimate interests of the controller.

Furthermore, since the GDPR states that the burden of proof regarding the existence of legitimate ground for processing is on the data controller, it will not be possible for the data controller to continue processing data if it cannot prove the necessity of continuation of the processing activities.[195] In addition, as the collection of personal data for the purpose of direct marketing may pose a threat to the privacy of the data subject, Article 21(2) of the GDPR provides data subjects an absolute right to object to marketing.

---

[191] General Data Protection Regulation, Art. 20.
[192] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 168
[193] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 58
[194] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 169
[195] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 159

The right to object is very important as it strikes a balance between data protection rights and the legitimate interests of other persons and strengthens the legality of data controllers by forcing them to carefully consider data processing activities based on legitimate interests.[196]

This right is not regulated under the PDPL. Considering that this right is designed to protect data subjects from online profiling activities and to increase privacy, it would not be wrong to say that the absence of this right in the PDPL puts data subjects in a disadvantageous position.[197]

1.9. The Right Not to Be Subject to Solely Automated Decisions

Article 22(1) of the GDPR provides that the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which has legal consequences for him/her. However, this right is not absolute, as Article 22(2) provides for exceptions. Since the inclusion of human intervention in decision-making mechanism is important to prevent negative consequences that may otherwise arise, this provision ensures that individuals are protected from the consequences of decisions based on automated processing and can request human intervention when necessary.[198]

The right of data subjects to object to the results of decisions based on automated processing is regulated in Article 11(1)(g) of the PDPL, and although it can be said thar this article is similar to Article 22 of the GDPR, these two provisions differ in scope. While Article 22 of the GDPR regulates only the right not to be subjected to automated decisions, Article 11(1)(g) of the PDPL recognises the right to object to such processing.[199]

[196] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 59
[197] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 59
[198] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 160
[199] Adife Gul Evren, 'A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects' (2023) 5 Kişisel Verileri Koruma Dergisi 39, 59

2. Obligations of Data Controllers

2.1. Obligations of the Data Controller under the GDPR

The organisational data protection obligations for data controllers and processors are set out in Articles 24 to 31 of the GDPR. These articles largely repeat the obligations already existing in the Directive 95/46/EC.[200] However, some new requirements have also been introduced, such as the keeping of Data Processing Records.

Article 24 of the GDPR is a general rule and sets out the general obligations of data controllers and emphasises that the controller must take appropriate technical and organisational measures for any personal data processing activities carried out by it or its behalf. The measures taken must be regularly reviewed and updated as necessary.[201]

With Article 24 of the GDPR, it is possible to say that it is aimed to expand the area of responsibility with a general regulation in cases where the special provisions regulated in the following articles are not sufficient.

Article 25 of the GDPR stipulates that the controller is obliged to ensure the protection of the rights of data subjects by taking appropriate technical and organisational measures to integrate the necessary safeguards for the effective implementation of the data protection principles and the fulfilment of the requirements of the GDPR. While Article 24 deals with the general risk assessment and the implementation of safeguards, Article 25 states in particular that the application of the data protection principles and appropriate measures for the protection of data must be effectively implemented at specific points in a project.[202]

The term 'joint controller' regulated in Article 26 of the GDPR is one of the important innovations introduces by the GDPR.[203] The relevant article clearly states that 'where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers'.[204]

---

[200] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 33
[201] General Data Protection Regulation, Art. 24(1).
[202] Rosemary Jay, *Guide to the General Data Protection Regulation* (1st edn, Sweet & Maxwell 2017) 177
[203] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 91
[204] General Data Protection Regulation, Art. 26.

Although Article 26 of the GDPR does not stipulate that the liability determination agreement between joint controllers must be in writing, it would be beneficial for the parties to record the nature and scope of their respective responsibilities in terms of transparency, clarity, determination of liability and proof.[205] In fact, Recital 79 also states that this determination should be made in a manner that allows a clear determination of responsibility.

As stated above, although the explanations regarding the regulations of the PDPL on obligations of the data controller will be made under the following heading. Interestingly, here is no separate regulation in the PDPL regarding joint data liability and that under Turkish law, joint controllers are jointly liable under the Turkish Code of Obligations No. 6098.

In Article 27 of the GDPR, in parallel with Article 3(2) of the GDPR stipulating that the GDPR shall apply to the processing of data of persons in the EU, even if the data controller or processor is not located in the EU, it is regulated that the controller or processor must appoint a representative in writing within the EU. Thus, even if the controller or processor are located outside the EU, the GDPR will be applicable as long as the data subjects is within the EU. The purpose of appointing a representative is to ensure that EU data subjects have an easily accessible presence to exercise their rights, as well as to assist the controller and processor to comply with the GDPR.[206]

The representative controller or processor must be expressly designated by a written authorisation to act on behalf of the controller or processor in relation to the GDPR obligations and the representative may only act within the scope of that authorisation.[207]

Article 27(2) refers to the exceptions to Article 27(1) and provides that, where processing is rare and does not involve large-scale processing of sensitive personal data, the appointment of a representative shall not be required unless the processing is likely to cause a risk to the rights and freedoms of natural persons, and where the relevant processing is carried out by a public organisation or body, it shall not be necessary for that organisation or body to appoint a representative within the EU.[208]

[205] Rosemary Jay, *Guide to the General Data Protection Regulation* (1st edn, Sweet & Maxwell 2017) 179
[206] Laura L Keogh, *Data Protection Compliance A guide to GDPR and Irish Data Protection Law* (1st edn, Clarus Press Ltd) 205
[207] Recitals of General Data Protection Regulation, Recital 80.
[208] General Data Protection Regulation, Art. 27(2).

Article 28 of the GDPR regulates the data processor, according to which, if the controller involves a processor, it must appoint an appropriate processor to ensure a high level of data protection. Before selecting a particular processor, the controller is obligated to assess whether that processor provides appropriate technical and organisational data protection measures and to monitor whether these measures are maintained.[209] The processor must act in accordance with the instructions of the controller and must obtain authorisation from the controller if the processor will use another processor.[210]

Pursuant to Article 28(3) of the GDPR, both parties must conclude a contract or other legal arrangement in order for the processor to undertake to fulfil the conditions set by the controller, the contract must be concluded in writing, including in electronic form.[211] In the absence of such a contract the processor cannot process the personal data and the controller cannot transfer the data to processor.[212] Another important aspect of Article 28 is that where the processor determines how and why the processing is carried out, the processor shall be deemed to be the controller for the purposes of the processing concerned and shall have the obligations and responsibilities of a controller, as set out in Article 28(10).

Article 30 of the GDPR regulates the keeping of records of personal data processing activities. Accordingly, 'each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility'. These records shall include explanations such as the name and contact details of the controller, data protection officer, purposes of data processing, data subjects and categories of personal data, recipients, data transfers, time limits for erasure of data.[213]

Article 30(5) limits the obliged persons to keep records and accordingly, for a business or organisation employing less than 250 persons, there is no obligation to keep records of processing activities unless it processes personal data of a special nature or is likely to cause a risk to the rights and freedoms of data subjects.

While Article 30 states that supervisory authorities should be assisted where necessary, Article 31 of the GDPR also states the obligation to cooperate with supervisory authorities.

---

[209] Paul Vogit & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing) 81
[210] General Data Protection Regulation, Art. 28(2).
[211] General Data Protection Regulation, Art. 28(9).
[212] Laura L Keogh, *Data Protection Compliance A guide to GDPR and Irish Data Protection Law* (1st edn, Clarus Press Ltd) 151
[213] General Data Protection Regulation, Art. 30(1).

Article 32 of the GDPR states that the controller and processor must implement appropriate technical and organisational measures to ensure the security of the processing of data. According to this Article, when taking the necessary measures, the controller and processor shall take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons.[214]

Pursuant to Article 33 of the GDPR, in the event of a personal data breach, if the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the controller is obliged to notify the supervisory authority of the persona data breach within 72 hours at the latest from the moment it becomes aware of the breach, and if the notification is not made within 72 hours, the reasons for the delay must be included in the notification. In the continuation of the same article, it is stated that the processor must also notify the controller immediately upon becoming aware of the security breach.[215] Article 33(3) sets out the minimum information that should be included in the notification and further information may be provided where appropriate.[216]

Article 34 of the GDPR states that 'where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is obliged to notify the data subject of the personal data breach without delay'. This notification should explain the nature of the personas data breach in clear and plain language and include information similar to that in the notification to the supervisory authority.[217] If the notification would require disproportionate effort, the controller cannot be expected to provide such notification and the data subject may be informed of the breach by other means, such as public notification.[218]

Article 35 of the GDPR imposes an obligation on the controller to carry out an assessment of the impact of the processing on the protection of personal data prior to the processing, where the processing is 'likely to result in a high risk to the rights and freedoms of natural persons'. Accordingly, data controllers must assess the purposes, necessity and proportionality of data processing, as well as the potential risks to the rights

[214] General Data Protection Regulation, Art. 32(1).
[215] General Data Protection Regulation, Art. 33(2).
[216] Laura L Keogh, *Data Protection Compliance A guide to GDPR and Irish Data Protection Law* (1st edn, Clarus Press Ltd) 138
[217] General Data Protection Regulation, Art. 34(2).
[218] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 125

of individuals.[219] The assessment enhances the risk-based approach to data protection by forcing the assessment of high risks before data processing begins, thus enabling controllers to prepare for any risk.[220]

Article 36 of the GDPR imposes an obligation on the controller to consult and obtain the prior opinion of the supervisory authority before processing, if a data protection impact assessment under Article 35 concludes that the processing constitutes a risk and is likely to infringe the rights and freedoms of natural persons.

Article 37 to 39 of the GDPR provide that in certain circumstances a data protection officer may be appointed to deal with matters relating to the protection of personal data. Accordingly, a data protection officer must be appointed if the data processing is carried out by public authorities or bodies, except courts acting in a judicial capacity; if the processing of personal data requiring regular and systematic monitoring of data subjects on a large scale is a core activity of the organisation; or if the organisation processes special categories of personal data or personal data relating to criminal convictions on a large scale.[221]

The data protection officer is responsible for ensuring compliance with data protection laws and has duties such as providing information and advice to controller or processors and the employees carrying out processing activities within the scope of the GDPR and the data protection law of the Member States, auditing compliance with policies on the protection of personal data, co-operating with the supervisory and, where necessary, obtaining opinions.[222]

Where a data protection officer has been appointed, the controller and the processor are obliged to ensure that the data protection officer is involved in all matters relating to the protection of personal data in an appropriate and timely manner and may not dismiss or penalise the data protection officer for the performance of his or her duties.[223]

2.2. Obligations of the Data Controller under the PDPL

[219] General Data Protection Regulation, Art. 35(7).
[220] Laura L Keogh, *Data Protection Compliance A guide to GDPR and Irish Data Protection Law* (1st edn, Clarus Press Ltd) 119
[221] General Data Protection Regulation, Art. 37(1).
[222] General Data Protection Regulation, Art. 39.
[223] General Data Protection Regulation, Art. 38.

The information to be provided to the data subject within the scope of obligation to inform is important both for the data subject to take control of his/her data and for the data controller to process data in accordance with the general principles.[224] Within the scope of the obligation regulated in Article 10 of the PDPL; the data controller or the person authorised by the data controller is obliged to inform the data subject about the identity of the data controller and its representative, if any, the purpose of data processing, to whom and for what purpose the data may be transferred, the method and legal grounds for data collection and other rights listed in Article 11. As stated in the justification of Article 10, the data controller's obligation to inform is regulated in parallel with the Directive 95/46/EC.

The first paragraph of Article 12 of the PDPL regulates the obligation to take measures in general. Accordingly, the data controller is obliged to take all necessary technical and administrative measures to ensure an appropriate level of security in order to prevent unlawful processing and access to personal data to ensure the preservation of personal data. As mentioned before, while Article 32 of the GDPR regulates the technical and administrative measures that may be taken and explains in detail Recital 83, Article 12(1) of the PDPL is expressed in a general manner and does not include any details and explanations regarding technical and administrative measures. In the doctrine, there are opinions arguing that this issue should not be interpreted as incomplete, but as a result of the PDPL being a general law.[225] In addition, this regulation is detailed in the 'Personal Data Security Guide' published by the Authority and the technical and administrative measures that can be taken to ensure data security are specified.[226]

Article 12(2) of the PDPL states that if personal data are processed by another natural or legal person on his/her behalf, the data controller shall be jointly responsible with such persons for taking the measures specified in the first paragraph. While Article 28 of the GDPR states that the controller must act prudently when selecting the processor, Article 12(2) of the PDPL indirectly imposes an obligation in selecting the data processor and regulates jointly liability in case the rights and freedoms of the data subject are damaged. Since there is no explicit provision in the PDPL on the qualifications of the

[224] Sehriban Ipek Asıkoglu, 'Information Obligation of Data Controllers In European Law and Turkish Law' (2019) 1 Kisisel Verileri Koruma Dergisi 41, 42
[225] Zehra Yuruk, 'Liability of The Data Controller to Take Administrative and Technical Measures Regarding Data Security' (2023) 22 İstanbul Ticaret Universitesi Sosyal Bilimler Dergisi 899, 905
[226] Personal Data Security Guide (Technical and Administrative Measures). https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf (03.08.2024).

data processor, the data controller is required to make inquiries about the relevant person and organisation and ensure that data security is provided at least at the level provided by them.[227]

Article 12(3) of the PDPL imposes an obligation on the data controller to carry out or have carried out the necessary audits in order to ensure the implementation of the provisions of the PDPL.

Article 12(4) of the PDPL imposes an indefinite confidentiality obligation on data controllers and data processors, according to which data controllers and data processors may not disclose the personal data they have learnt to others in violation of the provisions of the PDPL and may not use them for purposes other than processing. Since this article stipulates that this obligation will continue after their resignation, an indefinite confidentiality obligation is mentioned in this article. Although there is no article directly regulating the confidentiality obligation in the GDPR, Article 32 of the GDPR mentions the obligation of the controller regarding the confidentiality of the technical systems of the processing.

Pursuant to Article 12(5) of the PDPL, in the event that personal data are unlawfully obtained by others, the data controller is obliged to notify the Authority and the data subject as soon as possible. Although it can be said that this article is in parallel with Article 33 and 34 of the GDPR, the PDPL does not address the issues such as the latest period within which the notification shall be made and the nature, scope and content of the notification.

As a result, since both the PDPL and the GDPR expect the data controller to take 'necessary' measures, the data controller may be relieved from liability if it takes the necessary measures. In this framework, it would not be wrong to say that the data controller has a duty of care in a sense. In this context, the difference between the GDPR and the PDPL is that while the content of the obligation to 'take necessary measures' is explained in detail in the GDPR, the PDPL fails to fill the content of this provision.

Another important point is that while there was a binary distinction between data controllers and data processors terms of their responsibilities in the Directive 95/46/EC, the GDPR has eliminated this distinction.

[227] Zehra Yuruk, 'Liability of The Data Controller to Take Administrative and Technical Measures Regarding Data Security' (2023) 22 İstanbul Ticaret Universitesi Sosyal Bilimler Dergisi 899, 911

CHAPTER 4
THE MEANS OF PROTECTION OF PERSONAL DATA

In this chapter, the methods foreseen for the protection of personal data under the GDPR and the PDPL will be examined comparatively. I will discuss the legal remedies, administrative procedures, criminal sanctions, and general regulations that data subject can apply to protect their rights. In addition, the provisions of the PDPL and the GDPR regarding the supervisory mechanisms, the role of data protection authorities, and their sanctioning powers will be compared, highlighting their shortcomings and strengths.

1. Protection by Application to the Data Controller

Application to the data controller is a right granted to the data subject by Article 13 of the PDPL. Accordingly, the data subject may submit his/her request regarding the implementation of the provisions of the PDPL to the data controller in writing or by other methods to be determined by the Authority. In the PDPL, the general framework of the right to apply to the data controller is outlined, and the issues of how to make this application and in which cases a fee may be requested are left to the decision of the Authority.[228] Therefore, the procedures and principles other than the written application of the data subject are specified in the 'Notification on the Procedures and Principles of Application to the Data Controller' published by the Authority on 10 March 2018.[229]

In Article 13, it is also stated that the data controller shall finalise the request in the application free of charge as soon as possible and within thirty days as latest, and if the transaction requires an additional cost, the fee in the tariff determined by the Authority may be charged.[230] Article 13(3) states that the data controller may accept the request of the data subject or reject it with justification, and in case of acceptance, it is stated that the data controller must refund the costs incurred for the application.

The GDPR also has regulations parallel to the PDPL. In Article 12 of the GDPR, it is stated that the data subject may apply to the controller in accordance with the principle of transparency and it is regulated that the controller must respond to the application

[228] Personal Data Protection Law No. 6698, Art. 13(1).
[229] Notification on the Procedures and Principles of Application to the Data Controller No. 30356 https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm (24.07.2024).
[230] Personal Data Protection Law No. 6698, Art. 13(2).

within one month as in the PDPL. Since it is stated in the relevant article that possibility of the data subject to apply to the controller is for cases arising from the situations within the scope of Article 13 to 22 and Article 34, it can be said that the relevant provision of the GDPR is more concrete and restrictive compared to PDPL.

However, while many issues regarding the application to the data controller are regulated in the GDPR, the notification published by the Authority is taken as basis in the PDPL, and therefore the details regarding this issue are regulated by a lower legal norm.

2. Protection by Administrative Sanctions

Article 14 of the PDPL stipulates that in cases where the application made pursuant to Article 13 is rejected, the response is deemed inadequate, or the application is not responded in due time, the data subject may file a complaint to the Authority within thirty days from the date of learning the response of the data controller and in any case within sixty days from the date of application. The relevant article states that the application specified in Article 13 must be made before filing a complaint the Authority.[231] It is aimed to prevent the Authority from facing an intensive workload by requiring that the remedy of application to the data controller must have duly exhausted before a complaint application can be made to the Authority and a complaint cannot be filed without exhausting this remedy.[232]

Article 15 of the PDPL regulates in detail the procedures and principles of the examination to conducted by the Authority upon a complaint or ex officio upon learning of the alleged infringement. While a period of sixty days is stipulated for the Authority's examination upon a complaint, no period is stipulated for ex officio examinations.

Article 15(7) of the PDPL authorises the Authority to suspend the processing of data or the transfer of data abroad in the event of irreparable or irreparable damage and in the event of a clear violation of the law. Although it is not explicitly stated in the text of the article, it is inferred that this decision is an injunction.[233]

Article 77 of the GDPR provides in particular that if the data subject considers that the processing of personal data concerning him or her is contrary to the GDPR, he or

[231] Personal Data Protection Law No. 6698, Art. 14(2).
[232] Justification of the Personal Data Protection Law 2016, Art.14.
[233] Samet Saygı, 'Judicial Remedies in the Systematics of Law No. 6698' (2020) 2 Kisiel Verileri Koruma Dergisi 30, 44

she may lodge a complaint with a supervisory authority in the Member State of his or her habitual residence, place of work or place of the alleged infringement. Unlike the PDPL, the GDPR does not regulate the prerequisite of application to the data controller, nor does it provide that the supervisory authority may act ex officio.

Pursuant to Article 78 of the GDPR, once the supervisory authority has issued a decision on a complaint, every natural or legal person has the right to an effective remedy against legally binding decisions of that supervisory authority concerning them. This right applies to data subjects as well as controller and processors.[234]

Article 18 of the PDPL regulates misdemeanours regarding personal data, and the Authority will impose an administrative fine on the data controller if it decides that the misdemeanours listed under this article have occurred. These misdemeanours are; failure to fulfil the obligation to disclose, failure to fulfil the obligations regarding data security, failure to fulfil the decisions made by the Authority, violation of the obligation to register and notify the 'Data Controllers Registry' and the notification obligation stipulated in Article 9(5).[235] Although the Authority is obliged to impose an administrative fine in the event that it determines a misdemeanour, Article 18 does not stipulate in which cases the administrative fines may be imposed at the lower limit and in which cases at the upper limit, and the Authority is given discretionary power to determine the amount of the fine to be imposed between certain amounts.[236] In the justification of Article 18, it is stated that the unjust content of the mis demeanour, the fault and the economic situation of the perpetrator will be taken into consideration when determining the fine, and the amount of administrative fines to be determined in the event that a family company operating in a small city and a holding company operating nationwide violate the provisions of the PDPL will be different according to the economic situation of the companies in question.[237]

It is also stated in the justification of the same article that administrative fines will only be imposed on private legal entities and natural persons who are data controllers, the Authority cannot impose administrative fines on public legal entities, and if the data

[234] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 162
[235] Personal Data Protection Law No. 6698, Art. 18(1).
[236] Samet Saygı, 'Judicial Remedies in the Systematics of Law No. 6698' (2020) 2 Kisiel Verileri Koruma Dergisi 30, 48
[237] Justification of the Personal Data Protection Law 2016, Art.18.

controller is a public institution, disciplinary provisions regarding public officials who are responsible for the violation will be applied.

In addition, Article 18(3) stipulates that administrative fines imposed by the Board may be sued before the administrative courts.

Article 83 of the GDPR regulates in detail the determination of the amount of fines that the supervisory authority may impose. Article 83(2) explains in detail what the supervisory authority should take into account when deciding whether to impose an administrative fine and the amount of the administrative fine. Therefore, it is seen that the administrative fines regulated under Article 83 of the GDPR are broader in terms of type and quantity than the fines regulated under Article 18 of the PDPL. The GDPR also extends the scope of liability and increases the fines that can be imposed compared to the Directive 95/46/EC.[238]

Pursuant to Article 18(5), for infringements of data subjects' rights and non-compliance with the GDPR rules on data transfer abroad, supervisory authorities are authorised to impose administrative fines of up to EUR 20,000,000 or, if the controller or processor is an undertaking, up to 4% of its annual worldwide turnover for the preceding financial year. For other infringements, the supervisory authority may impose an administrative fine of up to EUR 10,000,000 or, if the controller or processor is an undertaking, up to 2% of its annual worldwide turnover for the preceding financial year.[239] The imposition of a fine based on the turnover of the undertaking is equitable and the PDPL does not provide for fines based on turnover.

3. Protection by Criminal Sanctions

Article 17 of the PDPL states that the provisions of Articles 135 to 140 of the Code No. 5237 shall apply to offences related to personal data. Thus, by referring to the Code No. 5237, a direct link has been established between the PDPL and the specified articles of the Code No. 5237.[240] Article 135 of the Code No. 5237 regulates the offence of recording personal data, Article 136 regulates the offence of unlawful provision and seizure of data,

[238] Murat Volkan Dulger, 'Protection of Personal Data in the Context of The European Union General Data Protection Regulation' (2019) 1 Yasar Hukuk Dergisi 71, 167
[239] General Data Protection Regulation, Art. 83(4).
[240] Murat Volkan Dulger, 'Protection of Personal Data with Criminal Norms in the context of Protection of Personal Data Law and Turkish Criminal Code' (2016) Istanbul Medipol Universitesi Hukuk Fakultesi Dergisi 101, 120

Article 137 regulates the qualified forms of the offences defies in Articles 135 and 136, Article 138 regulates the offence of destruction of data, Article 139 explains in which cases these offences will be considered within the scope of offences subject to complain and Article 140 explains the application of security measures on legal entities within the scope of these offences.

Article of the GDPR merely states that penalties for offences arising from the infringement of personal data must effective, proportionate and dissuasive, and allows the Member States to lay down rules for criminal sanctions for infringements of the provisions of the GDPR. Accordingly, the Member States may lay down rules on the imposition of penalties for infringements of the GDPR and local regulations adopted pursuant to the GDPR.[241] However, Recital 149 of the GDPR emphasises that national law may not punish data controllers and/or data processors twice for the same offence, in other words, it must not violate the principle of 'ne bis in idem'.[242]

4. Protection by the Facilities in General Regulations

Article 14(3) of the PDPL stipulates that persons whose personal rights have been infringed have the rights to claim compensation for such damage in accordance with the general provisions. The fact that Article 14 of the PDPL regulating the complaint to the Authority stipulates that compensation claims for violation of personal rights are reserved according to general provisions has raised the question of whether the previously mentioned station that the application to the data controller is mandatory for the complaint application is also a prerequisite for the application to the general provisions.[243] The general view in this regard is that such a precondition would be contrary to the purpose of the PDPL and that the PDPL does not limit or postpone the already existing litigation possibilities and rights of recourse and compensation under Turkish Civil Code No. 4721 and the Turkish Code of Obligations No. 6098.[244] Furthermore, in the 'Implementation Guide on the Law on the Protection of Personal Data', it is stated that the application and

[241] Recitals of General Data Protection Regulation, Recital 149.
[242] Laura L Keogh, *Data Protection Compliance A guide to GDPR and Irish Data Protection Law* (1st edn, Clarus Press Ltd) 227
[243] Samet Saygı, 'Judicial Remedies in the Systematics of Law No. 6698' (2020) 2 Kisiel Verileri Koruma Dergisi 30, 33
[244] ibid 35.

litigation remedies available under the general provisions can be used at every stage.[245] However, it should be noted that this guidance text is only a guiding text and is not binding.[246] Therefore, necessary arrangements should be made to eliminate the ambiguities in the PDPL and its justification.

Data subjects may file a lawsuit based on different types of liability pursuant to Article 25 of the Code No. 4721 in order to compensate for the damages suffered in cases such as breach of confidentiality or unlawful processing of personal data.[247] In addition, according to Article 25 of the Code No. 4721, in event of an attack on personal data, the data subject may request the prevention of the attack, the termination of the attack, and the determination of the illegality of the attack on personal data even if the attack has cased.

Article 79 of the GDPR stipulates that data subjects may take legal remedies due to transactions contrary to the GDPR. In Article 82 of the GDPR, it is regulated that any person who suffers material or moral damage as a result of a breach of the provisions of the GDPR has the right to compensation from the data controller or processor for the damage suffered. In Recital 146, it is stated that the concept of damage is to be interpreted broadly in the light of the case law of the Court of Justice, so as to fully reflect the objectives of the GDPR.

Article 82(2) provides that each data controller involved in the processing is liable for the damage caused, whereas the processor is only liable for the damage caused by the processing if he or she has acted contrary to the obligations of the GDPR specifically for data processors or has acted outside or contrary to the lawful instruction of the data controller.

Article 82(3) provides that in order to be exempt from compensation obligations, the controller or processor must prove that they are not in any way responsible for the processing that caused the damage.

Article 82(4) provides that where more than once controller or processor, or both a controller and a processor, engage in the same processing and are responsible for any damage caused by that processing, each controller or processor shall be held liable for the

[245] Personal Data Protection Authority, Implementation Guide on the Law on the Protection of Personal Data 2020, 104
[246] Samet Saygı, 'Judicial Remedies in the Systematics of Law No. 6698' (2020) 2 Kisiel Verileri Koruma Dergisi 30, 35
[247] ibid 37.

full amount of the damage. such a provision is introduced in order to ensure effective compensation of the data subject.

As a result, it is seen that Article 82 of the GDPR contains more detailed regulations on the subject when compared to the PDPL.[248]

CONCLUSION

With the GDPR, the aim is to address the current needs in the field of personal data protection under European law and to take into account future developments. In order to ensure uniformity in the protection of personal data in the EU, the GDPR has established a more comprehensive and detailed framework compared to the previous regulations and introduced serious sanctions in case of non-compliance with the rules.

In Turkey, although there were regulations on the protection of personal data in many legal texts, with the amendment of Article 20 of the Constitution made in 2010, the right to protect personal data was placed on a constitutional basis., during the periods when there was no framework law in Turkey, efforts were made to address the necessary regulations in the Constitution, regulations issued in accordance with the Constitution, and other articles of law. with the entry into force of the PDPL, a comprehensive and inclusive law was obtained. It is seen that the provisions of the Directive 95/46/EC, which was in force at that time, were taken as basis in the construction of the PDPL, not the provisions of the GDPR.

A comparison of the GDPR and the PDPL in terms of the basic principles of data processing reveals a great deal of harmonisation. Although some principles are not explicitly stated in the PDPL, it is understood that these principles are implicitly recognised by the provisions of the law and the guidance of the Authority.

In terms of the rights of data subjects, especially the lack of the right to object, the right to restriction of processing and the right to data portability, and the fact that the right to request a copy within the framework of the right of access is not clearly defined, shows that the PDPL offers more limited rights than the GDPR and creates a situation to the detriment of data subjects.

[248] Emel Badur & Nesibe Kurt Konca, 'Compensation for Damages Arising from The Unlawful Processing of Personal Data and The Authorized Court' (2022) I13 nonu Universitesi Hukuk Fakultesi Dergisi 476, 483

Regarding the regulations related to the obligations of the data controller, while the technical and administrative measures to be taken by the data controller are regulated in detail in the GDPR, there are no details and explanations in the PDPL, but they are set out in the guide published by the Authority.

With the entry into force of the PDPL, there is no doubt that many deficiencies in terms of the protection of personal data have been eliminated. However, many articles regarding the implementation procedures have not been clarified and these issues have been left to the Authority's initiative or secondary regulations to be made in the future. In other words, the PDPL has generally clarified the substantive issues, but has largely left the procedural issues to secondary regulations.

In conclusion, the GDPR has introduced stricter and more comprehensive rules, especially in terms of liability, sanctions, individual rights and data protection measures. Considering the increased responsibility of data processors, the legal definition of the right to be forgotten and the right to data portability, and the increase in administrative fines, it will be very useful to improve the PDPL, which was prepared in the basis of the Directive 95/46/EC and entered into force shortly before the adoption of the GDPR, according to the GDPR.

TABLE OF LEGISLATION

EU Law

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 26.10.2012 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M/TXT (05.08.2024)

Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108 (Convention 108)

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

European Convention on Human Rights (1950) [Council of Europe]

Recitals of General Data Protection Regulation

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 (General Data Protection Regulation) [2016] OJ L119/1

Translation of the Census Act Judgement https://freiheitsfoo.de/census-act/ (02.01.2024)

Turkish Law

Constitution of the Republic of Turkey, 1982

Directive on the Data Controllers Registry, 2017
https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=24276&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5 (05.08.2024)

Justification of the Personal Data Protection Law, 2016

Notification on the Procedures and Principles of Application to the Data Controller No. 30356, 10 March 2018 https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm (05.08.2024)

Personal Data Protection Authority, Explicit Consent 2017
https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf (03.08.2024)

Personal Data Protection Authority, Implementation Guide on the Law on the Protection of Personal Data 2020

Personal Data Protection Authority, Transfer of Personal Data Abroad 2017
https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20YURTDI%C5%9EINA%20AKTARILMASI.pdf (03.08.2024)

Personal Data Protection Law No. 6698 (Turkey), 24 March 2016, Official Gazette No. 29677

Personal Data Security Guide (Technical and Administrative Measures) https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf (03.08.2024)

Turkish Civil Code No. 4721, 22 November 2001

Turkish Code of Obligations No. 6098, 11 January 2011

Turkish Criminal Code No. 5237, 26 September 2004

Turkish Labour Law No. 4857, 10 May 2003

BIBLOGRAPHY

Akçalı Gur B, 'Transborder Flows of Personal Data: An International Law and EU Law Perspective' (2019) 25 Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 850

Akinci A N, 'Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakimindan Değerlendirilmesi' (2017) 6 T.C. Kalkinma Bakanliği Yayını 1

Akkurt S S, 'A Comparative Overview of the Ideas on the Legal Category of the Personal Data Concept' (2020) 2 Kişisel Verileri Koruma Dergisi 20

Aksoy H C, 'The Right to Personality and Its Different Manifestations As the Core of Personal Data' (2008) 5 Ankara Law Review 235

Antalya G, *Borclar Hukuku Genel Hukumler* (2nd edn, 2019, Seckin Yayincilik)

Asıkoglu S I, 'Information Obligation of Data Controllers In European Law and Turkish Law' (2019) 1 Kisisel Verileri Koruma Dergisi 41

Badur E & Kurt Konca N, 'Compensation for Damages Arising from The Unlawful Processing of Personal Data and The Authorized Court' (2022) I13 nonu Universitesi Hukuk Fakultesi Dergisi 476

Bulut I C, 'New Techniques and Enforcement Mechanisms Provided by the European Union General Data Protection Regulation' (2020) 20 Anadolu Üniversitesi Sosyal Bilimler Dergisi 127

Douglas M, 'Questioning the Right to Be Forgotten' (2015) 40 Alternative Law Journal 109

Dulger M V, ‘Protection of Personal Data in the Context of The European Union General Data Protection Regulation’ (2019) 1 Yasar Hukuk Dergisi 71

Dulger M V, ‘Protection of Personal Data with Criminal Norms in the context of Protection of Personal Data Law and Turkish Criminal Code’ (2016) Istanbul Medipol Universitesi Hukuk Fakultesi Dergisi 101

Evren A G, ‘A Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects’ (2023) 5 Kişisel Verileri Koruma Dergisi 39

Gursel I, 'Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law' (2016) 18 Dokuz Eylul Universitesi Hukuk Fakultesi Dergisi 33

Hert P & Lazcoz G, 'When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance' (2022) 8 Eur Data Prot L Rev 31

Hosnut Y, ‘Protection of Personal Data in Turkey and International Regulations’ (2019) 6 Yeni Medya, Hakemli, Akademik, E-Dergi 32, 38 https://dergipark.org.tr/tr/download/article-file/1302068 (04.04.2024)

Jay R, *Guide to the General Data Protection Regulation* (1st edn, Sweet & Maxwell 2017)

Keogh L L, *Data Protection Compliance A guide to GDPR and Irish Data Protection Law* (1st edn, Clarus Press Ltd)

Kılınc D, ‘Protection of Personal Data as a Constitutional Right’ (2012) 61 Ankara Universitesi Hukuk Fakultesi Dergisi 1089

Korkmaz I, ‘An Assessment of the Law on Protection of Personal Data’ (2016) 124 TBB Hukuk Dergisi 81

Kuner C & Bygrave L A & Docksey C (ed), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020)

Oguz S, ‘General Principles of Personal Data Protection Law’ (2018) 13 Bilgi Ekonomisi ve Yonetim Dergisi 121

Oguzman M K & Barlas N, *Medeni Hukuk* (20. edn, Vedat Kitapcilik 2014)

Ozkan R, 'Evaluation of Personal Data Protection Law within the Frame of Personal Right Protection' (2021) 3 Ankara Sosyal Bilimler Universitesi Hukuk Fakultesi Dergisi (ASBU Law Journal) 235

Pelen S, 'Transborder Transfer of Personal Data in Turkish Personal Data Protection Law' (2021) 12 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 458

Pendaroska L, 'International Transfer of Personal Data between the EU and Countries outside the EU' (2022) 13 Iustinianus Primus Law Review 1

Robinson N & Graux H & Botterman M & Valeri L, 'Review of the European Data Protection Directive' 2019 the RAND Corporation

Samuelson P, 'Privacy as Intellectual Property' (2000) 52 Stanford Law Review 1125

Saygı S, 'Judicial Remedies in the Systematics of Law No. 6698' (2020) 2 Kisiel Verileri Koruma Dergisi 30

Tekin N, 'An Assessment of the Turkish Draft Law on Protection of Personal Data in Light of the EU Data Protection Directive' (2014) 4 Uyusmazlik Mahkemesi Dergisi 222

Vogit P & Bussche A, *The EU General Data Protection Regulation (GDPR) A practical Guide* (1st edn, Springer International Publishing)

Yilmaz O B, *Turkiye ve Avrupa Birliği'nde Kisisel Verilerin Korunmasi ve Uygulanacak Hukuk* (1st edn, Adalet Yayınevi 2022)

Yuruk Z, 'Liability of The Data Controller to Take Administrative and Technical Measures Regarding Data Security' (2023) 22 İstanbul Ticaret Universitesi Sosyal Bilimler Dergisi 899